



# **SQL Anywhere® Server Datenbankadministration**

**Version 16.0**

**Februar 2013**

Version 16.0  
Februar 2013

© 2013 SAP AG oder ein SAP-Konzernunternehmen. Alle Rechte vorbehalten.

Sie können diese Dokumentation (ganz oder teilweise) unter folgenden Bedingungen benutzen, reproduzieren und verteilen: 1) Sie müssen diese und alle anderen Urheberrechtsvermerke auf allen Kopien oder Auszügen der Dokumentation wiedergeben. 2) Sie dürfen die Dokumentation nicht verändern. 3) Sie dürfen nichts tun, aus dem abgeleitet werden könnte, dass Sie oder jemand anderer als SAP Verfasser oder Quelle der Dokumentation ist. Die hier enthaltenen Informationen können jederzeit ohne vorherigen Hinweis geändert werden.

Einige Softwareprodukte, die von der SAP AG oder einem ihrer Vertriebspartner vermarktet werden, enthalten Softwarekomponenten anderer Softwareanbieter. Die nationalen Produktspezifikationen können unterschiedlich sein.

Diese Dokumentationen werden von der SAP AG und ihren Tochtergesellschaften ("SAP Group") lediglich zu Informationszwecken bereitgestellt, ohne dass eine Gewährleistung oder eine Garantie irgendeiner Art gegeben wird. Die SAP Group übernimmt keine Verantwortung im Hinblick auf Fehler oder Auslassungen in den Dokumentationen. Die einzigen Garantien für Produkte und Dienstleistungen der SAP Group sind diejenigen, die in den mit den Produkten und Dienstleistungen eventuell gelieferten ausdrücklichen Garantieerklärungen enthalten sind. Keine der hier enthaltenen Informationen kann als Gewährung einer weitergehenden Garantie betrachtet werden.

SAP und weitere erwähnte SAP-Produkte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern. Weitere Hinweise finden Sie unter <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark>.

---

---

# Inhalt

<b>Über diese Dokumentation .....</b>	<b>v</b>
<b>SQL Anywhere-Datenbankverbindungen .....</b>	<b>1</b>
Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen .....	1
Datenbankverbindungen .....	5
Kommunikationsprotokolle .....	102
Praktische Einführung: SQL Anywhere-Datenbank erstellen .....	114
Datenbankdateitypen .....	119
SQL Anywhere-Datenbankserver .....	150
Syntax des SQL Anywhere-Datenbankservers .....	203
Verbindungsparameter .....	337
Netzwerkprotokolloptionen .....	388
SQL Anywhere für Windows Mobile .....	423
<b>Datenbankkonfiguration .....</b>	<b>467</b>
SQL Anywhere-Umgebungsvariablen .....	467
Dateispeicherorte und Installationseinstellungen .....	482
Internationale Sprachen und Zeichensätze .....	491
Login-Richtlinien .....	535
Datenbankoptionen .....	544
Verbindungs-, Datenbank- und Datenbankservereigenschaften .....	710
SQL Anywhere-Einschränkungen von Größe und Anzahl .....	791
<b>Datenbankadministration .....</b>	<b>795</b>
SQL Anywhere - Grafische Administrationstools .....	795
Dienstprogramme für die Datenbankadministration .....	882
<b>Datenbankwartung .....</b>	<b>1027</b>
Sicherung und Datenwiederherstellung .....	1027

Datenbankvalidierung .....	1080
Aufgabenautomatisierung mit Abfolgeplanung und Ereignissen .....	1087
Ereignisprotokollierung .....	1101
Fehlerbehandlung im Zusammenhang mit SQL Anywhere-Problemen ...	1107
<b>Datenbank-Monitoring .....</b>	<b>1115</b>
SQL Anywhere-Monitor .....	1115
Der SQL Anywhere SNMP-Erweiterungsagent .....	1216
<b>Benutzer- und Datenbanksicherheit .....</b>	<b>1271</b>
Benutzersicherheit (Rollen und Privilegien) .....	1271
Datensicherheit .....	1402
Transportschichtssicherheit .....	1444
<b>Hochverfügbarkeit und Scale-Out-Systeme mit Schreibschutz ..</b>	<b>1467</b>
Datenbankspiegelung .....	1467
SQL Anywhere Veritas Cluster Server-Agenten .....	1527
SQL Anywhere-Scale-Out mit Schreibschutz .....	1536
<b>Replikation .....</b>	<b>1569</b>
SQL Anywhere als Open Server .....	1569
<b>Index .....</b>	<b>1575</b>

---

# Über diese Dokumentation

In diesem Handbuch wird beschrieben, wie Sie SQL Anywhere-Datenbanken betreiben, verwalten und konfigurieren. Es enthält Hinweise zu Datenbankverbindungen, Datenbankservern, Datenbankdateien, Datenbanksicherheit, Hochverfügbarkeit und zu den Dienstprogrammen und Optionen für die Datenbankadministration.



---

# SQL Anywhere-Datenbankverbindungen

## Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen

Die SQL Anywhere-Beispieldatenbank stellt ein kleines Unternehmen dar, das eine geringe Anzahl von Sportbekleidungsartikeln herstellt. Sie enthält interne Informationen über das Unternehmen, wie Mitarbeiter (employees), Abteilungen (departments) und Finanzdaten (financial\_data) sowie Produkt- und Verkaufsinformationen (products, sales\_orders, customers und contacts). Sämtliche Informationen in der Beispieldatenbank sind erfunden.

### Privilegien

Diese Aufgabe erfordert keine Privilegien.

### Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [[SQL Anywhere 16 - Einführung](#)]

## Lektion 1: Starten des SQL Anywhere-Datenbankservers und Anzeigen des Meldungsfensters für den Datenbankserver

Starten Sie einen SQL Anywhere-Datenbankserver und zeigen Sie das Meldungsfenster des Datenbankservers an, das Informationen über den Datenbankserver enthält.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen](#)“.

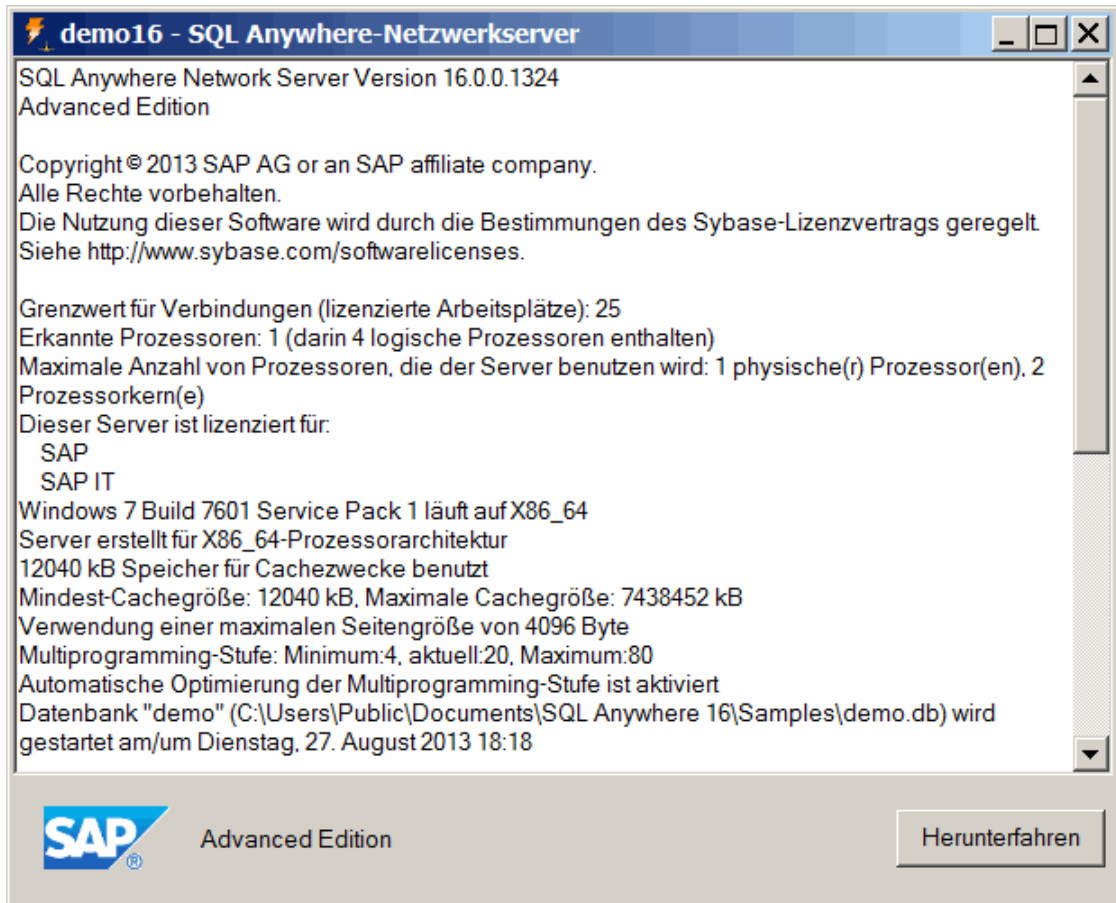
### Aufgabe

1. Führen Sie den folgenden Befehl an der Eingabeaufforderung aus, um den Datenbankserver zu starten, dem Datenbankserver mit der Serveroption -n den Namen demo16 zu geben und eine Verbindung mit der Beispieldatenbank herzustellen:

```
dbsrv16 -n demo16 "%SQLANYAMP16%\demo.db"
```

Unter Windows wird der Datenbankserver in der Taskleiste als Symbol angezeigt. Sie haben einen Datenbankserver erfolgreich gestartet, der die Beispieldatenbank ausführt. Sie können allerdings noch keine Daten sehen bzw. bearbeiten. Das Symbol des SQL Anywhere-Datenbankservers ist das einzige sichtbare Zeichen, dass etwas geschehen ist.

2. Doppelklicken Sie in der Taskleiste auf das Symbol des SQL Anywhere-Datenbankservers, um das Meldungsfenster des Datenbankservers anzuzeigen.



Das Meldungsfenster des Datenbankservers zeigt nützliche Informationen an, wie z.B.:

- **Den Servernamen** Der Name in der Titelleiste (in diesem Fall demo16) ist der **Servername**. In dieser praktischen Einführung haben Sie den Servernamen mithilfe der Serveroption -n zugeordnet. Wenn Sie keinen Servernamen angeben, erhält der Datenbankserver den Namen der ersten gestarteten Datenbank. Dieser Name kann von Anwendungen verwendet werden, wenn sie eine Verbindung zu einer Datenbank herstellen.
- **Versionsnummer und Build-Nummer** Die Zahlen nach dem Servernamen (z.B. **16.0.0.1403**) entsprechen der Versions- und Build-Nummer. Die Versionsnummer gibt die Version von SQL Anywhere an, die Build-Nummer zeigt die Instanz der Kompilierung.
- **Startinformationen** Wenn ein Datenbankserver aufgerufen wird, stellt er eine gewisse Menge an Speicherplatz bereit, den er bei der Verarbeitung von Datenbankanforderungen verwendet. Dieser reservierte Speicher wird **Cache** genannt. Der Umfang des Cachespeichers wird im Fenster angezeigt. Der Cache ist in **Seiten** fester Größe eingeteilt. Die Seitengröße wird ebenfalls im Fenster angezeigt. In diesem Fall handelt es sich bei den anfänglichen Cache- und Seitengrößen

um Standardwerte. Diese Standard-Startoptionen sind für viele Zwecke, einschließlich der in dieser praktischen Einführung behandelten, geeignet.

- **Datenbankinformationen** Die Namen der Datenbankdatei und ihrer Transaktionslogdateien werden im Fenster angezeigt.

## Ergebnisse

Ein Datenbankserver, der die Beispieldatenbank ausführt, wird gestartet und das Meldungsfenster des Datenbankservers wird angezeigt.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 2: Herstellen einer Verbindung mit der Datenbank“ auf Seite 3](#).

## Siehe auch

- [„Verbinden mit der Beispieldatenbank \(Sybase Central\)“ auf Seite 5](#)
- [„Verbinden mit der Beispieldatenbank \(Interactive SQL\)“ auf Seite 7](#)
- [„Verbinden mit der Beispieldatenbank unter Unix“ auf Seite 7](#)
- [„Verbindung zur Beispieldatenbank unter Mac OS X herstellen“ auf Seite 9](#)
- [„Datenbankserver starten“ auf Seite 153](#)
- [„SQL Anywhere-Datenbankserver“ auf Seite 150](#)
- [„Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203](#)

# Lektion 2: Herstellen einer Verbindung mit der Datenbank

Verbinden Sie sich mit der Beispieldatenbank mithilfe von Sybase Central.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Starten des SQL Anywhere-Datenbankservers und Anzeigen des Meldungsfensters für den Datenbankserver“ auf Seite 1](#).

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen“](#).

## Aufgabe

1. Starten Sie Sybase Central. Klicken Sie auf **Start&arrProgramme » SQL Anywhere 16 » Administrationtools » Sybase Central**.
2. Klicken Sie auf **Verbindungen » Verbinden mit SQL Anywhere 16**.
3. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Beispieldatenbank herzustellen:
  - a. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - b. Im Feld **Kennwort** geben Sie **sql** ein.

- c. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**.
- d. Im Feld **Servername** geben Sie **demo16** ein.

### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=*Servername*).

4. Klicken Sie auf **Verbinden**. Sybase Central stellt die Verbindung mit der Datenbank her.
5. (Optional) Führen Sie in Interactive SQL eine Abfrage der Customers-Tabelle aus.
  - a. Öffnen Sie Interactive SQL. Klicken Sie in Sybase Central auf **Datei » Interactive SQL öffnen**.
  - b. Führen Sie im Interactive SQL-Fenster die folgende SQL-Anweisung aus:

```
SELECT * FROM Customers;
```
  - c. Führen Sie die Anweisung aus. Drücken Sie F5 oder klicken Sie auf **SQL » Ausführen**.  
Die Ergebnismenge erscheint im Fensterausschnitt **Ergebnisse**.

### Ergebnisse

Sybase Central wird gestartet und mit der Beispieldatenbank verbunden.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: Stoppen des Datenbankservers](#)“.

### Siehe auch

- „[Verbinden mit der Beispieldatenbank \(Sybase Central\)](#)“ auf Seite 5

## Lektion 3: Stoppen des Datenbankservers

Stoppen Sie den Datenbankserver mithilfe des Serverstopp-Dienstprogramms.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Starten des SQL Anywhere-Datenbankservers und Anzeigen des Meldungsfensters für den Datenbankserver](#)“ auf Seite 1.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen](#)“.

## Kontext und Bemerkungen

In Windows-Umgebungen können Sie einen Datenbankserver stoppen, indem Sie im Meldungsfenster des Datenbankservers auf **Herunterfahren** klicken.

## Aufgabe

1. Führen Sie den folgenden Befehl aus, um den Datenbankserver zu stoppen, der die Beispieldatenbank ausführt:

```
dbstop demo16
```

2. Wenn gemeldet wird, dass die Datenbank Verbindungen hat, geben Sie **Y** ein.

## Ergebnisse

Der Datenbankserver wird gestoppt und alle Verbindungen zur Beispieldatenbank werden beendet.

## Nächste Schritte

(Optional) Erstellen Sie die Beispieldatenbank neu, um alle an ihr vorgenommenen Änderungen rückgängig zu machen. Siehe „[Neuerstellung der Beispieldatenbank \(demo.db\)](#)“ [[SQL Anywhere 16 - Einführung](#)].

## Siehe auch

- „Serverstopp-Dienstprogramm (dbstop)“ auf Seite 984
- „SQL Anywhere-Datenbankserver“ auf Seite 150

# Datenbankverbindungen

## Verbinden mit der Beispieldatenbank (Sybase Central)

Verbinden Sie sich mit der Beispieldatenbank, um sich mit SQL Anywhere vertraut zu machen und Beispiele auszuprobieren, wie Sie sie überall in der Dokumentation finden.

## Voraussetzungen

**Linux** Ihre Version von Linux muss das Linux-**Anwendungsmenü** unterstützen. Die Menüelemente müssen im Rahmen der SQL Anywhere-Installation installiert werden.

**Unix** Das Sourcen der SQL Anywhere-Dienstprogramme muss bereits abgeschlossen sein. Siehe „[Unix- und Mac OS X-Umgebungsvariablen](#)“ auf Seite 467.

**Mac OS X** Das Sourcen der SQL Anywhere-Dienstprogramme muss bereits abgeschlossen sein. Siehe „[Unix- und Mac OS X-Umgebungsvariablen](#)“ auf Seite 467.

### Kontext und Bemerkungen

Sybase Central ist ein grafisches Tool, das Sie als Alternative zu SQL-Anweisungen und Befehlszeilen-Dienstprogrammen verwenden können, um Ihre Datenbankserver und Datenbanken sowie die darin enthaltenen Objekte zu verwalten.

Diese Vorgehensweise gilt nicht für Windows Mobile.

### Aufgabe

1. Klicken Sie zum Öffnen von Sybase Central auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.

#### Hinweis

**Mac OS X** Doppelklicken Sie im Finder auf **Sybase Central** in */Applications/SQLAnywhere16*.

**Unix** Führen Sie in einer Terminalsitzung den folgenden Befehl aus:

```
scjview
```

**Linux** Klicken Sie auf **Anwendungen » SQL Anywhere 16 » Administrationstools » Sybase Central**.

2. Klicken Sie auf **Verbindungen » Verbinden mit SQL Anywhere 16**.
3. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit ODBC-Datenquelle verbinden**.
4. Klicken Sie auf **ODBC-Datenquellenname** und geben Sie im Feld darunter **SQL Anywhere 16 Demo** ein.

#### Hinweis

- Sie brauchen für diese Verbindung keine Benutzer-ID und kein Kennwort einzugeben, da die Datenquelle **SQL Anywhere 16 Demo** diese Informationen bereits enthält.  
In einer Produktionsumgebung sollten Sie keine Kennwörter in einer ODBC-Datenquelle speichern.
- Der Datenbankserver muss nicht laufen, bevor Sie eine Verbindung herstellen, da die Datenquelle **SQL Anywhere 16 Demo** genügend Informationen enthält, um den Datenbankserver automatisch zu starten.

5. (Optional) Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
6. Klicken Sie auf **Verbinden**.

## Ergebnisse

Der Datenbankserver und die Datenbank werden gestartet und Sybase Central stellt eine Verbindung mit der Beispieldatenbank her.

### Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [*SQL Anywhere 16 - Einführung*]
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „sa\_config.sh und sample\_config32.sh/sample\_config64.sh sourcen [Unix und Mac OS X]“ auf Seite 468
- Keine Kennwörter in ODBC-Datenquellen einschließen auf Seite 1411
- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20

## Verbinden mit der Beispieldatenbank (Interactive SQL)

Starten Sie Interactive SQL und stellen Sie über eine Eingabeaufforderung eine Verbindung mit der Beispieldatenbank her.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Für viele Beispiele in der Dokumentation wird die SQL Anywhere-Beispieldatenbank verwendet. Sie können sich mit dieser Datenbank verbinden und sich mit SQL Anywhere vertraut machen.

### Aufgabe

- Führen Sie den folgenden Befehl aus, um Interactive SQL zu starten und sich mit der Beispieldatenbank zu verbinden:

```
dbisql -c "UID=DBA;PWD=sql;DBF=%SQLANYAMP16%\demo.db"
```

### Ergebnisse

Interactive SQL wird gestartet und stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [*SQL Anywhere 16 - Einführung*]
- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20

## Verbinden mit der Beispieldatenbank unter Unix

Für viele Beispiele in der Dokumentation wird die SQL Anywhere-Beispieldatenbank verwendet. Verbinden Sie sich mit dieser Datenbank und machen Sie sich mit SQL Anywhere vertraut.

### Voraussetzungen

In der folgenden Prozedur wird Interactive SQL verwendet, um eine Verbindung mit der Datenbank herzustellen. Stellen Sie sicher, dass die Java-Laufzeitumgebung (Java Runtime Environment, JRE) installiert ist.

In einer typischen Unix-Installation ist die SQL Anywhere-Software, einschließlich der Beispieldatenbank, in einem Verzeichnis installiert, für das Sie keine Schreibberechtigungen haben. Bevor Sie beginnen, wechseln Sie in einem Terminalfenster zu einem Ordner mit Schreibberechtigung. Führen Sie den folgenden Befehl aus, um die Beispieldatenbankdatei in den Ordner zu kopieren:

```
cp "samples-dir/demo.db" .
```

Führen Sie in einem Terminalfenster den folgenden Befehl aus, um die Beispieldatenbank auf einem Datenbankserver zu starten:

```
dbeng16 demo.db
```

### Aufgabe

1. Starten Sie Interactive SQL in einem Terminalfenster:

```
dbisql
```

Standardmäßig wird das Fenster **Verbinden** eingeblendet.

2. Machen Sie im Fenster **Verbinden** die folgenden Angaben:
  - a. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - b. Im Feld **Kennwort** geben Sie **sql** ein.
  - c. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**.
  - d. Im Feld **Servername** geben Sie **demo** ein.
  - e. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
  - f. Klicken Sie auf **Verbinden**.

### Ergebnisse

Interactive SQL wird gestartet und stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [[SQL Anywhere 16 - Einführung](#)]
- „ODBC-Datenquellen unter Unix“ auf Seite 49
- „Verbindung zur Beispieldatenbank unter Mac OS X herstellen“ auf Seite 9

## Verbindung zur Beispieldatenbank unter Mac OS X herstellen

Für viele Beispiele in der Dokumentation wird die SQL Anywhere-Beispieldatenbank verwendet. Verbinden Sie sich mit dieser Datenbank und machen Sie sich mit SQL Anywhere vertraut.

### Voraussetzungen

- Ermitteln Sie im **Finder** den Speicherort der SQL Anywhere-Beispieldatenbank und kopieren Sie die Datei an einen Speicherort, für den Sie Lese- und Schreibzugriff haben. Standardmäßig befindet sich die Beispieldatenbank in */Applications/SQLAnywhere16/demo.db*;
- Starten Sie einen Datenbankserver. Im **Finder** doppelklicken Sie auf **DBLauncher**. Standardmäßig befindet sich **DBLauncher** in folgendem Pfad: */Applications/SQLAnywhere16* .
  1. Im Feld **Datenbank** navigieren Sie zum Speicherort der SQL Anywhere-Beispieldatenbank. (Beispiel: */Applications/SQLAnywhere16/System/demo.db*.)
  2. Im Feld **Servername** geben Sie **demo** ein.
  3. Klicken Sie auf **Lokaler Server**.

Bei der Option **Lokaler Server** ist eine Client/Serverkommunikation über ein Netzwerk nicht zulässig.

4. Klicken Sie auf **Start**, um einen Personal Datenbankserver namens **demo** zu starten.

### Aufgabe

1. Doppelklicken Sie im **Finder** auf **Interactive SQL** in */Applications/SQLAnywhere16*.
2. Verbinden Sie sich mit der SQL Anywhere-Beispieldatenbank, indem Sie im Fenster **Verbinden** die folgenden Angaben machen:
  - Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - Im Feld **Kennwort** geben Sie **sql** ein.
  - Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**, um eine Verbindung mit der Datenbank herzustellen, die auf Ihrem Computer läuft.
  - Im Feld **Servername** geben Sie **demo** ein.
  - Im Feld **Datenbankname** geben Sie **demo** ein.
  - Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
  - Klicken Sie auf **Verbinden**.

### Ergebnisse

Interactive SQL wird gestartet und stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [[SQL Anywhere 16 - Einführung](#)]
- „Verbinden mit der Beispieldatenbank unter Unix“ auf Seite 7
- „Erstellen einer ODBC-Datenquelle (Mac OS X)“ auf Seite 44

## Verbindungsprofile in Sybase Central

Wenn Sie zum ersten Mal eine Verbindung zu einem Datenbankserver oder einer Datenbank herstellen, geben Sie einen Benutzernamen, ein Kennwort und andere Verbindungsparameter an. Die Informationen müssen bei nachfolgenden Verbindungen wieder eingegeben werden. Um beim Arbeiten mit Sybase Central Zeit zu sparen und den Verbindungsvorgang zu vereinfachen, können Sie Verbindungsprofile erstellen und darin die Verbindungsparameter für die einzelnen Datenbanken speichern.

Wenn Sie Verbindungsprofile verwenden und verwalten möchten, klicken Sie in Sybase Central auf **Verbindungen » Verbindungsprofil**, um das Fenster **Verbindungsprofil** zu öffnen. Verwenden Sie das Fenster **Verbindungsprofil** für folgende Vorgänge:

- Neues Verbindungsprofil erstellen.
- Ein Verbindungsprofil so aktivieren, dass beim Start von Sybase Central damit automatisch eine Verbindung eingerichtet wird.
- Bestehendes Verbindungsprofil bearbeiten.
- Verbindung mit einem Verbindungsprofil herstellen.
- Ein Verbindungsprofil löschen.
- Ein Verbindungsprofil importieren oder exportieren.

#### Hinweis

Verbindungsprofile gelten nur für Sybase Central. Wenn Sie eine ODBC-Anwendung erstellen, können Sie ODBC-Datenquellen verwenden, um Funktionen einzurichten, die die Aufgaben von Verbindungsprofilen übernehmen. Siehe „[ODBC-Datenquellen](#)“ auf Seite 38.

## Verbindungsprofile erstellen

Um den Verbindungsvorgang in Sybase Central zu vereinfachen, können Sie ein Verbindungsprofil erstellen und darin die Verbindungsparameter für eine Datenbank speichern.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Verbindungsprofile gelten nur für Sybase Central. Wenn Sie eine ODBC-Anwendung erstellen, können Sie ODBC-Datenquellen verwenden, um Funktionen einzurichten, die die Aufgaben von Verbindungsprofilen übernehmen.

### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder unverschlüsselten Kennwörtern sowie Datenbankschlüsseln in einem Verbindungsprofil wird nicht empfohlen.

## Aufgabe

1. Klicken Sie in Sybase Central auf **Verbindungen** » **Verbindungsprofile**.
2. Klicken Sie auf **Neu**.
3. Im Feld **Name** geben Sie einen Namen für das neue Profil ein.
4. Klicken Sie auf **Neues Profil erstellen** und wählen Sie das betreffende Plug-In aus der Dropdown-Liste. Das Plug-In ist das Produkt, beispielsweise **SQL Anywhere 16** oder **UltraLite 16**.

Um Ihr neues Verbindungsprofil aus einem vorhandenen Profil zu erstellen, klicken Sie auf **Profil kopieren** und wählen in der Liste **Vorhandene Profile** das gewünschte Profil.

5. (Optional) Um anderen Benutzern Zugriff auf das Profil zu gewähren, klicken Sie auf **Dieses Verbindungsprofil mit anderen Benutzern gemeinsam nutzen**. Diese Einstellung ist auf Mehrbenutzerplattformen wie Unix sinnvoll.
6. Klicken Sie auf **OK**.
7. Im Fenster **Verbindungsprofil bearbeiten** geben Sie die gewünschten Werte ein und klicken anschließend auf **Speichern**, um das Fenster zu schließen.
8. Klicken Sie auf **Schließen**.

## Ergebnisse

Das Verbindungsprofil wird erstellt und Sie können es verwenden, um sich mit Ihrer Datenbank zu verbinden.

## Nächste Schritte

Sie können Sybase Central so konfigurieren, dass beim Starten von Sybase Central automatisch eine Verbindung mit diesem Verbindungsprofil hergestellt wird.

## Siehe auch

- [„ODBC-Datenquellen“ auf Seite 38](#)
- [„Verbindungen mit Verbindungsprofilen herstellen“ auf Seite 12](#)
- [„Verbindungsprofile exportieren und importieren“ auf Seite 13](#)

## Verbindungen mit Verbindungsprofilen herstellen

Verwenden Sie ein Verbindungsprofil, um über Sybase Central eine Verbindung mit einem Datenbankserver oder einer Datenbank herzustellen.

### Voraussetzungen

Ein Verbindungsprofil muss definiert werden.

### Kontext und Bemerkungen

Wenn Sie normalerweise in Sybase Central auf dasselbe Verbindungsprofil zurückgreifen, können Sie Sybase Central so konfigurieren, dass Ihr Verbindungsprofil standardmäßig verwendet wird. Beim Starten von Sybase Central wird das Verbindungsprofil verwendet, um automatisch eine Verbindung mit Ihrer Datenbank herzustellen.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Verbindungen » Verbindungsprofile**.

Das Fenster **Verbindungsprofile** wird eingeblendet.

2. Wählen Sie ein Profil und klicken Sie auf **Verbinden**.

#### Tipp

Damit Sybase Central automatisch eine Verbindung mit Ihrem Verbindungsprofil herstellt, klicken Sie auf **Startvorgabe**, um die Spalte **Beim Start verwenden** auf **Ja** zu setzen.

3. Klicken Sie auf **Schließen**.

### Ergebnisse

Sobald die Verbindung hergestellt ist, erscheint ein Symbol im Hauptfenster von Sybase Central.

### Siehe auch

- „Verbindungsprofile in Sybase Central“ auf Seite 10
- „Verbindungsprofile exportieren und importieren“ auf Seite 13

## Verbindungsprofile bearbeiten

Wenn sich die Verbindungsinformationen für ein Verbindungsprofil ändern, können Sie das Verbindungsprofil bearbeiten und die Verbindungsparameter speichern.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Verbindungen » Verbindungsprofile**.
2. In der Liste **Verbindungsprofile** wählen Sie ein Verbindungsprofil aus.
3. Klicken Sie auf **Bearbeiten**.
4. Im Fenster **Verbindungsprofil bearbeiten** bearbeiten Sie die Eingaben.
5. Klicken Sie auf **Speichern** und dann auf **Schließen**.

### Ergebnisse

Das Verbindungsprofil wird gespeichert.

### Siehe auch

- „Verbindungen mit Verbindungsprofilen herstellen“ auf Seite 12
- „Verbindungsprofile exportieren und importieren“ auf Seite 13
- „Verbindungsprofile erstellen“ auf Seite 10

## Verbindungsprofile exportieren und importieren

Um Verbindungsprofile mit Benutzern auf anderen Computern gemeinsam zu nutzen oder Ihre Verbindungsprofile zu sichern, können Sie sie in eine Datei exportieren. Um ein an anderer Stelle erstelltes Verbindungsprofil verwenden zu können, müssen Sie das Verbindungsprofil importieren.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Klicken Sie auf **Verbindungen » Verbindungsprofile**.
2. Wählen Sie eine der folgenden Optionen:

Option	Aktion
Verbindungsprofil importieren	<ol style="list-style-type: none"><li>a. Klicken Sie auf <b>Importieren</b>.</li><li>b. Im Feld <b>Dateiname</b> geben Sie den Namen der Verbindungsprofildatei ein, die Sie importieren möchten.</li><li>c. Klicken Sie auf <b>OK</b>.</li></ol>

Option	Aktion
Verbindungsprofil exportieren	<ol style="list-style-type: none"><li>In der Liste <b>Verbindungsprofile</b> wählen Sie ein Verbindungsprofil aus.</li><li>Klicken Sie auf <b>Exportieren</b>.</li><li>Im Feld <b>Dateiname</b> geben Sie einen Dateinamen für das Verbindungsprofil ein.</li><li>Klicken Sie auf <b>Speichern</b>.</li></ol>

3. Klicken Sie auf **Schließen**.

### Ergebnisse

Das Verbindungsprofil wird exportiert bzw. importiert.

### Siehe auch

- „Verbindungen mit Verbindungsprofilen herstellen“ auf Seite 12
- „Verbindungsprofile erstellen“ auf Seite 10

## Das Fenster Verbinden öffnen (Sybase Central)

Standardmäßig wird das Fenster **Verbinden** geöffnet, wenn Sie ein Administrationstool starten. Wenn in Sybase Central das Fenster **Verbinden** nicht automatisch geöffnet wird, können Sie es manuell öffnen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Sie können das Fenster **Verbinden** in Sybase Central verwenden, um eine Verbindung mit einem Datenbankserver oder einer Datenbank durch Angeben von Verbindungsparametern herzustellen.

Informationen, die Sie im Fenster **Verbinden** eingeben, werden beibehalten, solange das Administrationstool läuft.

### Aufgabe

1. Starten Sie Sybase Central.
2. Klicken Sie auf **Verbindungen » Verbinden mit SQL Anywhere 16**.

Alternativ können Sie das Menü **Verbindungen** durch Drücken der Taste F11 öffnen.

### Ergebnisse

Das Fenster **Verbinden** wird geöffnet.

**Siehe auch**

- „Verbinden mit der Beispieldatenbank (Sybase Central)“ auf Seite 5
- „Verbindungs-IDs“ auf Seite 30

## Das Fenster Verbinden öffnen (Interactive SQL)

Standardmäßig wird das Fenster **Verbinden** geöffnet, wenn Sie ein Administrationstool starten. Wenn in Interactive SQL das Fenster **Verbinden** nicht automatisch geöffnet wird, können Sie es manuell öffnen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Sie können das Fenster **Verbinden** in Interactive SQL verwenden, um eine Verbindung mit einem Datenbankserver oder einer Datenbank durch Angeben von Verbindungsparametern herzustellen.

Informationen, die Sie im Fenster **Verbinden** eingeben, werden beibehalten, solange das Administrationstool läuft.

**Aufgabe**

1. Starten Sie Interactive SQL.
2. Klicken Sie auf **SQL » Verbinden**.

Außerdem können Sie das Fenster **Verbinden** durch Drücken der Taste F11 aufrufen.

**Ergebnisse**

Das Fenster **Verbinden** wird geöffnet.

**Siehe auch**

- „Interactive SQL starten“ auf Seite 815
- „Verbindungs-IDs“ auf Seite 30

## Das Fenster Verbinden öffnen (Dienstprogramm dbconsole)

Standardmäßig wird das Fenster **Verbinden** geöffnet, wenn Sie ein Administrationstool starten. Wenn im SQL Anywhere-Konsolendienstprogramm das Fenster **Verbinden** nicht automatisch geöffnet wird, können Sie es manuell öffnen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Sie können das Fenster **Verbinden** im SQL Anywhere-Konsolendienstprogramm verwenden, um eine Verbindung mit einem Datenbankserver oder einer Datenbank durch Angeben von Verbindungsparametern herzustellen.

Informationen, die Sie im Fenster **Verbinden** eingeben, werden beibehalten, solange das Administrationstool läuft.

### Aufgabe

1. Starten Sie das SQL Anywhere-Konsolendienstprogramm.
2. Klicken Sie auf **Befehl » Verbinden**.

Alternativ können Sie das Fenster **Verbinden** durch Drücken der Taste F11 aufrufen.

### Ergebnisse

Das Fenster **Verbinden** wird geöffnet.

### Siehe auch

- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 877
- „Verbindungs-IDs“ auf Seite 30

## Datenbanken auf lokalen Computern starten und Verbindungen herstellen (Sybase Central oder Interactive SQL)

Um von demselben Computer aus einen Datenbankserver und eine Datenbank zu starten und anschließend eine Verbindung mit der lokalen Datenbank herzustellen, können Sie im Fenster **Verbinden** die Option **Eine Datenbank auf diesem Computer starten und eine Verbindung herstellen** wählen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. Geben Sie im Feld **Kennwort** das Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.

- d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Eine Datenbank auf diesem Computer starten und eine Verbindung herstellen**.
- e. Im Feld **Datenbankdatei** geben Sie den Dateipfad, den Dateinamen und die Dateierweiterung der Datenbank an. Geben Sie zum Beispiel Folgendes ein: *C:\Users\Public\Documents\SQL Anywhere 16\Samples\demo.db*.
- f. Um einen Datenbanknamen zu erstellen, der vom Dateinamen für nachfolgende Verbindungen abweicht, geben Sie einen Namen in das Feld **Datenbankname** ein. Geben Sie keinen Dateipfad und keine Erweiterung an.
- g. Im Feld **Servename** geben Sie einen Namen für den Datenbankserver ein. Geben Sie zum Beispiel Folgendes ein: **demo16**.

**Hinweis**

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=Servername).

3. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
4. Klicken Sie auf **Verbinden**.

**Ergebnisse**

Der Datenbankserver und die Datenbank werden gestartet und das Administrationstool stellt eine Verbindung mit der Datenbank her.

**Siehe auch**

- „Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen“ auf Seite 1
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14

## Verbindungen mit laufenden Datenbanken auf lokalen Computern herstellen

Um eine Verbindung mit einer lokalen Datenbank herzustellen, die derzeit ausgeführt wird, können Sie im Fenster **Verbinden** die Option **Mit einer laufenden Datenbank auf diesem Computer verbinden** wählen.

**Voraussetzungen**

Bei dieser Vorgehensweise wird angenommen, dass eine Datenbank auf einem Datenbankserver auf Ihrem Computer läuft. Wenn noch keine Datenbank läuft, starten Sie einen Datenbankserver und eine Datenbank. Führen Sie beispielsweise folgenden Befehl zum Starten der SQL Anywhere 16-Beispieldatenbank auf einem Personal Datenbankserver aus:

```
dbeng16 -n demo16 "%SQLANYAMP16%\demo.db"
```

### Aufgabe

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**, um eine Verbindung mit einer Datenbank herzustellen, die auf Ihrem Computer läuft.
  - e. Im Feld **Servername** geben Sie den Namen des laufenden Datenbankservers ein. Geben Sie zum Beispiel Folgendes ein: **demo16**.

#### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=*Servername*).

- f. Im Feld **Datenbankname** geben Sie den Namen der Datenbank ein. Geben Sie zum Beispiel Folgendes ein: **demo**.
3. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
  4. Klicken Sie auf **Verbinden**.

### Ergebnisse

Die Anwendung stellt eine Verbindung zur Datenbank her.

### Siehe auch

- „Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen“ auf Seite 1
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14

## Verbindungen mit Datenbanken auf lokalen Computern herstellen (Interactive SQL)

Sie können eine Verbindung mit einer lokalen Datenbank herstellen, indem Sie das Dienstprogramm Interactive SQL an einer Eingabeaufforderung ausführen. Sie können die Datenbank und den

Datenbankserver starten und eine Verbindung herstellen oder eine Verbindung mit einer laufenden Datenbank herstellen.

**Voraussetzungen**

Bei dieser Vorgehensweise wird angenommen, dass eine Datenbank auf einem Datenbankserver auf Ihrem Computer läuft. Wenn noch keine Datenbank läuft, starten Sie einen Datenbankserver und eine Datenbank. Führen Sie beispielsweise den folgenden Befehl aus, um die SQL Anywhere 16-Beispieldatenbank auf einem Datenbankserver zu starten:

```
dbsrv16 -n database-name "file path"
```

Es gibt keine Voraussetzungen für diese Aufgabe.

**Aufgabe**

- Führen Sie den folgenden Befehl aus, um Interactive SQL zu starten und sich mit einer Datenbank zu verbinden:

Option	Aktion
Datenbanken starten und Verbindungen herstellen	<code>dbisql -c "UID=user-id;PWD=password;ServerName=server-name;DBF=database-file"</code>
Mit einer laufenden Datenbank verbinden	<code>dbisql -c "UID=user-id;PWD=password;ServerName=server-name;DBN=database-name"</code>

**Ergebnisse**

Interactive SQL wird gestartet und stellt eine Verbindung mit der Datenbank her.

**Beispiel**

Führen Sie den folgenden Befehl aus, um über Interactive SQL einen Datenbankserver und eine Datenbank zu starten und eine Verbindung mit der Datenbank herzustellen:

```
dbisql -c "UID=DBA;PWD=sql;ServerName=mydemo;DBF=%SQLANYAMP16%demo.db"
```

# Verbindungen über ODBC-Datenquellen herstellen (Administrationstools)

Um eine Verbindung mit einer Datenbank über eine ODBC-Datenquelle herzustellen, wählen Sie im Fenster **Verbinden** die Option **ODBC-Datenquellenname**.

**Voraussetzungen**

Eine ODBC-Datenquelle für die Datenbank, mit der Sie eine Verbindung herstellen möchten.

Die Datenquelle **SQL Anywhere 16 Demo** ist so konfiguriert, dass sie den Datenbankserver und die Datenbank startet, wenn sie noch nicht laufen. Wenn Ihre ODBC-Datenquelle nicht so konfiguriert ist, dass sie die Datenbank und den Datenbankserver startet, müssen Sie sie starten. Führen Sie beispielsweise folgenden Befehl aus, um die Beispieldatenbank zu starten:

```
dbsrv16 -n demo16 "%SQLANYAMP16%\demo.db"
```

### Aufgabe

1. Öffnen Sie das Fenster **Verbinden** über die Administrationstools, z.B. Interactive SQL.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit ODBC-Datenquelle verbinden**.
  - e. Führen Sie eine der folgenden Aktionen aus:
    - Klicken Sie auf **ODBC-Datenquellenname** und geben Sie den Namen der Datenquelle ein. Geben Sie zum Beispiel Folgendes ein: **SQL Anywhere 16 Demo**.
    - Klicken Sie auf **ODBC-Datenquellendatei** und geben Sie den FileDataSourceName-Verbindungsparameter (FILEDSN) ein, der eine Datenquelle in einer Datei referenziert.
3. (Optional) Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
4. Klicken Sie auf **Verbinden**.

### Ergebnisse

Das Administrationstool stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „ODBC-Datenquellen“ auf Seite 38
- „ODBC-Datenquellen unter Unix“ auf Seite 49
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14

## Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)

Sie können eine Verbindung mit einer Datenbank über eine ODBC-Datenquelle herstellen, indem Sie das Dienstprogramm Interactive SQL an einer Eingabeaufforderung ausführen und den DataSourceName-Verbindungsparameter (DSN) eingeben.

## Voraussetzungen

Eine ODBC-Datenquelle für die Datenbank, mit der Sie eine Verbindung herstellen möchten.

Die Datenquelle **SQL Anywhere 16 Demo** ist so konfiguriert, dass sie den Datenbankserver und die Datenbank startet, wenn sie noch nicht laufen. Wenn Ihre ODBC-Datenquelle nicht so konfiguriert ist, dass sie die Datenbank und den Datenbankserver startet, müssen Sie sie starten. Führen Sie beispielsweise folgenden Befehl aus, um die Beispieldatenbank zu starten:

```
dbsrv16 -n demo16 "%SQLANYSAMPl6%\demo.db"
```

## Kontext und Bemerkungen

Wenn eine Verbindungszeichenfolge und eine ODBC-Datenquelle beide denselben Verbindungsparameter angeben, wird der Wert aus der Zeichenfolge verwendet und der Wert aus der Datenquelle ignoriert.

### Hinweis

Sie brauchen für diese Verbindung keine Benutzer-ID und kein Kennwort einzugeben, da die Datenquelle **SQL Anywhere 16 Demo** diese Informationen bereits enthält.

In einer Produktionsumgebung wird empfohlen, keine Kennwörter in einer ODBC-Datenquelle zu speichern.

## Aufgabe

- Führen Sie den folgenden Befehl aus, um eine Verbindung mit dem ODBC-Datenquellennamen herzustellen:

```
dbisql -c "DSN=SQL Anywhere 16 Demo"
```

## Ergebnisse

Interactive SQL wird gestartet und stellt eine Verbindung mit der Datenbank her.

## Siehe auch

- [„Verbindungsparameter DataSourceName \(DSN\)“ auf Seite 356](#)
- [„Syntaxregeln für Verbindungsparameter“ auf Seite 36](#)
- [„ODBC-Datenquellen“ auf Seite 38](#)
- [„ODBC-Datenquellen unter Unix“ auf Seite 49](#)
- [Keine Kennwörter in ODBC-Datenquellen einschließen auf Seite 1411](#)

## Verbindungen über ODBC-Datenquellen mit Verbindungszeichenfolgen herstellen (Administrationstools)

Um im Fenster **Verbinden** eine Verbindungszeichenfolge anzugeben, wählen Sie die Option **Mithilfe einer Verbindungszeichenfolge verbinden**. Diese Option ist nützlich, wenn Sie eine ODBC-Datenquelle haben und beim Herstellen der Verbindung zusätzliche oder andere Parameter angeben möchten.

### Voraussetzungen

Bei der hier beschriebenen Vorgehensweise enthält die Verbindungszeichenfolge den DSN-Verbindungsparameter, um eine Verbindung mit der Datenquelle **SQL Anywhere 16 Demo** herzustellen. Diese Datenquelle ist so konfiguriert, dass sie den Datenbankserver und die Datenbank startet, wenn sie noch nicht laufen. Wenn Ihre ODBC-Datenquelle nicht so konfiguriert ist, dass sie die Datenbank und den Datenbankserver startet, müssen Sie sie starten. Führen Sie beispielsweise folgenden Befehl aus, um die Beispieldatenbank zu starten:

```
dsbdrv16 -n SampleServer "%SQLANYAMP16%\demo.db"
```

### Kontext und Bemerkungen

Wenn eine Verbindungszeichenfolge und eine ODBC-Datenquelle beide denselben Verbindungsparameter angeben, wird der Wert aus der Zeichenfolge verwendet und der Wert aus der Datenquelle ignoriert.

### Aufgabe

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mithilfe einer Verbindungszeichenfolge verbinden**.
  - e. In das Feld **Parameter** geben Sie die Verbindungsparameter in einer durch Semikola getrennten Liste von Parameter=Wert-Paaren ein. Zum Beispiel:

```
DSN=SQL Anywhere 16 Demo;ServerName=SampleServer
```

Der Datenbankserver und die Datenbank werden gestartet und Interactive SQL stellt eine Verbindung mit der Datenbank her. Der Datenbankserver hat den Namen SampleServer.

#### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=Servername).

3. Klicken Sie auf **Verbinden**.

## Ergebnisse

Das Administrationstool stellt eine Verbindung mit der Datenbank her.

## Siehe auch

- [Als Verbindungszeichenfolge übergebene Verbindungsparameter auf Seite 31](#)
- [„Syntaxregeln für Verbindungsparameter“ auf Seite 36](#)

# Mit laufenden Datenbanken auf anderen Computern verbinden (Administrationstools)

Um eine Verbindung mit einer Datenbank herzustellen, die auf einem Netzwerk- Datenbankserver läuft, können Sie im Fenster **Verbinden** die Option **Mit einer laufenden Datenbank auf einem anderen Computer verbinden** wählen.

## Voraussetzungen

Bei dieser Vorgehensweise wird angenommen, dass eine Datenbank auf einem Netzwerk- Datenbankserver auf einem anderen Computer läuft. Wenn noch keine Datenbank läuft, starten Sie einen Datenbankserver und eine Datenbank. Führen Sie beispielsweise folgenden Befehl aus, um die Beispieldatenbank zu starten:

```
dbsrv16 -n demo16 "%SQLANYAMP16%\demo.db"
```

## Aufgabe

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf einem anderen Computer verbinden**, um eine Verbindung mit einer Datenbank herzustellen, die auf einem anderen Computer läuft.
  - e. Im Feld **Host** geben Sie den Hostnamen des Computers ein, auf dem der Datenbankserver läuft.
  - f. Im Feld **Servername** geben Sie den Namen des Servers ein oder klicken Sie auf **Suchen**. Geben Sie zum Beispiel Folgendes ein: **demo16**.

### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=*Servername*).

- g. Geben Sie in das Feld **Datenbankname** den Namen der Datenbank ein. Geben Sie zum Beispiel Folgendes ein: **demo**.
3. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
4. Klicken Sie auf **Verbinden**.

### Ergebnisse

Das Administrationstool stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen“ auf Seite 1

## Verbindungen mit laufenden Datenbanken auf anderen Computern herstellen (Befehlszeile)

Sie können eine Verbindung mit einer Datenbank herstellen, die auf einem Netzwerk-Datenbankserver läuft, indem Sie das Dienstprogramm Interactive SQL an einer Eingabeaufforderung ausführen und den Host-Verbindungsparameter eingeben.

### Voraussetzungen

Eine Datenbank muss auf einem anderen Computer laufen.

### Aufgabe

- Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=user-ID;PWD=password;ServerName=server-name;Host=host-name"
```

### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (ServerName=*Servername*).

### Ergebnisse

Die Anwendung stellt eine Verbindung mit der Datenbank her.

## Beispiel

Führen Sie den folgenden Befehl aus, um eine Verbindung mit der Beispieldatenbank auf dem Host my\_host herzustellen:

```
dbisql -c "UID=DBA;PWD=sql;ServerName=demo16;Host=my_host"
```

## Siehe auch

- „Host-Verbindungsparameter“ auf Seite 363

# Herstellen einer Verbindung zu einer Datenbank in einer Cloud (Administrationstools)

Um eine Verbindung mit einer Datenbank herzustellen, die derzeit in der Cloud ausgeführt wird, können Sie im Fenster **Verbinden** die Option **Verbindung mit einer laufenden Datenbank in einer Cloud herstellen** wählen.

## Voraussetzungen

Um eine Verbindung mit einer Datenbank in der Cloud herstellen zu können, müssen Sie mindestens einen Host in der Cloud, den Namen der Datenbank sowie Benutzer-ID und Kennwort für die Datenbank angeben.

## Kontext und Bemerkungen

Um sicherzustellen, dass Sie Verbindungen mit der Cloud herstellen können, wird empfohlen, dass Sie die Hosts und Ports für die Cloud-Partner und den Cloud-Arbiträr angeben.

### Vorsicht

Die Adresscachedatei des Cloud-Servers ist `saredir.ini`. Diese Datei dürfen Sie weder ändern noch löschen.

## Schritte

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Verbindung mit einer laufenden Datenbank in einer Cloud herstellen**, um eine Verbindung mit einer Datenbank herzustellen, die auf einem anderen Computer läuft.

- e. Geben Sie im Feld **Host** die Hostnamen für den Cloud-Arbiter und einen der Cloud-Partner ein.
  - f. Geben Sie im Feld **Port** den TCP/IP-Port ein, an dem der Cloud-Arbiter läuft, gefolgt von dem Port, an dem der Cloud-Partner läuft.
  - g. Geben Sie in das Feld **Datenbankname** den Namen der Datenbank ein. Geben Sie zum Beispiel Folgendes ein: **Tenant1**.
3. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.
  4. Klicken Sie auf **Verbinden**.

### Ergebnisse

Das Administrationstool stellt eine Verbindung mit der Datenbank her.

## Datenbanken auf anderen Computern starten und Verbindungen herstellen (Administrationstools)

Obwohl dies nicht empfohlen wird, können Sie das Fenster **Verbinden** verwenden, um eine Datenbank auf einem anderen Computer zu starten und eine Verbindung mit ihr herzustellen.

### Voraussetzungen

Wenn noch kein Netzwerk-Datenbankserver ausgeführt wird, starten Sie einen auf einem anderen Computer. Führen Sie beispielsweise folgenden Befehl aus, um einen Datenbankserver zu starten:

```
dbsrv16 -n myserver -gd all
```

Die `-gd all`-Option ist nicht empfehlenswert, weil sie es allen Benutzern ermöglicht, eine Datenbank auf einem Server zu starten. Diese Option ist für das folgende Szenario erforderlich. Wenn Ihre Datenbankseite größer ist als der Standardwert von 4096, geben Sie die `-gp`-Option an.

### Aufgabe

1. Öffnen Sie in Sybase Central oder Interactive SQL das Fenster **Verbinden**.
2. Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Datenbank herzustellen:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. In das Feld **Benutzer-ID** geben Sie einen Benutzernamen ein. Geben Sie zum Beispiel Folgendes ein: **DBA**.
  - c. In das Feld **Kennwort** geben Sie ein Kennwort für den Benutzer ein. Geben Sie zum Beispiel Folgendes ein: **sql**.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Eine Datenbank auf einem anderen Computer starten und eine Verbindung herstellen**.
  - e. Im Feld **Datenbankdatei** geben Sie den Pfad und die Erweiterung der Datenbankdatei relativ zum Datenbankserver ein.

Geben Sie zum Beispiel Folgendes ein: **C:\Users\Public\Documents\SQL Anywhere 16\Samples\demo.db.**

- f. Um einen Datenbanknamen zu erstellen, der vom Dateinamen für nachfolgende Verbindungen abweicht, geben Sie einen Namen in das Feld **Datenbankname** ein. Geben Sie keinen Dateipfad und keine Erweiterung an.

Geben Sie zum Beispiel Folgendes ein: **mydemo.**

- g. Im Feld **Servername** geben Sie einen Namen für den Server ein.

Verwenden Sie für dieses Beispiel den oben angegebenen Servernamen **myserver**.

Da auf dem Hostcomputer möglicherweise mehrere Datenbankserver laufen, wird empfohlen, dass Sie immer den Namen des Datenbankservers angeben.

- h. In das Feld **Host** geben Sie den Hostnamen des Computers ein, auf dem der Datenbankserver läuft.

3. Optional: Um eine Kopie der mit diesem Fenster erstellten Verbindungszeichenfolge zu erhalten, klicken Sie auf **Extras » Verbindungszeichenfolge in Zwischenablage kopieren**.

4. Klicken Sie auf **Verbinden**.

## Ergebnisse

Das Administrationstool stellt eine Verbindung mit der Datenbank her.

## Siehe auch

- „Praktische Einführung: Verbindung mit der Beispieldatenbank herstellen“ auf Seite 1
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „Datenbankserveroption -gd “ auf Seite 240
- „Datenbankserveroption -gp “ auf Seite 249
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14

# Datenbanken auf anderen Computern starten und Verbindungen herstellen (Befehlszeile)

Obwohl dies nicht empfohlen wird, können Sie eine Datenbank auf einem anderen Computer starten und eine Verbindung mit ihr herstellen.

## Voraussetzungen

Wenn noch kein Netzwerk-Datenbankserver ausgeführt wird, starten Sie einen auf einem anderen Computer. Führen Sie beispielsweise folgenden Befehl aus, um einen Datenbankserver zu starten:

```
dbsrv16 -n myservers -gd all
```

Die `-gd all`-Option ist nicht empfehlenswert, weil sie es allen Benutzern ermöglicht, eine Datenbank auf einem Server zu starten. Diese Option ist für das folgende Szenario erforderlich. Wenn Ihre Datenbankseite größer ist als der Standardwert von 4096, geben Sie die `-gp`-Option an.

### Aufgabe

- Führen Sie den folgenden Befehl aus (wobei Sie my\_host durch den Hostnamen des Computers ersetzen müssen, der auf dem Netzwerkserver läuft):

```
dbisql -c "Host=my_host;Server=myserver;DBF=C:\Users\Public\Documents\SQL  
Anywhere 16\Samples\demo.db;UID=DBA;PWD=sql "
```

Da auf dem Hostcomputer möglicherweise mehrere Datenbankserver laufen, wird empfohlen, dass Sie immer die Verbindungsoption für den Datenbankservernamen angeben (ServerName=Servername).

### Ergebnisse

Die Anwendung stellt eine Verbindung mit der Datenbank her.

### Siehe auch

- „Datenbankserveroption -gd “ auf Seite 240
- „Datenbankserveroption -gp “ auf Seite 249

## Verbindungen mit eingebetteten Datenbanken

Eine **eingebettete Datenbank** ist für die Verwendung durch eine bestimmte Anwendung vorgesehen, läuft auf demselben Computer wie die Anwendung und ist vor dem Benutzer im Allgemeinen verborgen.

Falls eine Anwendung eine eingebettete Datenbank verwendet, läuft der Personal Server in der Regel nicht, wenn sich die Anwendung verbindet. Die Datenbank wird mit einer Verbindungszeichenfolge und durch Angeben der Datenbankdatei im DatabaseFile-Parameter (DBF) der Verbindungszeichenfolge gestartet.

Um die Abfrageperformance für automatisch gestartete Datenbanken zu erhöhen, starten Sie die Datenbank sobald wie möglich, auch wenn sich noch keine Benutzer mit ihr verbinden. Damit kann sich der Cache vorwärmen, bis Abfragen in der Datenbank durchgeführt werden.

### ServerName-Verbindungsparameter (Server) verwenden

Wenn Sie mit einer eingebetteten Datenbank arbeiten, verwenden Sie den Verbindungsparameter ServerName (Server). Dies gewährleistet, dass sich die Datenbank mit dem korrekten Datenbankserver verbindet, falls es auf demselben Computer andere Anwendungen gibt, die SQL Anywhere-Datenbankserver ausführen.

Wenn der Datenbankserver einen alternativen Servernamen hat, kann die Clientanwendung nur den alternativen Servernamen verwenden, um sich mit der Datenbank zu verbinden, die den alternativen Servernamen angegeben hat. Sie können den alternativen Servernamen nicht verwenden, um eine Verbindung mit anderen auf diesem Datenbankserver laufenden Datenbanken herzustellen.

### DatabaseFile-Verbindungsparameter (DBF) verwenden

Mithilfe des DBF-Verbindungsparameters wird die zu verwendende Datenbankdatei angegeben. Die Datenbankdatei wird automatisch auf dem Datenbankserver gestartet, der zum ServerName-Verbindungsparameter passt (wenn sie noch nicht läuft), und ein Datenbankserver wird automatisch gestartet (wenn er noch nicht läuft).

Die Datenbank wird automatisch gestoppt, wenn keine Verbindungen mehr zur Datenbank bestehen (normalerweise wenn die Anwendung, die die Verbindung hergestellt hat, die Verbindung trennt). Wenn der Datenbankserver automatisch gestartet wurde, wird der Datenbankserver gestoppt, sobald die Datenbank heruntergefahren wird.

Im folgenden Beispiel wird die Beispieldatenbank als eingebettete Datenbank gestartet:

```
"DBF=%SQLANYAMP16%\demo.db"
```

### **StartLine-Verbindungsparameter [START] verwenden**

Die folgenden Verbindungsparameter zeigen, wie Sie das Starten der Beispieldatenbank als eingebettete Datenbank definieren können. Der StartLine-Verbindungsparameter ist nützlich, wenn Sie Datenbankserveroptionen verwenden möchten. Zum Beispiel:

```
"START=dbeng16 -xd -c 8M;DBF=%SQLANYAMP16%\demo.db"
```

Wenn die Option -xd angegeben wird, verhindert sie, dass der Datenbankserver der Standarddatenbankserver wird.

Um Benutzer daran zu hindern, die eingebettete Datenbank zu starten oder zu stoppen oder andere Datenbanken auf dem Datenbankserver zu starten, setzen Sie die Option -gd auf **none**.

Es gibt viele Verbindungsparameter, die den Start eines Datenbankservers beeinflussen. Es wird empfohlen, dass Sie die folgenden Verbindungsparameter benutzen und nicht die entsprechenden Serveroptionen im StartLine-Verbindungsparameter (START) übergeben:

- ServerName (Server)
- DatabaseFile (DBF)
- DatabaseSwitches (DBS)
- DatabaseName (DBN)

### **Elevate-Verbindungsparameter verwenden**

Wenn Sie in Ihrer Verbindungszeichenfolge die Einstellung ELEVATE=YES angeben, können Clientprozesse, deren Rechte nicht erhöht wurden, Server mit erhöhten Rechten automatisch starten. Dies ist unter Windows Vista oder höher möglicherweise notwendig, wenn für den Zugriff auf die Datenbankdatei Administrationsrechte erforderlich sind. Dieser Parameter wird ignoriert, wenn der Datenbankserver nicht automatisch gestartet wird.

### **Beispiele**

Nachstehend finden Sie ein Beispiel für eine vollständige Verbindungszeichenfolge einer Anwendung, die eine eingebettete Datenbank verwendet:

```
"UID=DBA;PWD=sql;DBF=c:\myapp\mydb.db;ServerName=myapp;START=dbeng16 -c 12M -xd"
```

### Siehe auch

- „Cachevorwärmung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Verbindungsparameter DatabaseFile (DBF)“ auf Seite 351
- „Verbindungsparameter ServerName (Server)“ auf Seite 383
- „Verbindungsparameter StartLine (START)“ auf Seite 385
- „Datenbankoption -sn “ auf Seite 332
- „Datenbankserveroption -gd “ auf Seite 240
- „Datenbankserveroption -xd “ auf Seite 307
- „Verbindungsparameter Elevate“ auf Seite 358
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „Verbindungs-IDs“ auf Seite 30

## SQL Anywhere-Dienstprogrammverbindungen

Alle Dienstprogramme für SQL Anywhere-Datenbanken verwenden Embedded SQL zur Kommunikation mit dem Datenbankserver.

### Wie Datenbank-Dienstprogramme Werte für Verbindungsparameter erhalten

Viele Administrationsdienstprogramme beziehen die Werte der Verbindungsparameter auf folgende Weise:

1. Sie verwenden in der Befehlszeile angegebene Werte. Beispiel: Der folgende Befehl startet die Sicherung der Standarddatenbank auf dem Standardserver mit der Benutzer-ID DBA und dem Kennwort sql:

```
dbbackup -c "UID=DBA;PWD=sql" c:\backup
```

2. Sie verwenden die Einstellungen der SQLCONNECT-Umgebungsvariablen, falls Werte fehlen. SQL Anywhere setzt diese Variable nicht automatisch.

### Siehe auch

- „Dienstprogramme für die Datenbankadministration“ auf Seite 882
- „SQLCONNECT-Umgebungsvariable“ auf Seite 479

## Verbindungs-IDs

Eine Datenbankserververbindung bildet einen Kanal, durch den der komplette Datenfluss zwischen Clientanwendung und Datenbank fließt. Clientanwendungen können mit dem Datenbankserver erst interagieren, wenn eine Verbindung hergestellt wurde. Bei Verbindungen mit einem Datenbankserver bestimmen die Privilegien eines Benutzers, welche Aktionen der Benutzer auf dem Datenbankserver ausführen darf.

Wenn ein Benutzer eine Verbindung mit einer Datenbank herstellt, ordnet der Datenbankserver der Verbindung dieses Benutzers eine eindeutige **Verbindungs-ID** zu. Für jede neue Verbindung mit dem Datenbankserver erhöht der Server den Wert der Verbindungs-ID um eins. Diese Verbindungs-IDs werden im Meldungslog des Datenbankservers protokolliert, das informative Meldungen, Fehler,

Warnungen und Meldungen von der MESSAGE-Anweisung protokolliert. Die Verbindungs-ID kann zur Durchführung folgender Aufgaben verwendet werden:

- Filtern von Informationen aus dem Anforderungslog
- Ermitteln der Verbindung, welche eine Sperre in der Datenbank gesetzt hat
- Protokollieren der Gesamtzahl der Verbindungen zu einem Datenbankserver seit seinem Start und der Reihenfolge, in der diese Verbindungen hergestellt wurden

Sie können die Funktion CONNECTION\_PROPERTY verwenden, um die Verbindungs-ID eines Benutzers durch Abfragen der Number-Verbindungseigenschaft zu erhalten.

#### Siehe auch

- [Number-Verbindungseigenschaft auf Seite 728](#)
- [„Protokollieren von Datenbankserver-Aktionen“ auf Seite 163](#)
- [„Anforderungsprotokollierung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„Funktionsweise von Sperren“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„Datenbankserveroption -z “ auf Seite 312](#)

## Verbindungsparameter und Verbindungszeichenfolgen

Wenn eine Verbindung mit einer Datenbank hergestellt wird, benutzt die Clientanwendung eine Gruppe von **Verbindungsparametern** zur Definition der Verbindung. Verbindungsparameter geben bestimmte Informationen an, etwa den Namen des Datenbankservers, den Namen der Datenbank sowie die Benutzer-ID.

Jeder Verbindungsparameter gibt ein Schlüsselwort-Wert-Paar in der Form *Parameter=Wert* an. Das nachstehende Beispiel zeigt den Kennwort-Verbindungsparameter für das Standardkennwort:

```
PWD=sql
```

### Als Verbindungszeichenfolge übergebene Verbindungsparameter

Verbindungsparameter werden in **Verbindungszeichenfolgen** zusammengefasst. In einer Verbindungszeichenfolge werden die einzelnen Verbindungsparameter durch ein Semikolon getrennt:

```
parameter1=value1;parameter2=value2;...
```

Zum Beispiel:

```
UID=DBA;PWD=sql;Host=myhost;DatabaseName=mydemo;ServerName=myserver
```

Im Allgemeinen entspricht die von einer Anwendung erstellte und an die Schnittstellenbibliothek übergebene Verbindungszeichenfolge nicht direkt der Form der Eingabe durch den Benutzer. Der Benutzer kann mehrere Felder in einem Fenster ausfüllen, oder die Anwendung liest die Verbindungsdaten aus einer Initialisierungsdatei.

Bei vielen Dienstprogrammen von SQL Anywhere kann mit der Option -c eine Verbindungszeichenfolge angegeben werden, die dann ohne Änderung an die Schnittstellenbibliothek übergeben wird. Das Folgende ist z.B. eine typische Befehlszeile des Sicherungsdienstprogramms (dbbackup):

```
dbbackup -c "HOST=myhost-pc;DBN=mydemo;UID=DBA;PWD=sql;ServerName=myserver"
SQLAnybackup
```

### Darstellung von Verbindungszeichenfolgen in der Dokumentation

In der SQL Anywhere-Dokumentation können Beispiele für Verbindungszeichenfolgen in der folgenden Form dargestellt werden:

```
parameter1=value1
parameter2=value2
...
```

Dieses Format entspricht der nachstehenden Verbindungszeichenfolge:

```
parameter1=value1;parameter2=value2
```

In Ihrer Anwendung *müssen* Sie eine Verbindungszeichenfolge mit durch Semikola getrennten Parametereinstellungen eingeben.

### Siehe auch

- „Häufig verwendete Verbindungsszenarien“ auf Seite 32
- „Syntaxregeln für Verbindungsparameter“ auf Seite 36
- „Verbindungsparameter“ auf Seite 337
- „Netzwerkprotokolloptionen“ auf Seite 388
- „Zeichensatzkonvertierung“ auf Seite 502

## Häufig verwendete Verbindungsszenarien

Die für das Verbinden mit einer Datenbank erforderlichen Verbindungsparameter können variieren, je nachdem, ob mehrere Datenbankserver auf demselben Computer laufen, ob mehrere Datenbanken auf demselben Datenbankserver laufen und ob die Clientanwendung auf demselben Computer wie der Datenbankserver ausgeführt wird.

#### Hinweis

Auf einem einzelnen Computer können mehrere Datenbankserver gleichzeitig laufen. Aus diesem Grund wird empfohlen, dass Sie immer den Datenbankservernamen (`ServerName=Servername`) angeben, wenn Sie sich bei einem Datenbankserver authentifizieren.

Auf jedem Datenbankserver können mehrere Datenbanken gleichzeitig laufen. Aus diesem Grund wird empfohlen, dass Sie immer den Datenbanknamen (`DatabaseName=Datenbankname`) angeben, wenn Sie sich bei einem Datenbankserver authentifizieren.

Die folgenden Tabellen enthalten mehrere häufige Verbindungsszenarien und die in den einzelnen Fällen erforderlichen Clientverbindungsparameter. Durch die Kombinationen dieser Verbindungsparameter können Sie die Datenbank, zu der eine Verbindung hergestellt werden soll, korrekt identifizieren. Zusätzlich zu den unten aufgelisteten Verbindungsparametern unterstützt SQL Anywhere viele weitere Verbindungsparameter für weniger häufige Verbindungsszenarien.

### Shared Memory-Verbindungen mit lokalen Servern

Ein X in der folgenden Tabelle zeigt an, dass der betreffende Verbindungsparameter für das oben in der Spalte angegebene Szenario erforderlich ist.

Verbindungsparameter	1 Server als Host für 1 Datenbank	1 Server als Host für viele Datenbanken	Viele Server als Hosts für jeweils 1 Datenbank	Viele Server als Hosts für jeweils viele Datenbanken
UserID (UID)	X	X	X	X
Password (PWD)	X	X	X	X
DatabaseName (DBN)		X		X
ServerName(Server)	1	1	X	X
Host <sup>2</sup>	1	1		

<sup>1</sup> Geben Sie den Servernamen (ServerName=*Servername*) an, wenn der Server mit der Option -xd ausgeführt wird.

<sup>2</sup> Bei Verwendung des Host-Verbindungsparameters (Host=*Hostname:Portnummer*) wird versucht, die Verbindung über TCP/IP statt über Shared Memory herzustellen. Diese Option ist für den Personal Datenbankserver nur dann geeignet, wenn das TCP/IP-Kommunikationsprotokoll auf dem Personal Datenbankserver mit der Option -x aktiviert wurde. Außerdem müssen Sie den Hostnamen **localhost** verwenden, wenn Sie eine Verbindung mit einem Personal Datenbankserver über TCP/IP herstellen.

### Verbindungen mit Netzwerkservern

Ein X in der folgenden Tabelle zeigt an, dass der betreffende Verbindungsparameter für das oben in der Spalte angegebene Szenario erforderlich ist.

Verbindungsparameter	1 Server als Host für 1 Datenbank	1 Server als Host für viele Datenbanken	Viele Server als Hosts für jeweils 1 Datenbank	Viele Server als Hosts für jeweils viele Datenbanken
UserID (UID)	X	X	X	X
Password (PWD)	X	X	X	X
DatabaseName (DBN)		X		X
ServerName(Server)	<sup>3</sup>	<sup>3</sup>	X	X
Host	X <sup>3</sup>	X <sup>3</sup>	X	X

<sup>3</sup> Geben Sie die Portnummer (Host=*Hostname:Portnummer*) oder den Servernamen (ServerName=*Servername*) an, wenn der Server nicht am standardmäßigen TCP/IP-Port (2638) läuft.

Wenn der Datenbankserver mit der nicht standardmäßigen Portnummer unter Mac OS X läuft oder wenn er mit der Option -sb gestartet wurde, müssen Sie die Portnummer (`Host=Hostname:Portnummer`) angeben, um die Verbindung herzustellen.

### Siehe auch

- „Verbindungsparameter Userid (UID)“
- „Verbindungsparameter Password (PWD)“
- „Verbindungsparameter DatabaseName (DBN)“
- „Verbindungsparameter ServerName (Server)“
- „Host-Verbindungsparameter“
- „Verbindungsparameter“ auf Seite 337
- „Datenbankserveroption -xd“ auf Seite 307

### Beispiele

**Nur ein Datenbankserver mit nur einer laufenden Datenbank auf demselben Computer wie die Clientanwendung**

```
dbisql -c "UID=DBA;PWD=sql"
```

**Nur ein Datenbankserver mit mehreren laufenden Datenbanken auf demselben Computer wie die Clientanwendung**

```
dbisql -c "UID=DBA;PWD=sql;DBN=demo"
```

**Mehrere Datenbankserver, jeder mit einer laufenden Datenbank, auf demselben Computer wie die Clientanwendung**

```
dbisql -c "UID=DBA;PWD=sql;ServerName=demo16"
```

**Mehrere Datenbankserver, jeder mit mehreren laufenden Datenbanken, auf demselben Computer wie die Clientanwendung**

```
dbisql -c "UID=DBA;PWD=sql;ServerName=demo16;DBN=demo"
```

**Nur ein Datenbankserver mit nur einer laufenden Datenbank auf einem anderen Computer als die Clientanwendung, wobei der Computer, auf dem der Datenbankserver läuft, den Namen myhost-pc hat**

```
dbisql -c "UID=DBA;PWD=sql;Host=myhost-pc"
```

**Mehrere Datenbankserver, jeder mit mehreren laufenden Datenbanken, auf einem anderen Computer als die Clientanwendung, wobei der Computer, auf dem der Datenbankserver läuft, den Namen myhost-pc hat**

```
dbisql -c "UID=DBA;PWD=sql;Host=myhost-pc;ServerName=demo16;DBN=demo"
```

**Eine Cloud mit mehreren Hosts, auf denen mehrere Datenbankserver laufen, jeder mit mehreren Datenbanken**

```
dbisql -c  
"UID=DBA;PWD=sql;Host=74.125.163.214:40200,74.125.167.240:9038;DBN=demo"
```

**Sie wissen nicht, ob der Datenbankserver bzw. die Datenbank läuft, und möchten sie auf demselben Computer starten wie die Clientanwendung, damit Sie sich mit der Datenbank verbinden können**

```
dbisql -c "UID=DBA;PWD=sql;ServerName=demo16;DBF=%SQLANYAMP16%\demo.db"
```

## Standard-Verbindungsparameter

### Hinweis

- Sie können das Standardverhalten verwenden, um eine Verbindung ohne Angabe bestimmter Verbindungsparameter herzustellen. Wenn Sie allerdings das Standardverhalten in einer Produktionsumgebung verwenden, kann dies größere Probleme verursachen, wenn die Anwendung mit anderen SQL Anywhere-Anwendungen installiert wird. Wenn Sie Verbindungsprobleme haben, besteht die Lösung meist darin, dass Sie explizite Werte angeben und nicht die Standardwerte verwenden.
- Es wird empfohlen, dass Sie immer den Servernamen unter Verwendung des ServerName-Verbindungsparameters angeben, vor allem, wenn Sie mit einem eingebetteten SQL Anywhere-Server arbeiten. Siehe „[Verbindungsparameter ServerName \(Server\)](#)“ auf Seite 383.

Die folgende Liste zeigt einige allgemeine Verbindungsszenarien und die im entsprechenden Fall erforderlichen Standard-Client-Verbindungsparameter.

### Keine Standardwerte für einen lokalen Server (empfohlene Methode)

Mit der folgenden Verbindungszeichenfolge verbinden Sie sich mit einem benannten lokalen Server unter Verwendung einer benannten Datenbank:

```
ServerName=server-name;DBN=db-name;UID=user-id;PWD=password
```

### Standard-Datenbankserver und Standarddatenbank

Verwenden Sie die Standardparameter, um eine Verbindung herstellen, wenn Sie sicher sind, dass nur ein Datenbankserver auf dem lokalen Computer läuft:

```
UID=user-id;PWD=password
```

### Standard-Datenbankserver

Wenn Sie sicher sind, dass nur ein Datenbankserver auf dem lokalen Computer läuft, verwenden Sie die Standard-Servereinstellungen und geben die Datenbank an, mit der Sie eine Verbindung herstellen wollen:

```
DBN=db-name;UID=user-id;PWD=password
```

### Standarddatenbank

Wenn mehr als ein Server auf dem lokalen Computer läuft, geben Sie an, mit welchem Server Sie die Verbindung herstellen wollen. Der Datenbankname muss nicht angegeben werden, wenn auf dem Datenbankserver nur eine Datenbank läuft. Mit der folgenden Verbindungszeichenfolge wird die Verbindung mit einem benannten Server und der Standarddatenbank eingerichtet:

```
ServerName=server-name;UID=user-id;PWD=password
```

### Standard-Datenbankserver auf einem anderen Computer

Die folgende Verbindungszeichenfolge stellt eine Verbindung mit der angegebenen Datenbank her, die auf dem Standard-Datenbankserver auf einem Netzwerkcomputer läuft. Bei dieser Verbindungszeichenfolge wird vorausgesetzt, dass der Datenbankserver am standardmäßigen TCP/IP-Port 2638 läuft.

```
Host=host-name;DBN=db-name;UID=user-id;PWD=password
```

Wenn der Datenbankserver nicht den Standard-TCP/IP-Port (2638) verwendet, müssen Sie den Datenbankservernamen (ServerName=*Servername*) oder die Portnummer (Host = *Hostname:Portnummer*) angeben. Wenn Sie den Servernamen angeben, können Sie möglicherweise keine Verbindung herstellen, falls der Server unter Mac OS X läuft oder der Datenbankserver mit der Option -sb gestartet wurde. In diesen Fällen müssen Sie die Portnummer angeben (Host=*Hostname:Portnummer*), um die Verbindung herzustellen.

## Syntaxregeln für Verbindungsparameter

- **Verbindungszeichenfolgen mit Leerstellen** Wenn Sie eine Verbindungszeichenfolge in der Befehlszeile angeben, müssen Sie die gesamte Verbindungszeichenfolge in Anführungszeichen setzen, wenn einer der Verbindungsparameterwerte Leerstellen enthält.
- **Boolesche Werte** Boolesche Argumente (TRUE oder FALSE) sind YES, ON, 1, TRUE, Y oder T bei TRUE, bzw. NO, OFF, 0, FALSE, N oder F bei FALSE.
- **Groß-/Kleinschreibung** Bei Verbindungsparameternamen spielt die Groß-/Kleinschreibung keine Rolle, auch wenn dies bei ihren Werte möglicherweise der Fall ist (z.B. Dateinamen unter Unix).
- **Einschränkungen des Zeichensatzes** Es wird empfohlen, dass der Name des Datenbankservers (angegeben durch den ServerName-Verbindungsparameter) mit Zeichen aus dem ASCII-Zeichensatz im Bereich von 32 bis 126 gebildet wird. Diese Beschränkung gilt nicht für andere Verbindungsparameterwerte.
- **Priorität**

#### Vorsicht

Geben Sie keinen Parameter mehr als einmal in der Verbindungszeichenfolge an. Wenn Sie einen Parameter mehrmals angeben, werden die Ergebnisse nicht garantiert und können inkonsistent sein. Auch das Verhalten kann sich in einer zukünftigen Version der Software ändern.

Folgende Regeln gelten für die Priorität von Verbindungsparametern:

- Die Einträge in einer Verbindungszeichenfolge werden von links nach rechts gelesen. Wenn derselbe Verbindungsparameter mehr als einmal angegeben ist, wird der in der Zeichenfolge zuletzt genannte verwendet. ODBC- und OLE DB-Clientanwendungen (mit Ausnahme von Sybase Central, Interactive SQL und dem SQL Anywhere-Konsolendienstprogramm) stellen eine Ausnahme dar: Wenn derselbe Parameter mehr als einmal angegeben ist, wird die erste Zeichenfolge verwendet.

- In der genannten Reihenfolge übernimmt die Interface-Bibliothek Verbindungsparameter aus den folgenden Quellen:

- **Verbindungszeichenfolge** Sie können Parameter in der Verbindungszeichenfolge explizit übergeben.
- **SQLCONNECT-Umgebungsvariable** Die Umgebungsvariable SQLCONNECT kann Verbindungsparameter speichern.
- **Datenquellen** ODBC-Datenquellen können Verbindungsparameter speichern.

Wenn eine Verbindungszeichenfolge und eine ODBC-Datenquelle beide denselben Verbindungsparameter angeben, wird der Wert aus der Zeichenfolge für die Verbindung verwendet und der Wert aus der Datenquelle wird ignoriert.

Nehmen Sie beispielsweise an, auf dem Datenbankserver demo16 laufen die Datenbanken demo und demo2. Der folgende Befehl erstellt eine Datenquelle für die Datenbank "demo" erstellt.

```
dbdsn -w demodsn -c "ServerName=demo16;Host=myhost-pc;DBN=demo" -y
```

Der DBN-Wert-(DBN=demo2) der Verbindungszeichenfolge hat eine höhere Priorität als der DBN-Wert der Datenquelle.

```
dbping -d -c "UID=DBA;PWD=sql;DBN=demo2;DSN=demodsn"
```

Die Verbindungsparameter für die Verbindung sind:

```
UID=DBA;PWD=sql;DBN=demo2;ServerName=demo16;Host=myhost-pc
```

- **Syntaktische Analyse von Verbindungszeichenfolgen** Wenn ein Problem bei der syntaktischen Analyse der Verbindungszeichenfolge auftritt, wird ein Fehler generiert, der anzeigt, welcher Verbindungsparameter das Problem verursachte.
- **Leere Verbindungsparameter** Verbindungsparameter, die mit leeren Werten angegeben werden, werden wie eine Zeichenfolge mit Nulllänge behandelt.

**Siehe auch**

- „Verbindungsparameter“ auf Seite 337
- „Verbindungszeichenfolgen und Zeichensätze“ auf Seite 503

## Desktop-Anwendungen und Windows Mobile-Datenbanken

Sie können über Anwendungen, die auf einem Desktopcomputer laufen, eine Verbindung mit einem Datenbankserver herstellen, der auf einem Windows Mobile-Gerät läuft. Für die Verbindung wird TCP/IP über die Microsoft ActiveSync-Verknüpfung (Windows Mobile-Gerätecenter) zwischen dem PC und dem Windows Mobile-Gerät verwendet.

**Siehe auch**

- „Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden“ auf Seite 434
- „ODBC-Datenquelle für eine Verbindung mit Ihrem Windows Mobile-Gerät erstellen“ auf Seite 435
- „IP-Adresse Ihres Windows Mobile-Geräts ermitteln“ auf Seite 438

## ODBC-Datenquellen

Microsoft **Open Database Connectivity (ODBC)** ist eine Standard-Programmierschnittstelle für die Verbindung von Clientanwendungen mit Datenbankmanagementsystemen unter Windows.

Viele Clientanwendungen, darunter auch Entwicklungssysteme für Anwendungen, benutzen eine ODBC-Schnittstelle für den Zugriff auf SQL Anywhere. Bei der Verbindung mit einer Datenbank verwenden ODBC-Anwendungen normalerweise ODBC-Datenquellen. Eine ODBC-Datenquelle besteht aus einer Reihe von Verbindungsparametern, die in der Registrierung oder in einer Datei gespeichert sind.

**Vorsicht**

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht-verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen. Siehe [Keine Kennwörter in ODBC-Datenquellen einschließen auf Seite 1411](#).

Der SQL Anywhere ODBC-Treiber hat den Namen *dbodbc16.dll* und befindet sich im Verzeichnis *%SQLANY16%\bin32*.

Mithilfe von ODBC-Datenquellen können Sie von den folgenden Anwendungen eine Verbindung zu SQL Anywhere herstellen:

- Sybase Central, Interactive SQL und das SQL Anywhere-Konsolendienstprogramm.
- Alle SQL Anywhere-Dienstprogramme.
- SAP Sybase PowerDesigner Physical Data Model.
- Sämtliche Umgebungen zur Anwendungsentwicklung, die ODBC unterstützen, z.B. Microsoft Visual Basic, Sybase PowerBuilder und Embarcadero Delphi.
- SQL Anywhere-Clientanwendungen unter Unix. Unter Unix wird die Datenquelle als Datei gespeichert.

Sie können ODBC-Datenquellen nicht mit Sybase Open Client oder jConnect verwenden.

**Siehe auch**

- „ODBC-Übereinstimmung“ [[SQL Anywhere Server - Programmierung](#)]

## SQL Anywhere-Verbindungsparameter in einer ODBC-Datenquelle

Sie können eine ODBC-Datenquelle zur Verbindung mit einer ODBC-Datenbank verwenden. Die ODBC-Datenquelle befindet sich auf dem Clientcomputer.

Die ODBC-Datenquelle enthält eine Reihe von Verbindungsparametern. Sie können Gruppen von SQL Anywhere-Verbindungsparametern als ODBC-Datenquellen in der Windows-Registrierung oder als Dateien speichern.

Bei SQL Anywhere geht die Verwendung von ODBC-Datenquellen über die von Windows-Anwendungen hinaus, welche die ODBC-Schnittstelle nutzen:

- SQL Anywhere-Clientanwendungen unter Unix und Windows können ODBC-Datenquellen verwenden.
- ODBC-Datenquellen können von allen SQL Anywhere-Clientschnittstellen außer jConnect und Sybase Open Client verwendet werden. Die Datenquelle wird unter Unix oder Windows Mobile in einer Datei gespeichert.

Wenn Sie eine Datenquelle eingerichtet haben, kann die Verbindungszeichenfolge den Namen der Datenquelle aufrufen, die verwendet werden soll:

- **Datenquellennamen** Verwenden Sie den DataSourceName-Verbindungsparameter (DSN), um eine Datenquelle in der Windows-Registrierung zu referenzieren:

`DSN=my-data-source`

- **Dateidatenquelle** Verwenden Sie den FileDataSourceName-Verbindungsparameter (FILEDSN), wenn Sie eine Datenquelle in einer Datei referenzieren wollen:

`FileDSN=mysource.dsn`

#### Hinweis

Wenn eine Verbindungszeichenfolge und eine ODBC-Datenquelle beide denselben Verbindungsparameter angeben, wird der Wert aus der Zeichenfolge verwendet und der Wert aus der Datenquelle ignoriert. Siehe „Syntaxregeln für Verbindungsparameter“ auf Seite 36.

#### Siehe auch

- „Dateidatenquellen unter Windows“ auf Seite 46
- „Verbindungsparameter“ auf Seite 337
- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20

## ODBC-Datenquellen erstellen (Administrationtools)

Um schnell eine ODBC-Datenquelle zu erstellen, verwenden Sie das Fenster **Verbinden** in den Administrationtools.

#### Voraussetzungen

Auf dem lokalen Computer läuft eine Datenbank.

#### Aufgabe

1. Öffnen Sie das Fenster **Verbinden**.

2. Wenn Sie Interactive SQL verwenden, klicken Sie ggf. auf **Datenbanktyp ändern** und anschließend auf **SQL Anywhere**.
3. Geben Sie eine **Benutzer-ID** ein.
4. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**, um eine Verbindung mit einer Datenbank herzustellen, die auf Ihrem Computer läuft.
5. Falls gewünscht, geben Sie einen **Servernamen** an.
6. Falls gewünscht, geben Sie einen **Datenbanknamen** an.
7. Klicken Sie auf **Extras » Als ODBC-Datenquelle speichern**.
8. Im Feld **Geben Sie den Namen für diese neue Datenquelle ein** geben Sie einen Namen für die Datenquelle ein.
9. Geben Sie in der Liste **Wählen Sie den Datenquellentyp aus** an, ob die Datenquelle nur für den aktuellen Benutzer oder für alle Benutzer (einschließlich Windows-Dienste) verfügbar sein soll.
10. (Optional) Klicken Sie auf **Benutzer-ID und Kennwort in der Datenquelle speichern**.

### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

11. (Optional) Wenn Sie mit der 64-Bit-Version der Administrationstools arbeiten und auch den 32-Bit-ODBC-Treiber installiert haben, können Sie auf **32-Bit- und 64-Bit-Datenquellen erstellen** klicken.
  - Wenn Sie eine Systemdatenquelle erstellen, wählen Sie diese Option, um zwei Systemdatenquellen einzurichten: eine Datenquelle, die von 32-Bit-Anwendungen verwendet werden kann, und eine Datenquelle, die von 64-Bit-Anwendungen verwendet werden kann.
  - Wenn Sie eine Benutzerdatenquelle erstellen, wird diese Option ignoriert.
12. Klicken Sie auf **Speichern** und bearbeiten Sie die Eingabeaufforderungen, um die Datenquelle(n) zu erstellen.

## Ergebnisse

Die ODBC-Datenquelle wird erstellt.

## Siehe auch

- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20
- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- Keine Kennwörter in ODBC-Datenquellen einschließen auf Seite 1411

## Erstellen einer ODBC-Datenquelle (ODBC-Datenquellen-Administrator)

Sie können den ODBC-Datenquellen-Administrator verwenden, um eine ODBC-Datenquelle zu erstellen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Unter Windows sind Systemdatenquellen für alle Benutzer des Computersystems und für Windows-Dienste verfügbar. Benutzerdatenquellen sind nur für den Benutzer verfügbar, für den sie erstellt wurden.

#### Hinweis

**Systemdatenquellen unter 64-Bit-Windows erstellen** Systemdatenquellen sind für alle Benutzer des Computersystems und für Windows-Dienste verfügbar. 64-Bit-Versionen von Windows verwalten in der Windows-Registrierung zwei Gruppen von Systemdatenquellen: eine für 64-Bit-Clientanwendungen und eine für 32-Bit-Clientanwendungen. Um eine Systemdatenquelle zu erstellen, die für 32-Bit-Anwendungen zugänglich ist, müssen Sie die 32-Bit-Version des ODBC-Datenquellen-Administrators (im Ordner `%windir%\syswow64`) ausführen. Um Verbindungsprobleme zu vermeiden, wird empfohlen, dass Sie sowohl 64-Bit- als auch 32-Bit-Systemdatenquellen erstellen und dafür sorgen, dass diese identisch konfiguriert sind.

**Benutzerdatenquellen unter 64-Bit-Windows erstellen** Definitionen von Benutzerdatenquellen werden in der Registrierung im Abschnitt für die Einstellungen des derzeit beim System angemeldeten Benutzers gespeichert. 64-Bit-Versionen von Windows verwalten in der Windows-Registrierung eine Gruppe von Benutzerdatenquellen für jeden Benutzer des Computers. Sie können entweder die 32-Bit- oder die 64-Bit-Version des ODBC-Datenquellen-Administrators verwenden, um eine Benutzerdatenquelle zu erstellen. Diese Datenquelle kann von 64-Bit- und 32-Bit-Clientanwendungen verwendet werden, sofern der passende ODBC-Treiber installiert ist.

### Aufgabe

1. Um die 32-Bit-Version des ODBC-Datenquellen-Administrators zu starten, klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » ODBC-Datenquellen-Administrator (32-Bit)**.

Um die 64-Bit-Version des ODBC-Datenquellen-Administrators zu starten, klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » ODBC-Datenquellen-Administrator (64-Bit)**.

2. Um eine ODBC-Datenquelle für den aktuellen Benutzer zu erstellen, klicken Sie auf die Registerkarte **Benutzer-DSN**.

Um eine System-ODBC-Datenquelle zu erstellen, klicken Sie auf die Registerkarte **System-DSN**.

3. Klicken Sie auf **Hinzufügen**.
4. In der Liste **Name** wählen Sie **SQL Anywhere 16**. Klicken Sie auf **Fertig stellen**.
5. Geben Sie Verbindungsparameter für die ODBC-Datenquelle ein.

**Vorsicht**

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht-verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

6. Klicken Sie auf **OK**.
7. Klicken Sie auf **OK**.

**Ergebnisse**

Die ODBC-Datenquelle wird erstellt.

**Siehe auch**

- [„Verbindungen mit ODBC-Datenquellen herstellen \(Interactive SQL\)“ auf Seite 20](#)

## Bearbeiten von ODBC-Datenquellen (ODBC-Datenquellen-Administrator)

Sie müssen den ODBC-Datenquellen-Administrator verwenden, um eine ODBC-Datenquelle zu bearbeiten.

**Voraussetzungen**

Eine ODBC-Datenquelle muss festgelegt werden.

**Kontext und Bemerkungen**

**Vorsicht**

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

**Aufgabe**

1. Wählen Sie **Start » Programme » SQL Anywhere 16 » Administrationstools » ODBC-Datenquellen-Administrator**.
2. Klicken Sie auf eine der Registerkarten **Benutzer-DSN** oder **System-DSN**.
3. In der Liste **Name** klicken Sie auf eine Datenquelle.
4. Klicken Sie auf **Konfigurieren**.

5. Bearbeiten Sie die Verbindungsparameter für die ODBC-Datenquelle.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **OK**.

### Ergebnisse

Die ODBC-Datenquelle wird bearbeitet und gespeichert.

## ODBC-Datenquellen erstellen (Dienstprogramm dbdsn)

Verwenden Sie zum Erstellen einer ODBC-Datenquelle das Dienstprogramm dbdsn.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Unter Windows sind Systemdatenquellen für alle Benutzer des Computersystems und für Windows-Dienste verfügbar. Benutzerdatenquellen sind nur für den Benutzer verfügbar, für den sie erstellt wurden. Dateidatenquellen können nicht mit dem Dienstprogramm dbdsn erstellt werden. Verwenden Sie zum Erstellen von Dateidatenquellen den ODBC-Datenquellen-Administrator.

Unter Linux und anderen Nicht-Windows-Systemen kann das Dienstprogramm dbdsn zum Erstellen von ODBC-Datenquellen verwendet werden.

#### Hinweis

**Eine Systemdatenquelle unter 64-Bit-Windows erstellen** Systemdatenquellen sind für alle Benutzer des Computersystems und für Windows-Dienste verfügbar. Die 64-Bit-Versionen von Windows verwalten in der Windows-Registrierung zwei Gruppen von Systemdatenquellen: eine für 64-Bit-Clientanwendungen und eine für 32-Bit-Clientanwendungen. Um eine Systemdatenquelle zu erstellen, die für 32-Bit-Anwendungen geeignet ist, müssen Sie das 32-Bit-Dienstprogramm dbdsn (im Unterverzeichnis bin32 Ihres SQL Anywhere-Installationsverzeichnis) ausführen. Um Verbindungsprobleme zu vermeiden, wird empfohlen, dass Sie sowohl 64-Bit- als auch 32-Bit-Systemdatenquellen erstellen und dafür sorgen, dass diese identisch konfiguriert sind.

**Benutzerdatenquellen unter 64-Bit-Windows erstellen** Definitionen von Benutzerdatenquellen werden in der Registrierung im Abschnitt für die Einstellungen des derzeit beim System angemeldeten Benutzers gespeichert. 64-Bit-Versionen von Windows verwalten in der Windows-Registrierung eine Gruppe von Benutzerdatenquellen für jeden Benutzer des Computers. Sie können entweder die 32-Bit- oder die 64-Bit-Version des Dienstprogramms dbdsn verwenden, um eine Benutzerdatenquelle zu erstellen. Diese Datenquelle kann von 64-Bit- und 32-Bit-Clientanwendungen verwendet werden, sofern der passende ODBC-Treiber installiert ist.

### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

### Aufgabe

- Führen Sie das Datenquellen-Dienstprogramm (dbdsn) über eine Eingabeaufforderung aus.

### Ergebnisse

Die ODBC-Datenquelle wird erstellt.

### Beispiel

Mit dem folgenden Befehl wird eine ODBC-Datenquelle für die Beispieldatenbank erstellt. Der Befehl muss in einer Zeile eingegeben werden:

```
dbdsn -w "My DSN" -c "DBF=$SQLANY16/demo.db"
```

### Siehe auch

- „Datenquellen-Dienstprogramm (dbdsn)“ auf Seite 905
- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20
- „Dateidatenquellen unter Windows“ auf Seite 46

## Erstellen einer ODBC-Datenquelle (Mac OS X)

Sie können eine ODBC-Datenquelle mit dem ODBC-Administratortool für Mac OS X erstellen.

### Voraussetzungen

Das ODBC-Administratortool für Mac OS X und der SQL Anywhere ODBC-Treiber müssen installiert sein.

### Kontext und Bemerkungen

Sie können auch das Datenquellen-Dienstprogramm (dbdsn) verwenden, um unter Mac OS X ODBC-Datenquellen zu erstellen.

### Aufgabe

1. Starten Sie das ODBC-Administrator-Tool für Mac OS X aus */Applications/Utilities*.
2. Klicken Sie auf der Registerkarte **Benutzer-DSN** auf **Hinzufügen**.
3. Klicken Sie in der Liste **Name** auf **SQL Anywhere 16**.
4. Klicken Sie auf **OK**.

5. Geben Sie im Feld **Datenquellenname** einen Namen für Ihre Datenquelle ein.
6. Fügen Sie folgende Verbindungsparameter hinzu. Bei Verbindungsparametern und -werten wird die Groß-/Kleinschreibung nicht berücksichtigt.

Schlüsselwort	Wert
UserID	DBA
Password	sql
StartLine	dbeng16
ServerName	demo16
ThreadManager	ON
Driver	SQL Anywhere 16

**Vorsicht**

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht-verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Übernehmen**.
9. Drücken Sie zum Beenden Befehlstaste+Q.

**Ergebnisse**

Die ODBC-Datenquelle wird erstellt.

**Siehe auch**

- „Verbindungen mit ODBC-Datenquellen herstellen (Interactive SQL)“ auf Seite 20
- „ODBC-Datenquellen unter Unix“ auf Seite 49
- „SQL Anywhere ODBC-Treiber hinzufügen (Mac OS X)“ auf Seite 45
- „Datenquellen-Dienstprogramm (dbdsn)“ auf Seite 905
- „Verbindungsparameter“ auf Seite 337

**SQL Anywhere ODBC-Treiber hinzufügen (Mac OS X)**

Im ODBC-Administratortool für Mac OS X müssen Sie den SQL Anywhere ODBC-Treiber hinzufügen, um eine ODBC-Datenquelle erstellen zu können.

**Voraussetzungen**

Das ODBC-Administratortool für Mac OS X muss installiert sein.

### Kontext und Bemerkungen

Sie können auch das Datenquellen-Dienstprogramm (dbdsn) verwenden, um unter Mac OS X ODBC-Datenquellen zu erstellen.

### Aufgabe

1. Starten Sie das ODBC-Administrator-Tool für Mac OS X aus */Applications/Utilities*.
2. Klicken Sie auf die Registerkarte **Drivers**.
3. Klicken Sie auf **Add**.
4. Geben Sie in das Feld **Beschreibung** die Beschreibung **SQL Anywhere 16** ein.
5. Klicken Sie auf **Auswählen** und wählen Sie den SQL Anywhere ODBC-Treiber in den Feldern **Treiberdateiname** und **Setup-Dateiname** aus. Standardmäßig befindet er sich im Verzeichnis */Applications/SQLAnywhere16/System/lib64/dbodbc16\_r.bundle*.

Das *\_r* im Bundle-Namen zeigt an, dass es sich um die Treiberversion mit Threading handelt. Es gibt auch eine Version ohne Threading (*dbodbc16.bundle*) für Anwendungen ohne Threading.

6. Klicken Sie auf **OK**.

Die ODBC-Konfigurationsdateien befinden sich unter */Library/ODBC* in Ihrem Stammverzeichnis. Es gibt die Datei *odbcinst.ini* für die Treiberinformationen und die Datei *odbc.ini* für die Datenquelleninformationen. Sie können die Informationen in einem Texteditor bearbeiten.

### Ergebnisse

Der SQL Anywhere ODBC-Treiber wird hinzugefügt.

### Siehe auch

- „SQL Anywhere ODBC-Treiber hinzufügen (Mac OS X)“ auf Seite 45
- „ODBC-Datenquellen erstellen (Dienstprogramm dbdsn)“ auf Seite 43

## Dateidatenquellen unter Windows

Unter Windows-Betriebssystemen werden ODBC-Datenquellen im Allgemeinen in der Systemregistrierung gespeichert. Dateidatenquellen sind eine Alternative, da sie als Datei gespeichert werden. Unter Windows haben Dateidatenquellen normalerweise die Erweiterung *.dsn*. Sie bestehen aus Abschnitten, wobei jeder Abschnitt mit einem Namen beginnt, der in eckige Klammern gesetzt ist.

Verwenden Sie den FileDataSourceName-Verbindungsparameter (FILEDSN), wenn Sie eine Verbindung mit einer vorhandenen Dateidatenquelle herstellen wollen. Sie können in derselben Verbindungszeichenfolge nicht sowohl "DataSourceName" (DSN) als auch "FileDataSourceName" (FILEDSN) verwenden.

Wenn die Verbindung nicht erfolgreich hergestellt werden kann, tritt eines der beiden folgenden Ereignisse ein.

- **Bei einer neuen Dateidatenquelle** Der Microsoft ODBC-Datenquellen-Administrator zeigt eine Meldung an, in der festgestellt wird, dass die angegebenen Dateidatenquellenparameter nicht verwendet werden können, um eine Verbindung herzustellen. In der Meldung werden Sie gefragt, ob Sie die nicht überprüfte Datei speichern wollen. Wenn Sie sich für das Speichern der Dateidatenquelle entscheiden, schreibt der ODBC-Datenquellen-Administrator nur die folgenden Zeilen in die Datei:

```
[ODBC]
DRIVER=SQL Anywhere 16
```

Die Treiberzeichenfolge richtet sich nach der Version von SQL Anywhere.

- **Bei einer vorhandenen Dateidatenquelle** Der Microsoft ODBC-Datenquellen-Administrator zeigt eine Meldung an, in der festgestellt wird, dass der angegebene Name für die Dateidatenquelle ungültig ist. Die Dateidatenquelle wird vom ODBC-Datenquellen-Administrator nicht aktualisiert.

Wenn die Verbindung erfolgreich hergestellt wurde, wird die neue oder aktualisierte Dateidatenquelle vom ODBC-Datenquellen-Administrator auf die Festplatte geschrieben, aber der Parameter PWD=password ist nicht enthalten (und wird entfernt, wenn er vorher in der Datei vorhanden war).

#### Hinweis

Sie können Dateidatenquellen verwenden, um die Datei an Benutzer zu verteilen und die Verwaltung von Verbindungen mit mehreren Benutzern zu vereinfachen. Wenn die Datei an den Standardspeicherort für Dateidatenquellen gesetzt wird, holt sie der ODBC-Administrator automatisch.

## Erstellen einer ODBC-Dateidatenquelle (ODBC-Datenquellen-Administrator)

Sie können die Informationen zu Ihrer ODBC-Datenquelle mit dem ODBC-Datenquellen-Administrator in einer Datei speichern.

### Voraussetzungen

Um eine Dateidatenquelle erfolgreich zu erstellen, müssen Sie eine Verbindung zu der Datenbank herstellen können, für die Sie eine Dateidatenquelle erstellen.

### Kontext und Bemerkungen

#### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

### Aufgabe

1. Wählen Sie **Start » Programme » SQL Anywhere 16 » Administrationstools » ODBC-Datenquellen-Administrator**.
2. Klicken Sie auf die Registerkarte **Datei-DSN**.

3. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie in der Liste **Driver** auf **SQL Anywhere 16**.
5. Klicken Sie auf **Weiter**.
6. Befolgen Sie die Anweisungen im **Assistenten für die Erstellung einer neuen Datenquelle**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **OK**.

### Ergebnisse

Die ODBC-Datenquellendatei wird erstellt.

## ODBC-Datenquellen unter Windows Mobile

Windows Mobile hat keinen ODBC-Treibermanager oder ODBC-Datenquellen-Administrator. Unter Windows Mobile benutzt SQL Anywhere ODBC-Datenquellen, die in Dateien gespeichert sind. Um diese Datenquellendefinitionen verwenden zu können, verwenden Sie den Verbindungsparameter DSN oder FILEDSN. Unter Windows Mobile sind DSN und FILEDSN synonym.

### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht-verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

### Speicherort der Datenquelle

Windows Mobile sucht die Datenquellendateien im Stammverzeichnis des Geräts: `\Dateiname.dsn`.

Jede Datenquelle ist in einer Datei gespeichert. Die Datei hat denselben Namen wie die Datenquelle, jedoch die Erweiterung `.dsn`.

### Eine Windows Mobile-Beispieldatenquelle

Das Folgende ist ein Beispiel für eine ODBC-Datenquelle für Windows Mobile.

```
[ODBC]
DRIVER=\windows\dbodbc16.dll
Integrated=No
AutoStop=Yes
Host=192.168.0.55
LOG=\sa_connection.txt
START=dbsrv16 -c 8M
SERVER=demo
```

### Siehe auch

- „ODBC-Datenquelle für eine Verbindung mit Ihrem Windows Mobile-Gerät erstellen“ auf Seite 435
- „Dateidatenquellen unter Windows“ auf Seite 46

## ODBC-Datenquellen unter Unix

Auf Unix-Betriebssystemen befinden sich ODBC-Datenquellen in einer Systeminformationsdatei. Diese Datei hat normalerweise den Namen *.odbc.ini*. Der SQL Anywhere-Datenbankserver durchsucht die folgenden Stellen (in der angegebenen Reihenfolge) nach der Systeminformationsdatei:

- Die Umgebungsvariable ODBCINI.
- Die Umgebungsvariable ODBC\_INI.
- Die Umgebungsvariable ODBCHOME.
- Die Umgebungsvariable HOME.
- Das Ausgangsverzeichnis des Benutzers (~).
- Die PATH-Umgebungsvariable.

### Hinweis

Die Umgebungsvariablen ODBCINI und ODBC\_INI können verwendet werden, um nach der Systeminformationsdatei zu suchen (normalerweise hat diese den Namen *.odbc.ini*). Die Umgebungsvariablen ODBCHOME und HOME können zum Festlegen des Pfads, unter dem die *.odbc.ini*-Datei abgelegt ist, verwendet werden.

ODBCINI und ODBC\_INI geben einen vollständigen Pfad einschließlich des Dateinamens an. Wenn sich die Systeminformationsdatei in einem von ODBCINI oder ODBC\_INI angegebenen Verzeichnis befindet, muss ihr Name nicht *.odbc.ini* lauten.

Dies ist eine Beispiel-Systeminformationsdatei:

```
[My Data Source]
Host=hostname
ServerName=myserver
```

Sie können beliebige Verbindungsparameter in die Systeminformationsdatei eingeben.

### Vorsicht

Das Speichern von Benutzer-IDs, verschlüsselten oder nicht verschlüsselten Kennwörtern und/oder Datenbankschlüsseln in einer Datenquelle wird nicht empfohlen.

Unter Unix verwenden Sie das dbdsn-Dienstprogramm, um ODBC-Datenquellen zu erstellen und zu verwalten.

### Vorsicht

Unter Unix dürfen Sie die Systeminformationsdatei (standardmäßig *.odbc.ini*) nicht mit dem Dienstprogramm zum Verschleiern von Dateien (*dbfhide*) verschleiern, es sei denn, Sie verwenden ausschließlich SQL Anywhere-Datenquellen. Wenn Sie vorhaben, andere Datenquellen (wie z.B. für die MobiLink-Synchronisation) zu verwenden, kann das Verbergen des Inhalts der Systeminformationsdatei möglicherweise dazu führen, dass andere Treiber nicht richtig funktionieren.

Außerdem enthält die ODBC-Initialisierungsdatei (standardmäßig mit dem Namen *.odbc.ini*) möglicherweise vertrauliche Daten und Sie sollten darauf achten, die Berechtigungen für die Datei so restriktiv wie möglich zu halten. Sie können beispielsweise den Befehl "chmod 600 *.odbc.ini*" für die Datei ausführen.

### Siehe auch

- „Verbindungsparameter“ auf Seite 337
- „ODBC-Datenquellen“ auf Seite 38
- „Datenquellen-Dienstprogramm (*dbdsn*)“ auf Seite 905
- „ODBCHOME-Umgebungsvariable [Unix]“ auf Seite 470
- „ODBCINI- und ODBC\_INI-Umgebungsvariable [Unix]“ auf Seite 471

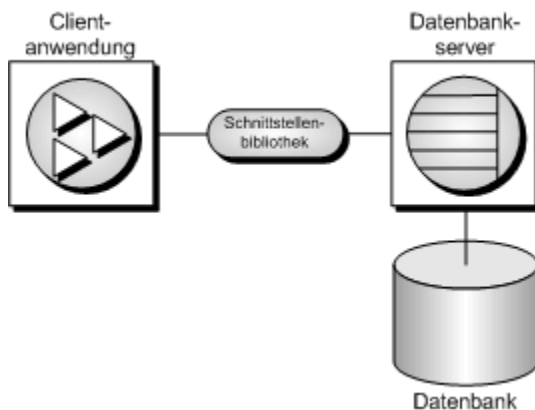
## SQL Anywhere-API-Verbindung

Um eine Verbindung mit einer Datenbank herzustellen, muss die Clientanwendung eine der folgenden SQL Anywhere-Funktionen aufrufen:

Schnittstelle	Details
ODBC	„ODBC-Unterstützung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ] „ODBC-Datenquellen“
OLE DB	„OLE DB- und ADO-Entwicklung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ]
ADO.NET	„Beispiele für eine .NET-Datenbankverbindung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ]
Embedded SQL	„Embedded SQL“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ]
Sybase Open Client	„SQL Anywhere als Open Server“ „Sybase Open Client-Unterstützung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ]
SQL Anywhere JDBC-Treiber	„Verbindungen aus einer JDBC-Clientanwendung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ] „JDBC-Unterstützung“ [ <a href="#">SQL Anywhere Server - Programmierung</a> ]

Schnittstelle	Details
jConnect JDBC-Treiber	<a href="#">„Verbindungen aus einer JDBC-Clientanwendung“ [SQL Anywhere Server - Programmierung]</a> <a href="#">„JDBC-Unterstützung“ [SQL Anywhere Server - Programmierung]</a>

Die SQL Anywhere-API verwendet Verbindungsinformationen im Aufruf der Clientanwendung, um den Datenbankserver zu finden und eine Verbindung mit ihm herzustellen. Von der Clientanwendung gesendete Informationen können Daten aus einer ODBC-Datenquelle, aus der SQLCONNECT-Umgebungsvariablen oder aus dem Server-Adressencache (*sassrv.ini*) enthalten. In der folgenden Abbildung wird eine vereinfachte Darstellung des Vorgangs gezeigt.



### Zusätzliche Informationen

Aufgabe	Empfohlene Lektüre
Eine Übersicht zum Verbinden von Sybase Central, Interactive SQL oder der SQL Anywhere-Konsole aus	<a href="#">„Das Fenster Verbinden öffnen (Sybase Central)“</a>
Einige Beispiele zur raschen praktischen Einführung, einschließlich Szenarien für Sybase Central und Interactive SQL	<a href="#">„Verbindungs-IDs“</a>
Erste Informationen über Datenquellen	<a href="#">„ODBC-Datenquellen“</a>
Informationen zu den verfügbaren Verbindungsparametern	<a href="#">„Verbindungsparameter“</a>
Ausführliche Beschreibung, wie Verbindungen eingerichtet werden	<a href="#">„Fehlerbehandlung: Verbindungen“</a>
Netzwerkspezifische Verbindungsthemen	<a href="#">„Kommunikationsprotokolle“</a>

Aufgabe	Empfohlene Lektüre
Informationen zum Einfluss von Zeichensätzen auf Verbindungen	<a href="#">„Verbindungszeichenfolgen und Zeichensätze“</a>
Informationen zu Verbindungen durch eine Firewall	<a href="#">„Firewall-Verbindungen“</a>

#### Siehe auch

- [„Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in sasrv.ini zwischenspeichern“](#) auf Seite 94
- [„SQLCONNECT-Umgebungsvariable“](#) auf Seite 479

## Integrierte Windows-Logins

Die Windows-Funktion **Integriertes Login** ermöglicht es, eine einzige Benutzer-ID und ein einziges Kennwort für die Anmeldung im Betriebssystem, im Netzwerk und für Datenbankverbindungen zu verwenden. So erstellen Sie ein integriertes Login:

- Aktivieren Sie die Funktion des integrierten Logins.
- Erstellen Sie einen Datenbankbenutzer, dem das integrierte Login zugeordnet werden soll (falls noch keiner existiert).
- Erstellen Sie eine Zuordnung eines integrierten Logins zwischen einem Windows-Benutzer- bzw. Gruppenprofil und einem bestehenden Datenbankbenutzer. Der Ordner **Login-Zuordnungen** in Sybase Central enthält alle Benutzer, die über Privilegien mit integriertem Login verfügen.
- Verbinden Sie sich von einer Clientanwendung aus und testen Sie die Funktion des integrierten Logins.

#### Unterstützte Betriebssysteme

Das integrierte Login ist für Datenbankserver unter Windows verfügbar. Windows-Clients können integrierte Logins verwenden, um eine Verbindung mit einem Netzwerkserver unter Windows herzustellen.

#### Vorteile integrierter Logins

Ein integriertes Login ist eine Zuordnung von Windows-Benutzern oder Windows-Benutzergruppen zu einem bestehenden Datenbankbenutzer. Ein Benutzer, der die Sicherheitsbarrieren für dieses Benutzerprofil oder diese Gruppe überwunden und sich an einem Computer angemeldet hat, kann sich mit einer Datenbank verbinden, ohne eine zusätzliche Benutzer-ID oder ein Kennwort eingeben zu müssen.

Um diese Funktion gewährleisten zu können, muss die Datenbank so konfiguriert sein, dass sie integrierte Logins akzeptiert, und das für die Anmeldung am Computer oder im Netzwerk benutzte Benutzerprofil muss einem Datenbankbenutzer zugeordnet werden.

Die Arbeit mit integrierten Logins ist einfacher für den Benutzer und ermöglicht die Einrichtung eines Sicherheitssystems zur Sicherstellung der Datenbank- und Netzwerksicherheit. Integrierte Logins haben folgende Vorteile:

- Die Benutzer müssen keine Benutzer-IDs oder Kennwörter eingeben.
- Die Benutzer werden vom Betriebssystem authentifiziert. Ein einziges System wird für die Datenbanksicherheit sowie die Computer- und Netzwerksicherheit eingesetzt.
- Mehrere Benutzerprofile oder Gruppen können einer einzelnen Datenbankbenutzer-ID zugeordnet werden.
- Der Name und das Kennwort für die Anmeldung beim Windows-Computer müssen nicht mit der Benutzer-ID und dem Kennwort für die Datenbank übereinstimmen.

**Vorsicht**

Integrierte Logins bieten den Vorteil eines einzigen Sicherheitssystems, können aber Sicherheitslücken öffnen, die der Datenbankadministrator berücksichtigen muss. Siehe [„Sicherheitsprobleme: Unbeschränkter Datenbankzugriff“](#) auf Seite 62 und [„Sicherheitsprobleme: Kopierte Datenbankdateien“](#) auf Seite 76.

**Siehe auch**

- [„Integriertes Login und die login\\_mode-Datenbankoption“](#) auf Seite 53
- [„Login-Zuordnungen für integrierte Windows-Logins und Kerberos-Prinzipale“](#) auf Seite 54

## Integriertes Login und die login\_mode-Datenbankoption

Die Datenbankoption login\_mode legt fest, ob die Funktion des integrierten Logins aktiviert ist oder nicht. Da die Datenbankoptionen nur für die Datenbank gelten, in der sie gefunden werden, können die Datenbanken unterschiedliche Einstellungen für das integrierte Login haben, auch wenn sie auf demselben Server geladen und ausgeführt werden.

Die Datenbankoption login\_mode akzeptiert die folgenden Werte:

- **Standard** Standard-Logins sind zulässig. Dies ist die Standardeinstellung. Standard-Verbindungslogins müssen eine Benutzer-ID und ein Kennwort liefern und verwenden nicht die Verbindungsparameter Integrated oder Kerberos. Falls eine Integrated- oder Kerberos-Login-Verbindung versucht wird, tritt ein Fehler auf.
- **Integrated** Integrierte Logins sind zulässig.
- **Kerberos** Kerberos-Logins sind zulässig.
- **LDAPUA** LDAP-Logins mit Benutzerauthentifizierung sind zulässig.
- **CloudAdmin** Dieser Login-Modus ist für die interne Verwendung durch die Cloud vorgesehen.

**Vorsicht**

Wenn die Datenbankoption login\_mode keine Standard-Logins zulässt, sind Verbindungen nur auf jene Benutzer und Gruppen beschränkt, denen eine integrierte, Kerberos-, LDAPUA- oder CloudAdmin-Login-Zuordnung erteilt wurde. Der Versuch, eine Verbindung mit einer Benutzer-ID und einem Kennwort herzustellen, führt zu einem Fehler, es sei denn, Sie sind ein Benutzer mit SYS\_AUTH\_DBA\_ROLE-Systemrolle.

Um mehr als eine Art von Login zu ermöglichen, geben Sie mehrere Werte für die login\_mode-Option an. Die folgende SQL-Anweisung z.B. setzt den Wert der Datenbankoption login\_mode so, dass Standardanmeldungen ebenso möglich sind wie integrierte Logins:

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

Wenn eine Datenbankdatei kopiert werden kann, sollte die temporäre öffentliche Option login\_mode verwendet werden (für andere Login-Modi als "Standard"). Auf diese Weise werden andere Login-Modi als "Standard" nicht standardmäßig unterstützt, wenn die Datei kopiert wird.

### Siehe auch

- [„Kerberos-Authentifizierung“ auf Seite 63](#)

## Login-Zuordnungen für integrierte Windows-Logins und Kerberos-Prinzipale

In SQL Anywhere können Sie Login-Zuordnungen erstellen, um ein Windows-Benutzerprofil oder ein Kerberos-Prinzipal einem vorhandenen Benutzer in einer Datenbank zuzuordnen.

### Siehe auch

- [„Erstellen eines integrierten Logins \(Sybase Central\)“ auf Seite 54](#)
- [„Integrierte Logins erstellen \(SQL\)“ auf Seite 55](#)
- [„Kerberos-Login-Zuordnungen erstellen“ auf Seite 70](#)
- [„Integrierte Windows-Logins“ auf Seite 52](#)
- [„Kerberos-Authentifizierung“ auf Seite 63](#)

## Erstellen eines integrierten Logins (Sybase Central)

Sie können ein integriertes Windows-Login mit SQL Anywhere verwenden, um eine einzelne Benutzer-ID und ein einzelnes Kennwort für Betriebssystem- und Netzwerk-Logins sowie für Ihre SQL Anywhere-Datenbankverbindungen zu verwalten.

### Voraussetzungen

Sie müssen das MANAGE ANY USER-Systemprivileg haben und entweder das SELECT ANY TABLE-Systemprivileg oder das SELECT-Privileg für die SYSLOGINMAP-Systemansicht.

Wenn Sie den Login-Modus ändern müssen, benötigen Sie außerdem das SET ANY SECURITY OPTION-Systemprivileg.

### Kontext und Bemerkungen

Ein Benutzer- bzw. Gruppenprofil braucht nicht zu existieren, um einer Datenbankbenutzer-ID zugeordnet zu werden. Derselben Datenbankbenutzer-ID kann mehr als ein Benutzerprofil zugeordnet werden.

Benutzerprofile können nur einer bestehenden Datenbankbenutzer-ID zugeordnet werden. Wenn diese Datenbankbenutzer-ID aus der Datenbank entfernt wird, werden alle auf dieser Datenbankbenutzer-ID basierenden integrierten Logins automatisch entfernt.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Login-Zuordnungen** und klicken Sie auf **Neu » Login-Zuordnung**.
3. Wählen Sie **Integrierte Login-Zuordnung** und klicken Sie auf **Weiter**.
4. Im Feld **Welcher Windows-Benutzer verbindet sich mit der Datenbank?** geben Sie den Namen des Benutzer- oder Gruppenprofils ein, für das das integrierte Login erstellt werden soll.
5. Wählen Sie in der Liste **Welchen Datenbankbenutzer wollen Sie mit dem Windows-Benutzer verknüpfen?** die Datenbankbenutzer-ID, der dieser Benutzer zugeordnet ist.
6. Befolgen Sie die restlichen Anweisungen im **Assistenten zum Erstellen von Login-Zuordnungen**.

### Ergebnisse

Das integrierte Login wird erstellt.

## Integrierte Logins erstellen (SQL)

Sie können ein integriertes Windows-Login mit SQL Anywhere verwenden, um eine einzelne Benutzer-ID und ein einzelnes Kennwort für Betriebssystem- und Netzwerk-Logins sowie für Ihre SQL Anywhere-Datenbankverbindungen zu verwalten.

### Voraussetzungen

Sie müssen das **MANAGE ANY USER**-Systemprivileg haben.

### Kontext und Bemerkungen

Ein Benutzer- bzw. Gruppenprofil braucht nicht zu existieren, um einer Datenbankbenutzer-ID zugeordnet zu werden. Derselben Datenbankbenutzer-ID kann mehr als ein Benutzerprofil zugeordnet werden.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie die Anweisung **GRANT INTEGRATED LOGIN TO** aus.

### Ergebnisse

Das integrierte Login wird erstellt.

### Beispiel

Mit der folgenden SQL-Anweisung können sich die Windows-Benutzer `fran_whitney` und `matthew_cobb` als DBA-Benutzer bei der Datenbank anmelden, ohne DBA-Benutzer-ID und DBA-Kennwort eingeben zu müssen.

```
GRANT INTEGRATED LOGIN  
TO fran_whitney, matthew_cobb  
AS USER DBA;
```

Mit der folgenden SQL-Anweisung können sich Windows-Benutzer, die Mitglieder der Windows-Gruppe `mywindowsusers` sind, als DBA-Benutzer bei der Datenbank anmelden, ohne DBA-Benutzer-ID und DBA-Kennwort eingeben zu müssen.

```
GRANT INTEGRATED LOGIN  
TO mywindowsusers  
AS USER DBA;
```

### Siehe auch

- „Integrierte Logins für Windows-Benutzergruppen“ auf Seite 58
- „GRANT CONNECT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Privilegien für integrierte Logins entziehen (Sybase Central)

Sie können ein Privileg für ein integriertes Login mit Sybase Central entziehen.

### Voraussetzungen

Sie müssen das `MANAGE ANY USER`-Systemprivileg haben und entweder das `SELECT ANY TABLE`-Systemprivileg oder das `SELECT`-Privileg für die `SYSLOGINMAP`-Systemansicht.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Im linken Fensterausschnitt klicken Sie auf **Login-Zuordnungen**.
3. Im rechten Fensterausschnitt rechtsklicken Sie auf die Login-Zuordnung, die Sie entfernen wollen, und klicken anschließend auf **Löschen**.
4. Klicken Sie auf **Ja**.

### Ergebnisse

Das Privileg für das integrierte Login wird entzogen.

### Siehe auch

- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Privilegien für integrierte Logins entziehen (SQL)

Sie können ein Privileg für ein integriertes Login mit der REVOKE-Anweisung entziehen.

### Voraussetzungen

Sie müssen das MANAGE ANY USER-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine REVOKE INTEGRATED LOGIN FROM-Anweisung aus.

### Ergebnisse

Das Privileg für das integrierte Login wird entzogen.

### Beispiel

Mit der folgenden SQL-Anweisung wird dem Windows-Benutzer "pchin" das Privileg für das integrierte Login entzogen:

```
REVOKE INTEGRATED LOGIN  
FROM pchin;
```

### Siehe auch

- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Verbindungen mit integrierten Logins aus Clientanwendungen

So verbinden Sie eine Clientanwendung mit einer Datenbank über ein integriertes Login:

- Setzen Sie den Parameter "Integrated" (INT) in der Liste der Verbindungsparameter auf YES (JA).
- Geben Sie weder eine Benutzer-ID noch ein Kennwort in der Verbindungszeichenfolge des Fensters **Verbinden** an.

Wenn der Parameter Integrated (INT) in der Verbindungszeichenfolge auf YES gesetzt ist, wird ein integriertes Login versucht. Der Server versucht ein Standard-Login, wenn der Verbindungsversuch fehlschlägt und die Datenbankoption login\_mode den Wert "Standard" enthält.

Wenn die Aufnahme der Verbindung mit einer Datenbank ohne Benutzer-ID oder Kennwort erfolgt, wird die Verbindung mit einem integrierten Login hergestellt. Der Erfolg des Loginversuchs hängt davon ab, ob der aktuelle Benutzerprofilname einer integrierten Login-Zuordnung in der Datenbank entspricht.

### Interactive SQL-Beispiele

Im folgenden Beispiel verläuft der Verbindungsversuch erfolgreich, wenn der Benutzer sich mit einem Benutzerprofil anmeldet, das zur integrierten Login-Zuordnung im Standard-Datenbankserver passt:

```
CONNECT USING 'INTEGRATED=yes' ;
```

Die CONNECT-Anweisung kann unter folgenden Voraussetzungen eine Verbindung mit einer Datenbank herstellen:

- Es läuft bereits ein Server.
- Bei der Standarddatenbank ist die Datenbankoption login\_mode so eingestellt, dass sie integrierte Login-Verbindungen akzeptiert.
- Es wurde ein integriertes Login zugeordnet, das dem Benutzerprofilnamen des aktuellen Benutzers entspricht bzw. für eine Windows-Benutzergruppe gilt, zu der der Benutzer gehört.
- Ein Benutzer klickt auf **OK**, ohne weitere Informationen einzugeben, wenn die Aufforderung zur Eingabe zusätzlicher Informationen erscheint.

### Siehe auch

- „login\_mode-Option“ auf Seite 623

## Integrierte Logins für Windows-Benutzergruppen

Wenn sich ein Windows-Benutzer anmeldet und keine explizite Zuordnung des integrierten Logins hat, aber einer Windows-Benutzergruppe angehört, für die es eine Zuordnung des integrierten Logins gibt, verbindet sich der Benutzer mit der Datenbank als der Datenbankbenutzer bzw. die Gruppe, die für diese Windows-Benutzergruppe in der Zuordnung des integrierten Logins festgelegt wurde.

### Vorsicht

Das Erstellen eines integrierten Logins für eine Windows-Benutzergruppe ermöglicht es jedem Benutzer, der ein Mitglied dieser Gruppe ist, sich mit der Datenbank zu verbinden, ohne die Benutzer-ID oder das Kennwort zu kennen.

Siehe „[Verbindungen mit Datenbanken für Mitglieder von Windows-Benutzergruppen verhindern](#)“ auf Seite 59.

### Mitglieder mehrerer Gruppen

Wenn der Windows-Benutzer zu mehr als einer Windows-Benutzergruppen gehört und mehr als eine Windows-Benutzergruppe auf dem Computer über eine integrierte Login-Zuordnung in der Datenbank verfügt, verläuft das integrierte Login nur erfolgreich, wenn alle Windows-Benutzergruppen auf dem Computer integrierte Login-Zuordnungen zu derselben Datenbankbenutzer-ID haben. Wenn mehrere Windows-Benutzergruppen integrierte Login-Zuordnungen zu verschiedenen Datenbankbenutzer-IDs haben, wird ein Fehler zurückgegeben und das integrierte Login schlägt fehl.

Beispiel: Eine Datenbank mit zwei Benutzer-IDs, "dbuserA" bzw. "dbuserB", und dem Windows-Benutzer "windowsuser", der zu den Windows-Benutzergruppen "xpgroupA" und "xpgroupB" gehört.

Verwendete SQL-Anweisung	Funktion
<pre>GRANT INTEGRATED LOGIN TO windowsuser AS USER dbuserA;</pre>	windowsuser verbindet sich mit der Datenbank unter Verwendung der Zuordnung des integrierten Logins, die explizit für windowsuser eingestellt ist.
<pre>GRANT INTEGRATED LOGIN TO xpgroupA AS USER dbuserB;</pre>	windowsuser verbindet sich mit der Datenbank unter Verwendung der Zuordnung des integrierten Logins, die xpgroupA erteilt wurde.
<pre>GRANT INTEGRATED LOGIN TO xpgroupA AS USER dbuserB; GRANT INTEGRATED LOGIN xpgroupb AS USER dbuserB;</pre>	windowsuser verbindet sich mit der Datenbank, weil beide Windows-Benutzergruppen, zu denen windowsuser gehört, eine Zuordnung des integrierten Logins für denselben Datenbankbenutzer haben.
<pre>GRANT INTEGRATED LOGIN TO xpgroupA AS USER dbuserA; GRANT INTEGRATED LOGIN TO xpgroupb AS USER dbuserB;</pre>	Keine Verbindung mit der Datenbank. Wenn windowsuser versucht, sich mit der Datenbank zu verbinden, schlägt das integrierte Login fehl, weil jede Windows-Benutzergruppe eine Zuordnung eines integrierten Logins für eine andere Datenbank hat und windowsuser ein Mitglied von beiden Windows-Benutzergruppen ist.

### Domain-Controller-Standorte

Standardmäßig wird der Computer, auf dem der SQL Anywhere-Datenbankserver läuft, zur Verifizierung der Windows-Benutzergruppenmitgliedschaft verwendet. Wenn der Domain Controller-Server ein anderer Computer als der ist, auf dem der Datenbankserver läuft, können Sie den Namen des Domain-Controller-Servers angeben, indem Sie die Option `integrated_server_name` verwenden. Zum Beispiel:

```
SET OPTION PUBLIC.integrated_server_name = '\\\\myserver-1';
```

Siehe „`integrated_server_name`-Option“ auf Seite 618.

## Verbindungen mit Datenbanken für Mitglieder von Windows-Benutzergruppen verhindern

Es gibt zwei Möglichkeiten, um einen Benutzer, der ein Mitglied einer Windows-Benutzergruppe mit integriertem Login ist, daran zu hindern, sich mit einer Datenbank unter Verwendung des integrierten Gruppen-Logins zu verbinden:

- Erstellen Sie ein integriertes Login für den Benutzer einer Datenbankbenutzer-ID, die kein Kennwort hat.
- Erstellen Sie eine gespeicherte Prozedur, die von der login\_procedure-Option aufgerufen wird, um zu überprüfen, ob ein Benutzer berechtigt ist, sich anzumelden, und um eine Ausnahmebedingung anzuzeigen, wenn ein gesperrter Benutzer einen Verbindungsversuch unternimmt.

### Ein integriertes Login für eine Benutzer-ID ohne Kennwort erstellen

Wenn ein Benutzer ein Mitglied einer Windows-Benutzergruppe mit integriertem Login ist, aber auch ein explizites integriertes Login für seine Benutzer-ID hat, wird das integrierte Login des Benutzers verwendet, um ihn mit der Datenbank zu verbinden. Um einen Benutzer daran zu hindern, sich unter Verwendung seines integrierten Windows-Benutzergruppenlogins mit der Datenbank zu verbinden, können Sie für den Windows-Benutzer ein integriertes Login für eine Benutzer-ID ohne Kennwort erstellen. Datenbankbenutzer-IDs, die kein Kennwort haben, können sich nicht mit einer Datenbank verbinden.

Sie können in SQL ein integriertes Login für eine Benutzer-ID ohne Kennwort erstellen.

1. Fügen Sie der Datenbank einen Benutzer ohne ein Kennwort hinzu. Zum Beispiel:

```
CREATE USER db_user_no_password;
```

2. Erstellen Sie für den Windows-Benutzer ein integriertes Login, das dem Datenbankbenutzer ohne Kennwort zugeordnet wird. Zum Beispiel:

```
GRANT INTEGRATED LOGIN TO WindowsUser  
AS USER db_user_no_password;
```

### Eine Prozedur erstellen, um Windows-Benutzer am Verbinden zu hindern

Die Option login\_procedure gibt eine gespeicherte Prozedur an, die jedes Mal aufgerufen wird, wenn ein Verbindungsversuch mit einer Datenbank unternommen wird. Standardmäßig wird die Prozedur dbo.sp\_login\_environment aufgerufen. Sie können die login\_procedure-Option so einstellen, dass eine von Ihnen geschriebene Prozedur aufgerufen wird, die bestimmte Benutzer am Verbinden mit der Datenbank hindert.

Das folgende Beispiel erstellt eine Prozedur namens login\_check, die von der login\_procedure-Option aufgerufen wird. Die login\_check-Prozedur überprüft den angegebenen Benutzernamen anhand einer Liste von Benutzern, die sich nicht mit der Datenbank verbinden dürfen. Wenn der angegebene Benutzername auf der Liste gefunden wird, schlägt die Verbindung fehl. In diesem Beispiel ist es den Benutzern Joe, Harry oder Martha nicht gestattet, sich zu verbinden. Wenn der Benutzer nicht auf der Liste steht, wird die Datenbankverbindung wie üblich fortgesetzt und die sp\_login\_environment-Prozedur aufgerufen.

```
CREATE PROCEDURE DBA.user_login_check()  
BEGIN  
    DECLARE INVALID_LOGON EXCEPTION FOR SQLSTATE '28000';  
    // Disallow certain users  
    IF( CURRENT USER IN ('Joe','Harry','Martha') ) THEN  
        SIGNAL INVALID_LOGON;  
    ELSE  
        CALL sp_login_environment;  
    END IF;
```

```

END
go
GRANT EXECUTE ON DBA.user_login_check TO PUBLIC
go
SET OPTION PUBLIC.login_procedure='DBA.user_login_check'
go

```

## Netzwerkaspekte der integrierten Logins

Wenn sich die Datenbank auf einem Netzwerkservers befindet, muss eine von zwei Bedingungen gegeben sein, damit integrierte Logins verwendet werden können:

- Das für die Verbindung mit integriertem Login verwendete Benutzerprofil muss auf dem lokalen Computer und auf dem Server vorhanden sein. Die Kennwörter für beide Benutzerprofile müssen identisch sein.

Beispiel: Wenn der Benutzer "jsmith" versucht, sich mit einem integrierten Login mit einer Datenbank zu verbinden, die auf einem Netzwerkservers geladen ist, müssen identische Benutzerprofilnamen und Kennwörter auf dem lokalen Computer und auf dem Computer bestehen, auf dem die Datenbank läuft. Der Benutzer "jsmith" muss die Berechtigung haben, sich auf beiden Computern anzumelden.

- Wenn der Netzwerkzugriff von einer Microsoft-Domäne gesteuert wird, muss der Benutzer, der ein integriertes Login versucht, die Domänenberechtigung für den Domänen-Controller-Server haben und im Netzwerk angemeldet sein. Ein Benutzerprofil auf dem Netzwerkservers, das zu dem Benutzerprofil auf dem lokalen Computer passt, ist nicht erforderlich.

## Standardbenutzer für das integrierte Login

Eine Standardbenutzer-ID für das integrierte Login kann erstellt werden, damit die Verbindung über ein integriertes Login erfolgreich verläuft, auch wenn für das aktuell verwendete Benutzerprofil keine Zuordnung für ein integriertes Login existiert.

### Beispiel

Beispiel: Wenn keine Zuordnung für ein integriertes Login für den Benutzer mit dem Profil JSMITH existiert, schlägt ein integriertes Login normalerweise fehl, wenn JSMITH das gerade benutzte Benutzerprofil ist.

Wenn Sie aber eine Benutzer-ID namens "Guest" in einer Datenbank erstellen, wird das integrierte Login erfolgreich der "Guest"-Benutzer-ID zugeordnet, falls das Benutzerprofil JSMITH nicht explizit durch eine Zuordnung für ein integriertes Login identifiziert wird.

#### Vorsicht

Durch den Standardbenutzer für ein integriertes Login können alle Benutzer, die ein integriertes Login versuchen, erfolgreich eine Verbindung mit einer Datenbank herstellen, wenn die Datenbank eine Benutzer-ID Guest enthält. Die Rollen und Privilegien, die der Benutzer-ID "Guest" erteilt werden, bestimmen, welche Rollen und Privilegien dem neu verbundenen Benutzer erteilt werden.

## Sicherheitsprobleme: Unbeschränkter Datenbankzugriff

Die Funktion des integrierten Logins benutzt das Login-Kontrollsystem von Windows anstelle des Sicherheitssystems von SQL Anywhere, um sich mit einer Datenbank ohne Angabe einer Benutzer-ID bzw. eines Kennworts zu verbinden. Im Wesentlichen gilt: Der Benutzer überwindet die Sicherheitsschranken der Datenbank, wenn er sich beim Computer anmelden kann, auf dem die Datenbank läuft.

Wenn sich der Benutzer bei einem Windows-Server erfolgreich als "dsmith" anmeldet, kann er sich ohne weitere Sicherheitsprüfung mit der Datenbank verbinden, sofern seinem Login ein integriertes Login zugeordnet ist oder er eine Standardbenutzer-ID mit integriertem Login verwendet.

Bei Verwendung von integrierten Logins müssen Datenbankadministratoren darauf achten, wie Windows die Login-Sicherheit gewährleistet, damit ein unberechtigter Zugriff auf die Datenbank verhindert wird.

### **Vorsicht**

Wenn das "Guest"-Benutzerprofil aktiviert bleibt, kann dies zu unbeschränktem Zugriff auf die Datenbank führen, die auf diesem Server läuft.

Wenn das "Guest"-Benutzerprofil aktiviert ist und ein leeres Kennwort hat, verläuft die Anmeldung beim Server erfolgreich. Es ist nicht erforderlich, dass ein Benutzerprofil auf dem Server existiert oder dass die angegebene Login-ID die Berechtigung zur Anmeldung in der Domäne hat. Jeder beliebige Benutzer kann sich mit einer beliebigen Benutzer-ID und einem Kennwort beim Server anmelden, weil er standardmäßig mit dem Benutzerprofil "Guest" angemeldet wird.

Dies hat bedeutende Auswirkungen für die Anmeldung bei einer Datenbank, für die das integrierte Login aktiviert wurde.

Überlegen Sie sich folgendes Szenario (dabei wird angenommen, dass der Windows-Server, auf dem die Datenbank läuft, ein Benutzerprofil "Guest" hat, das mit einem leeren Kennwort aktiviert wurde):

- Zwischen dem Benutzer fran\_whitney und der DBA-ID besteht eine Zuordnung für ein integriertes Login. Wenn die Benutzerin fran\_whitney über ihre richtige Login-ID und ihr Kennwort eine Verbindung mit dem Server herstellt, erfolgt die Verbindung zur Datenbank als Benutzer DBA mit vollen Administrationsrechten.

Jeder andere, der als fran\_whitney eine Verbindung mit dem Server herstellt, wird ebenfalls beim Server angemeldet, unabhängig davon, welches Kennwort eingegeben wird, da Windows diesen Verbindungsversuch dem Benutzerprofil "Guest" zuordnet. Nachdem sich der nicht autorisierte Benutzer mit der Login-ID "fran\_whitney" erfolgreich beim Server angemeldet hat, wird durch die Zuordnung des integrierten Logins auch eine Anmeldung als DBA bei der Datenbank durchgeführt.

### **Hinweis**

Aus Sicherheitsgründen sollten Sie das Benutzerprofil "Guest" deaktivieren. Die sicherste Methode für integrierte Logins besteht darin, das Benutzerprofil "Guest" auf allen Windows-Computern zu deaktivieren, auf denen eine SQL Anywhere-Datenbank läuft. Dies können Sie über die Windows-Benutzerverwaltung tun.

## LDAP-Authentifizierung

**LDAP (Lightweight Directory Access Protocol)** ist ein Branchenstandard für den Zugriff auf Verzeichnisdienste. Die LDAP-Benutzerauthentifizierung ermöglicht es Clientanwendungen, Benutzer-ID- und Kennwortinformationen an den Datenbankserver zu senden, wo diese vom LDAP-Server statt über den Katalog authentifiziert werden. Die Authentifizierung durch den LDAP-Server ermöglicht eine organisationsweite Kennwortverwaltung.

Die LDAP-Benutzerauthentifizierung ist ideal für Organisationen mit vorhandener Computerumgebung, die die Benutzeradministration vereinfachen und zentralisieren möchten, oder für Benutzer in einer neuen Computerumgebung, die Benutzer in unterschiedlichen Anwendungen und Datenbanken verwalten müssen und dies möglichst unkompliziert gestalten möchten.

Die Datenbankoption `login_mode` enthält einen LDAPUA-Modus, der die möglichen Authentifizierungsmechanismen um die LDAP-Benutzerauthentifizierung erweitert. Dank der Unterstützung der LDAP-Benutzerauthentifizierung kann SQL Anywhere in vorhandene, auf LDAP basierende unternehmensweite Verzeichniszugriffs-Frameworks integriert werden.

### Siehe auch

- „LDAP-Benutzerauthentifizierung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Kerberos-Authentifizierung

Mit dem Kerberos-Login können Sie für die Anmeldung im Betriebssystem, für das Netzwerk und für Verbindungen zur Datenbank dieselbe Benutzer-ID und dasselbe Kennwort verwenden. Die Arbeit mit Kerberos-Logins ist einfacher für den Benutzer und ermöglicht die Einrichtung eines einzigen Sicherheitssystems für die Datenbank- und Netzwerksicherheit. Dabei gibt es folgende Vorteile:

- Der Benutzer muss keine Benutzer-ID bzw. ein Kennwort liefern, um sich mit der Datenbank zu verbinden.
- Mehrere Benutzer können einer einzigen Datenbankbenutzer-ID zugeordnet werden.
- Name und Kennwort für die Anmeldung bei Kerberos müssen nicht mit der Datenbankbenutzer-Benutzerkennung und dem Datenbankkennwort übereinstimmen.

Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das eine starke Authentifizierung und Verschlüsselung unter Verwendung einer Geheimschlüssel-Chiffrierung zur Verfügung stellt. Benutzer, die bereits bei Kerberos angemeldet sind, können sich mit einer Datenbank ohne Angabe einer Benutzer-ID bzw. eines Kennworts verbinden.

Kerberos kann für die Authentifizierung verwendet werden. Folgende Voraussetzungen müssen für die Delegation der Authentifizierung an Kerberos gegeben sein:

- Sie müssen den Server und die Datenbank für die Verwendung von Kerberos-Login konfigurieren.
- Sie müssen die ID des Benutzers, der sich am Computer oder im Netzwerk anmeldet, der ID des Datenbankbenutzers zuordnen.

### Vorsicht

Im Zusammenhang mit der Verwendung von Kerberos-Logins als einzige Sicherheitsfunktion sind einige wichtige Sicherheitsüberlegungen anzustellen. Siehe „[Sicherheitsprobleme: Kopierte Datenbankdateien](#)“ auf Seite 76.

SQL Anywhere wird ohne Kerberos-Software geliefert. Sie muss getrennt erworben werden. Nachstehende Komponenten werden mit der Kerberos-Software mitgeliefert:

- **Kerberos-Bibliotheken** Diese werden als Kerberos Client- oder GSS-API-Laufzeitbibliotheken (Generic Security Services-Bibliotheken) bezeichnet. Diese Kerberos-Bibliotheken implementieren die wohldefinierte GSS-API. Die Bibliotheken müssen auf allen Client- und Servercomputern vorhanden sein, die Kerberos verwenden sollen. Die integrierte Windows SSPI-Schnittstelle kann statt einer Kerberos-Clientbibliothek von Drittherstellern verwendet werden, wenn Sie Active Directory als Ihr Schlüsselverteilungszentrum (KDC, Key Distribution Center) verwenden.

SSPI kann nur von SQL Anywhere-Clients im Kerberos-Verbindungsparameter verwendet werden. SQL Anywhere-Datenbankserver können SSPI nicht verwenden - sie benötigen einen anderen unterstützten Kerberos-Client als SSPI.

- **Ein Kerberos-KDC-Server** Das KDC (Key Distribution Center, Schlüsselverteilungszentrum) von Kerberos dient als Speicher für Benutzer und Server. Es verifiziert auch die Identifizierung von Benutzern und Servern. Das KDC wird üblicherweise auf einem Servercomputer installiert, der nicht für Anwendungen oder Benutzerlogins bestimmt ist.

SQL Anywhere unterstützt Kerberos-Authentifizierungen von DBLib-, ODBC-, OLE DB- und ADO.NET-Clients sowie von Sybase Open Client- und jConnect-Clients. Kerberos-Authentifizierungen können mit der Transportschichtssicherheit-Verschlüsselung von SQL Anywhere verwendet werden, aber SQL Anywhere unterstützt keine Kerberos-Verschlüsselung bei der Netzwerkkommunikation.

Windows verwendet Kerberos für Windows-Domänen und Domänenkonten. Active Directory Windows Domain Controller implementieren ein Kerberos-KDC. Ein Kerberos-Client bzw. eine Laufzeitbibliothek von Drittanbietern ist in dieser Umgebung dennoch auf dem Datenbankservercomputer zur Authentifizierung erforderlich, aber die Windows-Clientcomputer können die integrierte Windows SSPI-Schnittstelle statt eines Kerberos-Clients bzw. einer Laufzeitbibliothek von Drittanbietern verwenden.

### Siehe auch

- „[SSPI für Kerberos-Logins unter Windows verwenden](#)“ auf Seite 72

## Kerberos-Clients

Kerberos-Authentifizierung ist auf mehreren Plattformen verfügbar. Eine Liste getesteter Kerberos-Clients finden Sie unter <http://www.sybase.com/detail?id=1061807>.

Die folgende Tabelle listet die Standardnamen und -Standorte der Keytab- und GSS-API-Dateien auf, die von den unterstützten Kerberos-Clients verwendet werden.

**Hinweis**

SSPI kann nur von SQL Anywhere-Clients im Kerberos-Verbindungsparameter verwendet werden. SQL Anywhere-Datenbankserver können SSPI nicht verwenden - sie benötigen einen anderen unterstützten Kerberos-Client als SSPI.

Kerberos-Client	Standard-Keytab-Datei	GSS-API-Bibliotheksdatei name	Hinweise
Windows MIT Kerberos-Client	<i>C:\WINDOWS\krb5kt</i>	<i>gssapi32.dll</i> oder <i>gssapi64.dll</i>	Die Umgebungsvariable KRB5_KTNAME kann vor dem Start des Datenbankservers gesetzt werden, um eine andere Keytab-Datei anzugeben.
Windows CyberSafe Kerberos-Client	<i>C:\Programme\CyberSafe\v5srvtab</i>	<i>gssapi32.dll</i> oder <i>gssapi64.dll</i>	Die Umgebungsvariable CSFC5KTNAME kann vor dem Start des Datenbankservers gesetzt werden, um eine andere Keytab-Datei anzugeben.
Unix MIT Kerberos-Client	<i>/etc/krb5.keytab</i>	<i>libgssapi_krb5.so<sup>1</sup></i>	Die Umgebungsvariable KRB5_KTNAME kann vor dem Start des Datenbankservers gesetzt werden, um eine andere Keytab-Datei anzugeben.
Unix CyberSafe Kerberos-Client	<i>/krb5/v5srvtab</i>	<i>libgss.so<sup>1</sup></i>	Die Umgebungsvariable CSFC5KTNAME kann vor dem Start des Datenbankservers gesetzt werden, um eine andere Keytab-Datei anzugeben.
Unix Heimdal Kerberos-Client	<i>/etc/krb5.keytab</i>	<i>libgssapi.so.1<sup>1</sup></i>	

<sup>1</sup> Diese Dateinamen können abhängig von Ihrem Betriebssystem und der Kerberos-Clientversion variieren.

## Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten

Sie können die Kerberos-Authentifizierung für die Verwendung mit SQL Anywhere konfigurieren.

### Voraussetzungen

Sie müssen über die Kerberos-Authentifizierung bei Ihrem Computer angemeldet sein.

### Kontext und Bemerkungen

Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das eine starke Authentifizierung und Verschlüsselung unter Verwendung einer Geheimschlüssel-Chiffrierung zur Verfügung stellt.

### Aufgabe

1. Installieren und konfigurieren Sie ggf. die Kerberos-Clientsoftware, einschließlich der GSS-API-Laufzeitbibliothek, sowohl auf dem Client als auch auf dem Server.

Auf Windows-Clientcomputern, die ein Active Directory-Schlüsselverteilungscenter (KDC) verwenden, können Sie SSPI benutzen und müssen nicht den Kerberos-Client installieren.

2. Falls erforderlich, erstellen Sie für jeden Benutzer einen Kerberos-Prinzipal im Kerberos-KDC.

Ein Kerberos-Prinzipal ist eine Kerberos-Benutzer-ID im Format *Benutzer/Instanz@Bereich*, wobei *Instanz* optional ist. Wenn Sie bereits Kerberos verwenden, sollte der Prinzipal vorhanden sein, sodass Sie nicht mehr einen Kerberos-Prinzipal für jeden Benutzer erstellen müssen.

Bei Prinzipalen wird die Groß-/Kleinschreibung berücksichtigt, d.h., sie müssen in der korrekten Schreibweise angegeben werden. Zuordnungen für mehrere Prinzipale, die sich nur in der Groß- und Kleinschreibung unterscheiden, werden nicht unterstützt (z.B. können Sie keine Zuordnungen für jjordan@MYREALM.COM und JJordan@MYREALM.COM erhalten).

3. Erstellen Sie einen Kerberos-Prinzipal für den SQL Anywhere-Datenbankserver.

Der standardmäßige Kerberos-Prinzipal für den Datenbankserver hat das Format *Servename@Bereich*, wobei *Servename* der Name des SQL Anywhere-Datenbankservers ist. Wenn Sie einen anderen Serverprinzipal verwenden möchten, verwenden Sie die Serveroption *-kp*. Bei Prinzipalen wird die Groß-/Kleinschreibung berücksichtigt und der *Servename* darf weder Mehrbyte-Zeichen noch die Zeichen */*, *\* oder *@* enthalten.

Sie müssen einen Server Service Principal (SPN) im KDC erstellen, da Server eine Keytab-Datei für die KDC-Authentifizierung verwenden. Die Keytab-Datei ist geschützt und verschlüsselt.

4. Extrahieren Sie die Keytab-Datei für den Prinzipal *Servename@Bereich* gesichert aus dem KDC auf den Computer, auf dem der SQL Anywhere-Datenbankserver läuft. Der Standardspeicherort der Keytab-Datei hängt vom Kerberos-Client und der Plattform ab. Die Berechtigungen für die Keytab-Datei sollten so eingerichtet sein, dass der SQL Anywhere-Server sie lesen kann, aber nicht autorisierte Benutzer keine Leseberechtigung haben.

## Ergebnisse

Das Kerberos-System wird authentifiziert und für die Verwendung mit SQL Anywhere konfiguriert.

## Nächste Schritte

Konfigurieren Sie SQL Anywhere-Datenbankserver und -Datenbank für die Verwendung mit Kerberos.

## Siehe auch

- „SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren“ auf Seite 67
- „SSPI für Kerberos-Logins unter Windows verwenden“ auf Seite 72

# SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren

Sie können SQL Anywhere-Datenbanken für die Verwendung von Kerberos-Logins konfigurieren.

## Voraussetzungen

Sie müssen die Systemprivilegien SET ANY PUBLIC OPTION und MANAGE ANY USER haben.

Sie müssen bereits Kerberos konfiguriert haben, bevor SQL Anywhere es verwenden kann.

## Kontext und Bemerkungen

Mit dem Kerberos-Login können Sie für die Anmeldung bei Betriebssystemen oder Netzwerken und für Verbindungen mit Datenbanken dieselbe Benutzer-ID und dasselbe Kennwort verwenden.

## Aufgabe

1. Starten Sie den SQL Anywhere-Datenbankserver mit der Option -krb oder -kr, um die Kerberos-Authentifizierung zu aktivieren, oder verwenden Sie die Option -kl, um den Speicherort der GSS-API-Bibliothek anzugeben und Kerberos zu aktivieren.
2. Ändern Sie die öffentliche oder temporäre Option login\_mode auf einen Wert, der Kerberos umfasst. Da die Datenbankoptionen nur für die Datenbank gelten, in der sie gefunden werden, können verschiedene Datenbanken unterschiedliche Einstellungen für das Kerberos-Login haben, auch wenn sie auf demselben Server geladen und ausgeführt werden. Zum Beispiel:

```
SET OPTION PUBLIC.login_mode = 'Kerberos,Standard';
```

### Vorsicht

Wenn die Datenbankoption login\_mode auf "Kerberos" gesetzt ist, werden Verbindungen auf die Benutzer beschränkt, denen ein Kerberos-Login zugeordnet wurde. Der Versuch, eine Verbindung mit einer Benutzer-ID und einem Kennwort herzustellen, führt zu einem Fehler, es sei denn, Sie sind ein Benutzer mit SYS\_AUTH\_DBA\_ROLE-Systemrolle.

3. Erstellen Sie eine Datenbankbenutzer-ID für den Clientbenutzer. Sie können eine vorhandene Datenbankbenutzer-ID für das Kerberos-Login verwenden, sofern dieser Benutzer die passenden Privilegien hat. Zum Beispiel:

```
CREATE USER "kerberos-user"  
IDENTIFIED BY abc123;
```

4. Führen Sie die Anweisung GRANT KERBEROS LOGIN TO aus, um eine Zuordnung vom Kerberos-Prinzipal des Clients zu einer bestehenden Datenbankbenutzer-ID herzustellen. Zum Beispiel:

```
GRANT KERBEROS LOGIN TO "pchin@MYREALM.COM"  
AS USER "kerberos-user";
```

Wenn Sie eine Verbindung herstellen möchten, die einen Kerberos-Prinzipal ohne Zuordnung verwendet, vergewissern Sie sich, dass die Datenbankbenutzer-ID "Guest" existiert und ein Kennwort hat.

5. Vergewissern Sie sich, dass sich der Benutzer unter Verwendung seines Kerberos-Prinzipals bereits angemeldet hat (ein gültiges Ticket-erteilendes Kerberos-Ticket hat), und dass das Kerberos-Ticket des Clients nicht abgelaufen ist. Ein über ein Domänenkonto angemeldeter Windows-Benutzer hat bereits ein Ticket-erteilendes Ticket, wodurch er sich bei Servern authentifizieren kann, sofern sein Prinzipal ausreichende Berechtigungen hat.

Ein Ticket-erteilendes Ticket ist ein mit dem Kennwort des Benutzers verschlüsseltes Kerberos-Ticket, das vom Ticket Granting Service verwendet wird, um die Identität des Benutzers zu verifizieren.

6. Stellen Sie die Verbindung vom Client aus unter Angabe des KERBEROS-Verbindungsparameters her. (Häufig ist "KERBEROS=YES" erforderlich, aber auch "KERBEROS=SSPI" oder "KERBEROS=GSS-API-Bibliotheksdatei" kann verwendet werden.) Wenn Benutzer-ID- oder Kennwort-Verbindungsparameter angegeben werden, werden sie ignoriert. Zum Beispiel:

```
dbisql -c "KERBEROS=YES;Server=my_server_princ"
```

### Ergebnisse

Die SQL Anywhere-Datenbank ist so konfiguriert, dass sie die Kerberos-Authentifizierung verwendet.

### Nächste Schritte

Sie können die Kerberos-Authentifizierung verwenden, um von einem Client aus eine Verbindung herzustellen. Optional können Sie eine Kerberos-Login-Zuordnung erstellen.

### Beispiel

Ein Verbindungsversuch mit der folgenden SQL-Anweisung ist erfolgreich, wenn sich der Benutzer mit einem Benutzerprofilnamen anmeldet, der einer Kerberos-Login-Zuordnung für die Standarddatenbank auf einem Datenbankserver entspricht:

```
CONNECT USING 'KERBEROS=YES';
```

Die CONNECT-Anweisung kann eine Verbindung mit einer Datenbank herstellen, wenn die folgenden Bedingungen erfüllt sind:

- Es läuft bereits ein Datenbankserver.
- Die Standarddatenbank auf dem aktuellen Datenbankserver wurde so eingerichtet, dass sie Kerberos-authentifizierte Verbindungen akzeptiert.
- Eine Kerberos-Login-Zuordnung wurde für den aktuellen Kerberos-Prinzipal des Benutzers erstellt.
- Wenn der Datenbankserver ein Fenster anzeigt, mit dem er weitere Verbindungsinformationen anfordert (z.B. bei Verwendung von Interactive SQL), klickt der Benutzer auf **OK**, ohne zusätzliche Informationen einzugeben.

**Siehe auch**

- „Datenbankserveroption -kl “ auf Seite 260
- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Datenbankserveroption -krb “ auf Seite 263
- „login\_mode-Option“ auf Seite 623
- „GRANT CONNECT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kerberos-Login-Zuordnungen erstellen“ auf Seite 70
- „Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten“ auf Seite 66
- „Standardbenutzer für das integrierte Login“ auf Seite 61
- „SSPI für Kerberos-Logins unter Windows verwenden“ auf Seite 72

## Verbindungen aus Sybase Open Client- oder jConnect-Anwendungen

So stellen Sie eine Verbindung von einer Open Client- oder jConnect-Anwendung aus her:

- Richten Sie die Kerberos-Authentifizierung ein.
- Konfigurieren Sie SQL Anywhere für die Verwendung mit Kerberos. Siehe <http://www.sybase.com/detail?id=1029260>.
- Richten Sie Sybase Open Client oder jConnect so ein wie für die Kerberos-Authentifizierung mit Adaptive Server Enterprise. Der Servername muss der Name des SQL Anywhere-Servers sein und die Groß-/Kleinschreibung muss berücksichtigt werden. Es ist nicht möglich, von Sybase Open Client- oder jConnect-Anwendungen aus unter Verwendung eines alternativen Servernamens eine Verbindung herzustellen.

Weitere Hinweise zur Einrichtung der Kerberos-Prinzipale und zur Extrahierung der Keytab-Datei finden Sie unter <http://www.sybase.com/detail?id=1029260>.

### Siehe auch

- „Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten“ auf Seite 66
- „SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren“ auf Seite 67
- „Datenbankserveroption -krb “ auf Seite 263
- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Datenbankserveroption -kl “ auf Seite 260
- „login\_mode-Option“ auf Seite 623
- „GRANT CONNECT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindungsparameter Kerberos (KRB)“ auf Seite 367
- „Fehlerbehandlung: Kerberos-Verbindungen“ auf Seite 73

## Kerberos-Login-Zuordnungen erstellen

Sie können mithilfe von Sybase Central eine Kerberos-Login-Zuordnung erstellen, wobei ein einzelner Benutzer für die Kerberos-Authentifizierung beim Datenbankserver konfiguriert wird.

### Voraussetzungen

Sie müssen bereits Kerberos konfiguriert haben, bevor SQL Anywhere es verwenden kann. Sie müssen SQL Anywhere-Datenbankserver und -Datenbank bereits für die Verwendung von Kerberos konfiguriert haben.

Der Datenbankbenutzer und der Kerberos-Prinzipal müssen bereits vorhanden sein.

Sie müssen das **MANAGE ANY USER**-Systemprivileg haben und entweder das **SELECT ANY TABLE**-Systemprivileg oder das **SELECT**-Privileg für die **SYSLOGINMAP**-Systemansicht.

Wenn Sie den Login-Modus ändern müssen, benötigen Sie außerdem das **SET ANY SECURITY OPTION**-Systemprivileg.

### Kontext und Bemerkungen

Eine Kerberos-Login-Zuordnung ist die Verbindung zwischen der ID des Benutzers, der sich beim Computer oder im Netzwerk anmeldet, und dem Datenbankbenutzer.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Login-Zuordnungen** und klicken Sie auf **Neu » Login-Zuordnung**.
3. Wählen Sie **Kerberos-Login-Zuordnung** und klicken Sie auf **Weiter**.
4. Im Feld **Welcher Kerberos-Prinzipal verbindet sich mit der Datenbank?** geben Sie den Namen des Kerberos-Prinzipals ein, für den das Kerberos-Login erstellt werden soll.

5. Wählen Sie in der Liste **Welchen Datenbankbenutzer wollen Sie mit dem Kerberos-Prinzipal verknüpfen?** die Datenbankbenutzer-ID, der dieser Kerberos-Prinzipal zugeordnet ist.
6. Befolgen Sie die restlichen Anweisungen im **Assistenten zum Erstellen von Login-Zuordnungen**.

### Ergebnisse

Eine Kerberos-Login-Zuordnung wird erstellt.

### Siehe auch

- „Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten“ auf Seite 66
- „SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren“ auf Seite 67
- „GRANT CONNECT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Kerberos-Login-Zuordnungen entziehen

Sie können mithilfe von Sybase Central eine Kerberos-Login-Zuordnung entziehen.

### Voraussetzungen

Sie müssen bereits Kerberos konfiguriert haben, bevor SQL Anywhere es verwenden kann. Sie müssen SQL Anywhere-Datenbankserver und -Datenbank bereits für die Verwendung von Kerberos konfiguriert haben.

Der Datenbankbenutzer und der Kerberos-Prinzipal müssen bereits vorhanden sein.

Sie müssen das MANAGE ANY USER-Systemprivileg haben und entweder das SELECT ANY TABLE-Systemprivileg oder das SELECT-Privileg für die SYSLOGINMAP-Systemansicht.

### Kontext und Bemerkungen

Eine Kerberos-Login-Zuordnung ist die Verbindung zwischen der ID des Benutzers, der sich beim Computer oder im Netzwerk anmeldet, und dem Datenbankbenutzer.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Im linken Fensterausschnitt klicken Sie auf **Login-Zuordnungen**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf die Login-Zuordnung und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Ja**.

### Ergebnisse

Die Kerberos-Login-Zuordnung wird entzogen.

### Siehe auch

- „Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten“ auf Seite 66
- „SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren“ auf Seite 67
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## SSPI für Kerberos-Logins unter Windows verwenden

In einer Windows-Domäne kann SSPI auf Windows-Computern ohne installierten Kerberos-Client verwendet werden. Windows-Domänenkonten haben bereits zugeordnete Kerberos-Prinzipale.

### Voraussetzungen

Sie müssen bereits Kerberos konfiguriert haben, bevor SQL Anywhere es verwenden kann. Sie müssen SQL Anywhere-Datenbankserver und -Datenbank bereits für die Verwendung von Kerberos konfiguriert haben.

### Kontext und Bemerkungen

SSPI kann nur von SQL Anywhere-Clients im Kerberos-Verbindungsparameter verwendet werden. SQL Anywhere-Datenbankserver können SSPI nicht verwenden - sie benötigen einen anderen unterstützten Kerberos-Client als SSPI.

### Aufgabe

- Stellen Sie vom Clientcomputer aus eine Verbindung mit der Datenbank her. Zum Beispiel:

```
dbisql -c "KERBEROS=SSPI;Server=my_server_princ"
```

Wenn "Kerberos=SSPI" in der Verbindungszeichenfolge angegeben ist, wird ein Kerberos-Login versucht.

Ein Verbindungsversuch mit der folgenden SQL-Anweisung ist ebenfalls erfolgreich, sofern sich der Benutzer mit einem Benutzerprofilnamen angemeldet hat, der einer Kerberos-Login-Zuordnung für die Standarddatenbank auf einem Datenbankserver entspricht:

```
CONNECT USING 'KERBEROS=SSPI';
```

### Ergebnisse

Sie können SSPI für die Kerberos-Authentifizierung unter Windows verwenden.

### Siehe auch

- „Kerberos-Systeme für die Verwendung mit SQL Anywhere einrichten“ auf Seite 66
- „SQL Anywhere-Datenbanken für die Verwendung von Kerberos konfigurieren“ auf Seite 67

## Fehlerbehandlung: Kerberos-Verbindungen

Wenn Sie unerwartete Fehlermeldungen erhalten, während Sie versuchen, die Kerberos-Authentifizierung zu aktivieren oder zu verwenden, wird empfohlen, zusätzliche Diagnosemeldungen auf dem Datenbankserver und auf dem Client zu aktivieren.

Geben Sie beim Start des Datenbankservers die Option `-z` an oder verwenden Sie `CALL sa_server_option( 'DebuggingInformation', 'ON' )`, falls der Server bereits läuft, um zusätzliche Diagnosemeldungen auf der Serverkonsole zu erhalten. Der Verbindungsparameter `LogFile` schreibt Client-Diagnosemeldungen in die angegebene Datei.

Als Alternative zum `LogFile`-Verbindungsparameter können Sie das Ping-Dienstprogramm (`dbping`) mit dem Parameter `-z` verwenden. Der Parameter `-z` zeigt Diagnosemeldungen an, die dazu beitragen können, die Ursache des Verbindungsproblems zu ermitteln.

### Schwierigkeiten beim Start des Datenbankservers

Symptom	Übliche Lösungen
Meldung "Kerberos GSS-API-Bibliothek konnte nicht geladen werden"	<ul style="list-style-type: none"> <li>• Vergewissern Sie sich, dass ein Kerberos-Client sowie die GSS-API-Bibliothek auf dem Datenbankserver-Computer installiert sind.</li> <li>• Die Ausgabe der Datenbankserveroption <code>-z</code> listet den Namen der Bibliothek auf, die der Datenbankserver zu laden versucht. Überprüfen Sie, ob der Bibliotheksname richtig ist. Erforderlichenfalls verwenden Sie die Option <code>-kl</code>, um den richtigen Bibliotheksnamen anzugeben.</li> <li>• Vergewissern Sie sich, dass das Verzeichnis und etwaige Supportbibliotheken im Bibliothekspfad angegeben sind (%PATH% unter Windows).</li> <li>• Wenn die Ausgabe der Datenbankserveroption <code>-z</code> angibt, dass der GSS-API-Bibliothek Eintrittspunkte fehlen, dann ist die Bibliothek keine unterstützte Kerberos Version 5 GSS-API-Bibliothek.</li> </ul>
Meldung "Abrufen der Kerberos-Anmeldedaten für Servername ' <i>Servername</i> ' nicht möglich"	<ul style="list-style-type: none"> <li>• Vergewissern Sie sich, dass im KDC ein Prinzipal für <i>Servername@Bereich</i> vorhanden ist. Prinzipale berücksichtigen die Groß-/Kleinschreibung, daher vergewissern Sie sich, dass der Datenbankservername dieselbe Schreibweise wie der Benutzerabschnitt des Prinzipalnamens hat.</li> <li>• Vergewissern Sie sich, dass der Name des SQL Anywhere-Servers der Primär-/Benutzerabschnitt des Prinzipals ist.</li> <li>• Vergewissern Sie sich, dass der Prinzipal des Servers in eine Keytab-Datei extrahiert wurde und dass die Keytab-Datei den korrekten Standort für den Kerberos-Client angibt.</li> <li>• Wenn sich der Standard-Realm für den Kerberos-Client auf dem Datenbankserver-Computer vom Realm im Server-Prinzipal unterscheidet, verwenden Sie die Option <code>-kr</code>, um den Realm im Server-Prinzipal anzugeben.</li> </ul>

Symptom	Übliche Lösungen
Client-Fehler "Kerberos-Login fehlgeschlagen"	<ul style="list-style-type: none"> <li>Überprüfen Sie die Diagnosemeldungen des Datenbankservers. Manche Probleme mit der vom Server verwendeten Keytab-Datei werden erst erkannt, wenn ein Client versucht, sich zu authentifizieren.</li> </ul>

### Fehlerbehandlung bei Kerberos-Clientverbindungen

Wenn der Client einen Fehler beim Versuch erhielt, unter Verwendung der Kerberos-Authentifizierung eine Verbindung herzustellen:

Symptom	Übliche Lösungen
Fehler "Kerberos-Logins werden nicht unterstützt" und LogFile enthält die Meldung "Laden der Kerberos GSS-API-Bibliothek fehlgeschlagen"	<ul style="list-style-type: none"> <li>Vergewissern Sie sich, dass ein Kerberos-Client auf dem Clientcomputer installiert ist, einschließlich der GSS-API-Bibliothek.</li> <li>Die von LogFile angegebene Datei listet den Namen der Bibliothek auf, die zu laden versucht wird. Überprüfen Sie, ob der Bibliotheksname korrekt ist, und verwenden Sie falls erforderlich den Kerberos-Verbindungsparameter, um den korrekten Bibliotheksnamen anzugeben.</li> <li>Vergewissern Sie sich, dass das Verzeichnis, das etwaige Supportbibliotheken enthält, im Bibliothekspfad angegeben ist (%PATH% unter Windows).</li> <li>Wenn die LogFile-Ausgabe angibt, dass der GSS-API-Bibliothek Eintrittspunkte fehlten, dann ist die Bibliothek keine unterstützte Kerberos Version 5 GSS-API-Bibliothek.</li> </ul>
Fehler "Kerberos-Logins werden nicht unterstützt"	<ul style="list-style-type: none"> <li>Vergewissern Sie sich, dass der Datenbankserver Kerberos-Logins aktiviert hat, indem Sie eine oder mehrere der Serveroptionen -krb, -kl oder -kr angeben.</li> <li>Vergewissern Sie sich, dass Kerberos-Logins von SQL Anywhere auf der Client- und auf der Serverplattform unterstützt werden. Siehe „<a href="#">Kerberos-Clients</a>“ auf Seite 64.</li> </ul>

Symptom	Übliche Lösungen
Fehler "Kerberos-Login fehlgeschlagen"	<ul style="list-style-type: none"> <li>• Vergewissern Sie sich, dass der Benutzer bei Kerberos angemeldet ist und ein gültiges Ticket-erteilendes Ticket hat, das noch nicht abgelaufen ist.</li> <li>• Vergewissern Sie sich, dass beim Clientcomputer und beim Servercomputer die Uhrzeiten mit maximal 5 Minuten Unterschied synchronisiert sind.</li> </ul>
Fehler "Login-Modus 'Kerberos' bei login_mode-Einstellung nicht zulässig"	<ul style="list-style-type: none"> <li>• Die öffentliche oder temporäre Datenbankoptionseinstellung bei der login_mode-Option muss den Wert "Kerberos" enthalten, um Kerberos-Logins zuzulassen.</li> </ul>
"Die Login-ID ' <i>Client-Kerberos-Prinzipal</i> ' wurde keiner Datenbankbenutzer-ID zugeordnet"	<ul style="list-style-type: none"> <li>• Der Kerberos-Prinzipal muss einer Datenbankbenutzer-ID mit der Anweisung GRANT KERBEROS LOGIN zugeordnet werden. Beachten Sie, dass der vollständige Client-Prinzipal einschließlich des Realms in der Anweisung GRANT KERBEROS LOGIN angegeben werden muss, und dass Prinzipale, die sich nur in der Instanz oder im Realm unterscheiden, als unterschiedlich behandelt werden.</li> <li>• Wenn jeder gültige Kerberos-Prinzipal, der nicht explizit zugeordnet wurde, in der Lage sein soll, eine Verbindung herzustellen, können Sie auch unter Verwendung von GRANT CONNECT die Datenbankbenutzer-ID Guest mit einem Kennwort erstellen.</li> </ul>

**Siehe auch**

- „Datenbankserveroption -z “ auf Seite 312
- „Kerberos-Clients“ auf Seite 64
- „login\_mode-Option“ auf Seite 623
- „Ping-Dienstprogramm (dbping)“ auf Seite 955

## Sicherheitsprobleme: Temporäre öffentliche Optionen als zusätzliche Sicherheitsmaßnahmen

Wenn Sie den Wert der login\_mode-Option für eine bestehende Datenbank mit der SET OPTION-Anweisung so setzen, dass sie eine Kombination aus integrierten sowie Standard-, Kerberos- und LDAPUA-Logins zulässt, werden die angegebenen Login-Typen für diese Datenbank permanent aktiviert. Die folgende Anweisung z.B. lässt permanent Standard- und integrierte Logins zu:

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

Wenn die Datenbank heruntergefahren und neu gestartet wird, bleibt der Wert der Option gleich und integrierte Logins bleiben weiterhin zulässig.

Wenn Sie die Option `login_mode` mit `SET TEMPORARY OPTION` setzen, ermöglicht dies weiterhin einen Benutzerzugriff über integrierte Logins, aber nur bis die Datenbank heruntergefahren wird. Mit der folgenden Anweisung wird der Optionswert temporär geändert:

```
SET TEMPORARY OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

Wenn der permanente Optionswert "STANDARD" ist, kehrt die Datenbank zu diesem Wert zurück, wenn sie heruntergefahren und wieder heraufgefahren wird.

Durch das Einstellen temporärer öffentlicher Optionen kann Ihre Datenbank mit zusätzlichen Sicherheitsfunktionen versehen werden. Wenn Sie einer Datenbank integrierte, Kerberos- oder LDAPUA-Logins hinzufügen, ist die Datenbank von den Sicherheitsfunktionen des Betriebssystems abhängig, unter dem sie läuft. Wenn die Datenbank auf einen anderen Computer kopiert wird, fallen die Zugriffsberechtigungen zur Datenbank auf das SQL Anywhere-Sicherheitsmodell zurück.

### Siehe auch

- „Sicherheitsprobleme: Kopierte Datenbankdateien“ auf Seite 76
- „SET OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Sicherheitsprobleme: Kopierte Datenbankdateien

Wenn die Datenbankdatei kopiert werden kann, benutzen Sie die temporäre öffentliche Option `login_mode` für integrierte und Kerberos-Logins. Wenn die Datei kopiert wird, werden die integrierten und Kerberos-Logins standardmäßig nicht unterstützt.

Wenn eine Datenbank schützenswerte Daten enthält, muss der Computer, auf dem die Datenbankdateien gespeichert sind, gegen nicht autorisierten Zugriff geschützt werden. Sonst könnten die Datenbankdateien kopiert und ohne Autorisierung auf einem anderen Computer eingesehen werden. So erhöhen Sie die Datenbanksicherheit:

- Kennwörter sollten komplex und schwer zu erraten sein.
- Stellen Sie die Datenbankoption `PUBLIC.login_mode` auf Standard ein. Um integrierte oder Kerberos-Logins zu aktivieren, sollte nur die temporäre öffentliche Option beim Serverstart geändert werden. Dies gewährleistet, dass nur Standard-Logins zulässig sind, falls die Datenbank kopiert wird.
- Verwenden Sie für die Datenbankdatei eine starke Verschlüsselung mit dem AES-Verschlüsselungsalgorithmus. Der Chiffrierschlüssel sollte komplex und schwer zu erraten sein.

### Siehe auch

- „Sicherheitsprobleme: Temporäre öffentliche Optionen als zusätzliche Sicherheitsmaßnahmen“ auf Seite 75

## Verbindungspooling

Verbindungspooling kann die Performance von Anwendungen verbessern, die viele kurze Verbindungen zum Datenbankserver herstellen. Wenn Verbindungspooling für eine Verbindung aktiviert ist, wird sie bei der Trennung automatisch im Cache zwischengespeichert und kann wieder verwendet werden, wenn die Anwendung erneut eine Verbindung herstellt. Verbindungspooling wird mit dem Verbindungsparameter ConnectionPool (CPOOL) gesteuert. Wenn eine Anwendung eine bestimmte Anzahl von Verbindungen mit derselben Verbindungszeichenfolge erstellt, wird die Verbindung gepoolt.

Eine Anwendung muss fünf Verbindungen mit derselben Verbindungszeichenfolge herstellen, bevor eine Verbindung im Cache zwischengespeichert wird. Der Verbindungsname kann jedes Mal anders sein, alle anderen Verbindungsparameter müssen jedoch identisch sein, damit eine im Cache gespeicherte Verbindung wiederverwendet werden kann.

Wenn der Anwendungsprozess erneut eine Verbindung herstellt und im Cache zwischengespeicherte Verbindungen für dieselbe Verbindungszeichenfolge verfügbar sind, wird die Verbindung im Cache wieder verwendet. Verbindungen bleiben für den im Verbindungsparameter ConnectionPool (CPOOL) angegebenen Zeitraum (standardmäßig 60 Sekunden) im Cache.

Im Cache zwischengespeicherte Verbindungen werden nicht wieder verwendet, wenn dies das Verhalten der Anwendung ändern würde. Zum Beispiel werden im Cache zwischengespeicherte Verbindungen nicht wiederverwendet:

- Bei Datenbanken, die automatisch stoppen, wenn keine Verbindungen zu ihnen vorhanden sind.
- Wenn Verbindungen deaktiviert sind.
- Wenn der Datenbankserver seine Verbindungsobergrenze erreicht hat.
- Wenn ein Kennwort geändert wurde.
- Wenn die login\_mode-Option gesetzt ist.

Um sicherzustellen, dass die Verbindungspoolfunktion für die Anwendung eindeutig erkennbar ist, wird eine Verbindung getrennt, wenn beim Caching der Verbindung im Cache ein Fehler auftritt. Wenn beim Versuch, eine Verbindung im Cache wieder zu verwenden, ein Fehler auftritt, versucht der Datenbankserver auf die übliche Art und Weise eine Verbindung herzustellen.

Eine Verbindung wird im Cache zwischengespeichert, wenn sie getrennt wird und die durch den Verbindungsparameter CPOOL angegebene maximale Anzahl von Verbindungen noch nicht erreicht ist. Die Verbindung wird erneut initialisiert und die Verbindung im Cache bleibt mit dem Datenbankserver bestehen, selbst wenn die Anwendung diese getrennt hat. Das Bereinigen und Reinitialisieren einer Verbindung umfasst die folgenden Aktivitäten:

- Alle ausstehenden Transaktionen werden zurückgesetzt.
- Temporäre Tabellen, temporäre Funktionen und Variablen werden gelöscht.
- Verbindungsoptionen und Verbindungszähler werden zurück- bzw. auf Null gesetzt.

- Die Zähler für die Datenbankserververbindung werden erhöht bzw. verringert. Sie werden nicht über vorhandene aktive Verbindungen informiert, wenn ein Datenbankserver nur mit im Cache zwischengespeicherten Verbindungen heruntergefahren wird.
- Es werden alle definierten Trenn- und Verbindungsereignisse ausgeführt.
- Die Datenbankoption login\_procedure wird ausgeführt und die Login-Richtlinie überprüft.
- Die Verbindungs-ID wird zurückgesetzt.

### Verwenden von SQL Anywhere-Verbindungspools mit anderen Verbindungspooling-Produkten

Wenn Sie ein Produkt oder eine API verwenden, das bzw. die Verbindungspooling unterstützt, hat das Verbindungspooling des Produkts oder der API Vorrang vor dem SQL Anywhere-Verbindungspooling. Beide Arten des Verbindungspoolings können gleichzeitig aktiv sein.

Das Verhalten des Verbindungspoolings in Ihrem Produkt oder Ihrer API kann sich signifikant vom SQL Anywhere-Verbindungspooling unterscheiden. Wenn das Verhalten des Verbindungspoolings in Ihrem Produkt oder Ihrer API ungeeignet für eine Anwendung ist, kann das SQL Anywhere-Verbindungspooling verwendet und damit möglicherweise die Performance bestimmter Anwendungen verbessert werden.

### Verbindungspooling und Scale-Out mit Schreibschutz

Wenn der NodeType-Verbindungsparameter (NODE) ebenfalls für eine Verbindung angegeben wird, stellt die Anwendung in der Regel eine Verbindung mit dem Primärserver her und der Primärserver ermittelt, welcher Kopieknoten am wenigsten ausgelastet ist. Die Verbindung wird dann auf diesen Knoten umgeleitet. Wenn die Anwendung innerhalb eines kurzen Zeitraums mehrere Verbindungen dieser Art herstellt und löscht, wird die Verbindung gepoolt und der Primärserver wird nicht gefragt, welcher Kopieknoten verwendet werden soll. Dieses Verhalten reduziert die Auslastung auf dem Primärserver, weist aber möglicherweise nicht das erwartete Verhalten auf.

### Siehe auch

- [„Verbindungsparameter ConnectionPool \(CPOOL\)“ auf Seite 350](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [ConnPoolCachedCount-Datenbankeigenschaft auf Seite 771](#)
- [ConnPoolHits-Datenbankeigenschaft auf Seite 771](#)
- [ConnPoolMisses-Datenbankeigenschaft auf Seite 771](#)

## Temporäre Verbindungen

Der SQL Anywhere-Datenbankserver verwendet temporäre Verbindungen zum Durchführen von Vorgängen wie z.B. dem Ausführen von Sicherungen oder Initialisieren von Datenbanken. Sie können Informationen über temporäre Verbindungen mit den Systemprozeduren sa\_conn\_info oder sa\_conn\_list abrufen. Die Eigenschaft ParentConnection gibt die Verbindungs-ID der Verbindung zurück, die die temporäre Verbindung erzeugt hat.

Temporäre Verbindungen haben Verbindungs-IDs, die größer sind als 1 Milliarde (1000000000) und deren Name die Funktion der Verbindung beschreibt.

Im folgende Beispiel wird mithilfe der sa\_conn\_info-Systemprozedur eine Ergebnismenge zurückgegeben, die zeigt, welche Verbindung eine temporäre Verbindung erstellt hat.

```
SELECT Number, Name, ParentConnection FROM sa_conn_info();
```

Verbindung 8 hat die temporäre Verbindung erzeugt, von der eine CREATE DATABASE-Anweisung ausgeführt wurde.

Number	Name	ParentConnection
1000000048	INT: CreateDB	8
9	SQL_DBC_14675af8	(NULL)
8	SQL_DBA_152d5ac0	(NULL)

#### Siehe auch

- [ParentConnection-Verbindungseigenschaft auf Seite 729](#)
- [Name-Verbindungseigenschaft auf Seite 727](#)
- [„sa\\_conn\\_info-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„sa\\_conn\\_list-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„CONNECTION\\_PROPERTY-Funktion \[System\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Fehlerbehandlung: Verbindungen

Zur Lösung von Verbindungsproblemen ist ein besseres Verständnis der Art, wie SQL Anywhere Verbindungen einrichtet, hilfreich. Weitere Informationen zu Netzwerkfragen einschließlich Verbindungen über Firewalls finden Sie unter [„Kommunikationsprotokolle“ auf Seite 102](#).

SQL Anywhere geht bei der Einrichtung einer Verbindung wie folgt vor:

1. Suchen der Schnittstellenbibliothek. Siehe [„Fehlerbehandlung: Der Speicherort der Schnittstellenbibliothek“ auf Seite 80](#).
2. Zusammenstellen einer Liste von Verbindungsparametern. Siehe [„Fehlerbehandlung: Verbindungen einrichten“ auf Seite 81](#).
3. Suchen eines Datenbankservers. Wenn der Datenbankserver nicht gefunden wird, startet SQL Anywhere einen Personal Server. Siehe [„Fehlerbehandlung: Datenbankserver suchen“ auf Seite 83](#).
4. Suchen der Datenbank. Siehe [„Fehlerbehandlung: Datenbankserver suchen“ auf Seite 94](#).

Der Vorgang für die Einrichtung von Verbindungen durch SQL Anywhere ist für folgende Anwendungen identisch:

- Alle **ODBC-Anwendungen**, die die SQLDriverConnect-Funktion (die übliche Methode für die Verbindung von ODBC-Anwendungen) verwenden. Viele Anwendungs-Entwicklungssysteme, wie Sybase PowerBuilder, gehören zu dieser Klasse von Anwendungen. Die SQLConnect-Funktion ist auch für ODBC-Anwendungen verfügbar.
- Jede Clientanwendung, die **Embedded SQL** und die empfohlene Funktion für die Verbindung mit einer Datenbank verwendet (db\_string\_connect). Zusätzlich steht die SQL-Anweisung CONNECT für

Embedded SQL-Anwendungen sowie in Interactive SQL zur Verfügung. Sie hat zwei Formate: CONNECT AS und CONNECT USING. Alle Datenbankdienstprogramme (einschließlich dbisqlc) benutzen db\_string\_connect.

- Jede **.NET**-Anwendung, die ADO.NET verwendet. Die Anwendung erstellt ein SAConnection-Objekt und übergibt die Verbindungszeichenfolge an den Konstruktor oder legt dieConnectionString-Eigenschaft fest. Danach ruft die Anwendung die Open-Methode für das SAConnection-Objekt auf, um die Verbindung herzustellen.
- Jede **ADO-Anwendung**, die das ADODB-Verbindungsobjekt verwendet. Die Provider-Eigenschaft wird verwendet, um den OLE DB-Treiber zu lokalisieren. DieConnectionString-Eigenschaft kann **DataSource** als Alternative zu **DataSourceName** und **User ID** als Alternative zu **UserID** verwenden.
- Anwendungen, die den **SQL Anywhere JDBC-Treiber** verwenden, um die URL **jdbc:sqlanywhere:**, gefolgt von einer Standard-Verbindungszeichenfolge, als Parameter an die DriverManager.GetConnection-Methode zu übergeben.

### Siehe auch

- „Fehlerbehandlung beim Datenbankserverstart“ auf Seite 1109
- „Fehlerbehandlung für Netzwerkverbindungen“ auf Seite 1113

## Fehlerbehandlung: Der Speicherort der Schnittstellenbibliothek

Im Allgemeinen ist der Speicherort dieser DLL oder gemeinsamen Bibliothek für den Benutzer transparent.

### Speicherort des ODBC-Treibers

Für ODBC wird die Schnittstellenbibliothek auch als ODBC-Treiber bezeichnet. Eine ODBC-Clientanwendung ruft den ODBC-Treiber-Manager auf, und dieser ermittelt den Speicherort des SQL Anywhere-Treibers.

Der ODBC-Treiber-Manager durchsucht die übergebene Datenquelle, um festzustellen, wo sich der Treiber befindet. Wenn Sie mit dem ODBC-Datenquellen-Administrator oder dem dbdsn-Dienstprogramm eine Datenquelle erstellen, füllt SQL Anywhere den aktuellen Speicherort für den ODBC-Treiber aus. Die Datenquelleninformationen werden unter Windows in der Registrierung bzw. unter Unix in einer Systeminformationsdatei (standardmäßig mit dem Namen *.odbc.ini*) gespeichert.

### Speicherort der Schnittstellenbibliothek für Embedded SQL

Embedded SQL-Anwendungen werden normalerweise über die SQL Anywhere Embedded SQL-Importbibliothek verknüpft. Die Interface-Bibliothek wird anhand des Namens geladen, wenn die Anwendung gestartet wird. Der Name der Embedded SQL-Schnittstellenbibliothek von SQL Anywhere lautet wie folgt:

- **Windows** *dblib16.dll*
- **Unix** *libdblib16* mit einer betriebssystemspezifischen Erweiterung

**OLE DB-Treiberspeicherort**

Der Providernamen (SAOLEDB) wird zur Ermittlung der SQL Anywhere OLE DB Provider-DLL (*dboledb16.dll*) aufgrund der Einträge in der Registrierung verwendet. Diese Einträge werden erstellt, wenn der SAOLEDB-Provider installiert oder neu registriert wird.

**ADO.NET**

ADO.NET-Programme fügen eine Referenz zum SQL Anywhere ADO.NET-Provider hinzu, der *iAnywhere.Data.SQLAnywhere.dll* genannt wird. Die .NET Data Provider DLL wird während der Installation dem .NET Global Assembly Cache (GAC) hinzugefügt.

**SQL Anywhere JDBC-Treiberspeicherort**

Wenn Sie Ihre Anwendung ausführen, muss das Java-Paket *sajdbc4.jar* (JDBC 4.0) im Classpath enthalten sein. Das System muss in der Lage sein, die nativen DLLs oder Shared Objects zu ermitteln.

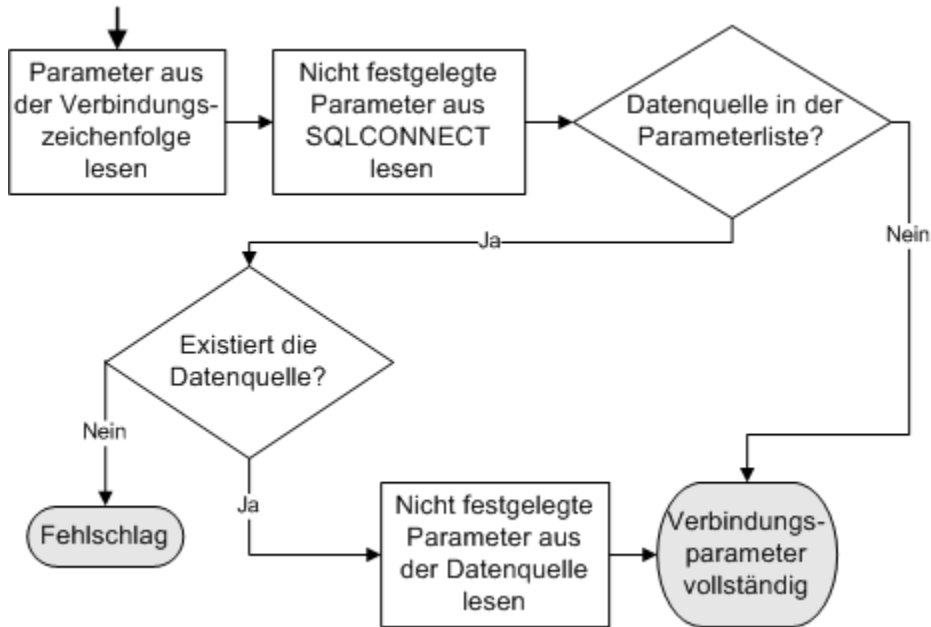
- **Windows** Unter Windows werden das aktuelle Verzeichnis, der Systempfad sowie die Verzeichnisse *Windows* und *Windows\system32* durchsucht.
- **Unix** Unter Unix werden der Systempfad und der Benutzerbibliothekspfad durchsucht.

**Wenn die Bibliothek gefunden wurde**

Eine Verbindungszeichenfolge wird an die Schnittstellenbibliothek gesendet, wenn sie von der Clientanwendung gefunden wird. Die Zeichenfolge wird von der Schnittstellenbibliothek verwendet, um eine Liste von Verbindungsparametern zusammenzustellen und eine Serververbindung einzurichten.

**Fehlerbehandlung: Verbindungen einrichten**

Das nachstehende Diagramm zeigt, wie die Schnittstellenbibliothek die Liste von Verbindungsparametern zusammenstellt und eine Verbindung herstellt.



- **Vorrang** Parameter, die an mehr als einer Stelle benutzt werden, müssen folgende Vorrangregeln beachten:

1. Verbindungszeichenfolge
2. SQLCONNECT-Umgebungsvariable
3. ODBC-Datenquelle

#### Hinweis

Wenn eine Verbindungszeichenfolge und eine ODBC-Datenquelle beide denselben Verbindungsparameter angeben, wird der Wert aus der Zeichenfolge verwendet und der Wert aus der Datenquelle ignoriert. Siehe „Syntaxregeln für Verbindungsparameter“ auf Seite 36.

- **Fehler** An dieser Stelle kann ein Fehler auftreten, wenn die Verbindungszeichenfolge falsche Syntax bzw. einen unbekannten Verbindungsparameter enthält, oder in der Verbindungszeichenfolge bzw. in SQLCONNECT eine Datenquelle festgelegt wird, die nicht existiert.
- **Ignorierte Parameter** Abhängig von anderen, bereits eingerichteten Verbindungen kann es sein, dass bestimmte Verbindungsparameter ignoriert werden:
  - **AutoStop** Wird ignoriert, wenn die Datenbank bereits geladen ist.
  - **DatabaseFile** Dieser Wert wird ignoriert, wenn "DatabaseName" angegeben wird und eine Datenbank mit diesem Namen bereits ausgeführt wird.

Die Schnittstellenbibliothek verwendet die vollständige Liste der Verbindungsparameter zum Herstellen einer Verbindung.

**Siehe auch**

- [„Syntaxregeln für Verbindungsparameter“ auf Seite 36](#)

**Fehlerbehandlung: Datenbankserver suchen**

Wenn SQL Anywhere einen laufenden Server findet, wird versucht, die verlangte Datenbank auf diesem Server zu finden oder zu starten. Siehe [„Fehlerbehandlung: Datenbankserver suchen“ auf Seite 94](#).

Falls kein laufender Server gefunden wird, kann SQL Anywhere versuchen, abhängig von den Verbindungsparametern einen Personal Server zu starten.

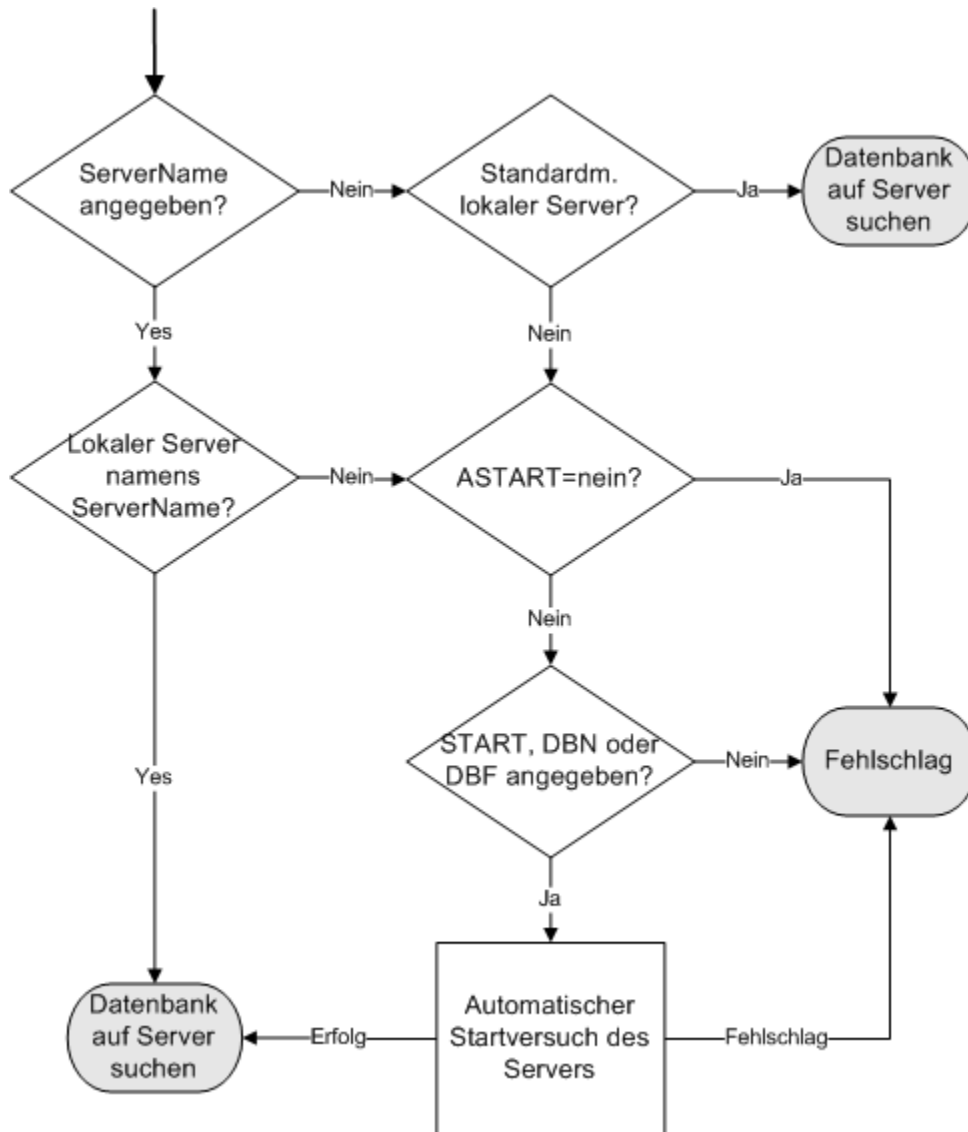
**Hinweis**

- Bei lokalen Verbindungen ist die Ermittlung des Speicherortes eines Servers ein einfacher Vorgang. Bei Verbindungen über ein Netzwerk wird der Host-Verbindungsparameter empfohlen.
- Weitere Hinweise dazu, wie der Client einen Netzwerkserver ermittelt, finden Sie unter [„Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen“ auf Seite 87](#).
- Wenn der Server automatisch gestartet wird, werden Informationen der Verbindungsparameter START, DBF, DBKEY, DBS, DBN, Server und AutoStop verwendet, um die Verbindungsparameter für den automatisch gestarteten Server zu ermitteln. Der Server wird nicht automatisch gestartet, wenn der Verbindungsparameter "Host" oder "CommLinks=TCPIP" angegeben ist.
- Wenn der Server einen alternativen Servernamen hat, können Sie nur den alternativen Servernamen verwenden, um sich mit der Datenbank zu verbinden, die den alternativen Servernamen angegeben hat. Sie können den alternativen Servernamen nicht verwenden, um eine Verbindung mit anderen auf diesem Datenbankserver laufenden Datenbanken herzustellen. Siehe [AS PRIMARY-Klausel](#), [CREATE MIRROR SERVER-Anweisung](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*] und [„Datenbankoption -sn“](#).

Die folgenden Diagramme veranschaulichen, wie SQL Anywhere den Speicherort eines Datenbankservers ermittelt.

**Verbindungszeichenfolge enthält die CommLinks- oder Host-Verbindungsparameter nicht**

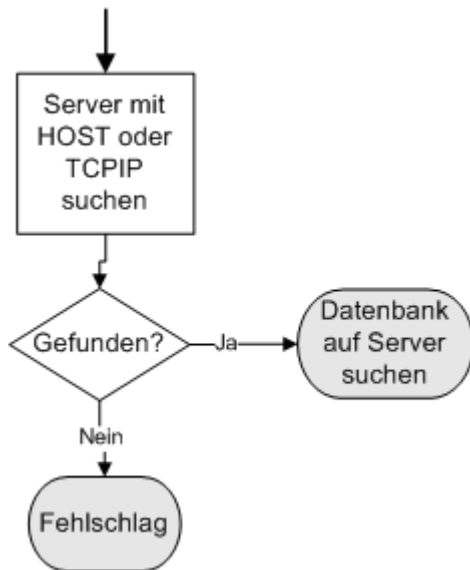
Das folgende Diagramm beschreibt, wie SQL Anywhere den Speicherort einer Datenbank mit Shared Memory ermittelt, wenn die Verbindungszeichenfolge nicht den CommLinks- oder Host-Verbindungsparameter enthält.



Falls kein laufender Server gefunden wird, kann SQL Anywhere versuchen, abhängig von den Verbindungsparametern einen Personal Server zu starten.

### Verbindungszeichenfolge enthält den Host-Verbindungsparameter oder der CommLinks-Verbindungsparameter gibt TCPIP an

Das folgende Diagramm zeigt, wie SQL Anywhere den Speicherort eines Datenbankservers ermittelt, wenn die Verbindungszeichenfolge den Host- oder den CommLinks-Verbindungsparameter enthält und TCPIP angibt.



### Verbindungszeichenfolge enthält einen CommLinks-Verbindungsparameter, der auf ShMem und TCPIP festgelegt ist

Wenn die Verbindungszeichenfolge CommLinks=ShMem, TCPIP oder CommLinks=TCPIP, ShMem ist, geht SQL Anywhere wie folgt vor:

- Eine Shared Memory-Verbindung wird versucht ohne zu versuchen, den Datenbankserver zu starten. Siehe [Verbindungszeichenfolge enthält die CommLinks- oder Host-Verbindungsparameter nicht auf Seite 83](#).

Wenn SQL Anywhere den Server über Shared Memory nicht finden kann, versucht er es mit einer TCPIP-Verbindung. Siehe [Verbindungszeichenfolge enthält den Host-Verbindungsparameter oder der CommLinks-Verbindungsparameter gibt TCPIP an auf Seite 84](#).

### Siehe auch

- „Datenbankserveroption -xd “ auf Seite 307
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- „db\_string\_ping\_server-Funktion“ [*SQL Anywhere Server - Programmierung*]
- „Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen“ auf Seite 87
- „Fehlerbehandlung: Datenbankserver mithilfe des Verbindungsparameters "CommLinks=TCPIP" suchen“ auf Seite 90

## Fehlerbehandlung: Datenbankserver mithilfe des Broadcast Repeater-Dienstprogramms suchen

Mit dem Broadcast Repeater-Dienstprogramm (dbns16) können SQL Anywhere-Clients auch SQL Anywhere-Datenbankserver finden, die in anderen Subnetzen und hinter Firewalls laufen, wo sie von UDP-Broadcasts ohne Host-Verbindungsparameter oder LDAP normalerweise nicht erreicht werden.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Beliebig viele DBNS-Prozesse können miteinander kommunizieren. Jeder DBNS-Prozess verbindet sich mit jedem anderen ihm bekannten DBNS-Prozess, und die verschiedenen DBNS-Prozesse benutzen ihre Listen der DBNS-Prozesse gemeinsam. Sie starten z.B. die beiden DBNS-Prozesse A und B. Wenn Sie einen dritten DBNS-Prozess, C, in einem dritten Subnetz starten, indem Sie die Adresse von B an C weiterleiten, dann informiert B C über A, und schließlich verbindet sich C mit A.

#### Hinweis

Es ist im Allgemeinen nicht notwendig und wird auch nicht empfohlen, mehrere DBNS-Prozesse in einem einzelnen Subnetz auszuführen.

Wenn mehrere DBNS-Prozesse in einem einzelnen Subnetz ausgeführt werden müssen, legen Sie für jeden DBNS-Prozess einen anderen Port fest. Ein einzelner DBNS-Prozess kann nur auf einem Port warten. Verwenden Sie im Broadcast Repeater-Dienstprogramm (dbns16) den Parameter -ap.

Wenn entweder der Host-Verbindungsparameter oder die HOST-Protokolloption verwendet wird, ist das Broadcast Repeater-Dienstprogramm nicht erforderlich.

### Aufgabe

1. Starten Sie einen DBNS-Prozess (Database Name Service) auf einem Computer im Subnetz.
2. Starten Sie einen DBNS-Prozess auf einem Computer in einem anderen Subnetz und übergeben Sie den Computernamen oder die IP-Adresse als Parameter an den ersten Computer.

Die beiden DBNS-Prozesse stellen eine TCP/IP-Verbindung zueinander her.

3. Die DBNS-Prozesse hören nun Broadcasts in ihren jeweiligen Subnetzen ab. Jeder DBNS-Prozess leitet Anforderungen über die TCP/IP-Verbindung an den anderen DBNS-Prozess weiter, der wiederum ein Broadcast der Anforderungen in seinem Subnetz durchführt und auch die Antworten zurück an den Ausgangsprozess leitet, welcher sie an den ursprünglichen Client sendet.

### Ergebnisse

Reguläre SQL Anywhere-Broadcasts auf beiden Subnetzen erreichen Datenbankserver auf dem entfernten Subnetz, und Clients sind in der Lage, sich mit Servern auf dem entfernten Subnetz zu verbinden, ohne den HOST-Parameter anzugeben.

### Siehe auch

- „Broadcast Repeater-Dienstprogramm (dbns16)“ auf Seite 891

## Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen

Ein SQL Anywhere-Client, der versucht, einen Datenbankserver über TCP/IP unter Verwendung der Host-Verbindungsparameter zu finden, führt dabei folgende Schritte aus:

1. [Schritt 1: Überprüfen Sie den Datenbankserver-Adressencache \(sasrv.ini\).](#)
2. [Schritt 2: Versuch einer TCP/IP-Verbindung mit der \(den\) Adresse\(n\), die im Host-Verbindungsparameter angegeben ist/sind.](#)
3. [Schritt 3: UDP-Datenbankserver-Suchanforderungen absetzen.](#)

Wenn der Datenbankserver nicht gefunden wird, teilt das System in einer Meldung mit, dass der Server nicht gefunden wurde. Wenn ein anderer Fehler auftritt, schlägt der Verbindungsversuch fehl, ohne dass weitere Schritte versucht werden. Siehe „[Datenbankserver nicht gefunden](#)“ [[Fehlermeldungen](#)].

Wenn sich der Client mit dem Datenbankserver erfolgreich verbunden hat, versucht er, eine Verbindung mit der Datenbank herzustellen. Siehe „[Fehlerbehandlung: Datenbankserver suchen](#)“ auf Seite 94.

**Schritt 1: Überprüfen Sie den Datenbankserver-Adressencache (sasrv.ini)** Wenn die Verbindungszeichenfolge den Host-Verbindungsparameter enthält, aber nicht den Parameter ServerName, kann der SQL Anywhere-Client die *sasrv.ini*-Datei nicht verwenden. Siehe [Schritt 2: Versuch einer TCP/IP-Verbindung mit der \(den\) Adresse\(n\), die im Host-Verbindungsparameter angegeben ist/sind](#) auf Seite 88.

Der Client überprüft die *sasrv.ini*-Datei auf einen Eintrag, der mit dem Datenbankservernamen übereinstimmt, der vom Verbindungsparameter ServerName festgelegt wird.

Wenn kein übereinstimmender Cacheeintrag gefunden wird, versucht der Client eine direkte TCP/IP-Verbindung. Siehe [Schritt 2: Versuch einer TCP/IP-Verbindung mit der \(den\) Adresse\(n\), die im Host-Verbindungsparameter angegeben ist/sind](#) auf Seite 88.

Wenn ein Cacheeintrag sowohl mit dem Verbindungsparameter ServerName als auch der vom Host-Verbindungsparameter festgelegten Adresse übereinstimmt, versucht der Client eine TCP/IP-Verbindung mit der IP-Adresse, die im Cache gelistet ist.

- Wenn der Client mit dieser IP-Adresse eine Verbindung zum Datenbankserver aufnimmt, vergleicht er den Namen des Datenbankservers mit dem von ServerName angegebenen Wert.

Wenn der Datenbankservername übereinstimmt, kommt die Verbindung erfolgreich zustande.

Wenn der Datenbankservername nicht übereinstimmt, entfernt der Client den Eintrag aus der *sasrv.ini*-Datei und der Client versucht, eine direkte TCP/IP-Verbindung einzurichten. Siehe [Schritt 2: Versuch einer TCP/IP-Verbindung mit der \(den\) Adresse\(n\), die im Host-Verbindungsparameter angegeben ist/sind](#) auf Seite 88.

- Wenn der Client keine Verbindung herstellen kann, entfernt er den Eintrag aus der *sasrv.ini*-Datei und versucht, eine direkte TCP/IP-Verbindung einzurichten. Siehe [Schritt 2: Versuch einer TCP/IP-Verbindung mit der \(den\) Adresse\(n\), die im Host-Verbindungsparameter angegeben ist/sind](#) auf Seite 88.

**Hinweis**

Der Dateiname für den Datenbankserver-Adressencache ist unter Unix *.sasrv.ini*. Siehe [„Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in sasrv.ini zwischenspeichern“](#) auf Seite 94.

**Schritt 1: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152.

Für die Verbindungszeichenfolge `Host=kangaroo;ServerName=joey` findet der Client einen Eintrag in seiner *sasrv.ini*-Datei, der mit dem Servernamen joey übereinstimmt. Die IP-Adresse im Cache ist 10.25.13.5:49152. Der Client vergleicht die Adresse des angegebenen Hostnamens mit 10.25.13.5. Die Adressen stimmen überein, sodass der Client eine Verbindung über TCP/IP mit 10.25.13.5:49152 einrichtet und dann prüft, ob der verbundene Server joey heißt. Die Verbindung ist erfolgreich.

**Schritt 2: Versuch einer TCP/IP-Verbindung mit der (den) Adresse(n), die im Host-Verbindungsparameter angegeben ist/sind** Wenn mehrere Adressen angegeben werden, versucht der Client, sich mit jeder Adresse in der Reihenfolge zu verbinden, in der sie im Host-Verbindungsparameter angegeben werden. Der Client versucht, Verbindungen aufzunehmen, bis eine Verbindung erfolgreich ist oder alle Adressen aufgebraucht sind.

Wenn eine Adresse einen Port enthält, versucht der Client eine TCP/IP-Verbindung mit der angegebenen Adresse und Portnummer. Wenn kein Port angegeben ist, versucht der Client eine TCP/IP-Verbindung an der angegebenen Adresse über den Standardport 2638.

- Wenn der Client eine Verbindung mit dem Datenbankserver herstellt und `ServerName` angegeben ist, vergleicht der Client den Namen des Datenbankservers mit dem von `ServerName` angegebenen Wert. Wenn der Datenbankservername übereinstimmt, kommt die Verbindung erfolgreich zustande. Der Client aktualisiert seine *sasrv.ini*-Datei. Wenn der Datenbankservername nicht übereinstimmt, versucht der Client eine Verbindung über UDP-Serversuchanforderungen. Siehe [Schritt 3: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 89](#).
- Wenn der Client eine Verbindung mit dem Datenbankserver herstellt und `ServerName` nicht angegeben wurde, kommt die Verbindung erfolgreich zustande.
- Wenn der Client keine Verbindung herstellen kann und ein `ServerName`-Parameter angegeben ist, versucht der Client eine Verbindung über UDP-Serversuchanforderungen. Siehe [Schritt 3: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 89](#).
- Wenn der Client keine Verbindung herstellen kann und der `ServerName`-Parameter nicht angegeben wurde, schlägt die Verbindung fehl.

**Schritt 2: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152. Dies ist das erste Mal, dass sich der Client mit diesem Server verbindet, daher gibt es keine im Cache gespeicherte Adresse in seiner *sasrv.ini*-Datei.

Für die Verbindungszeichenfolge `Host=kangaroo:49152;ServerName=joey` verbindet sich der Client über TCP/IP mit 10.25.13.5:49152 und prüft dann, ob der verbundene Server joey heißt. Die Verbindung ist erfolgreich, daher aktualisiert der Client seine *sasrv.ini*-Datei.

**Schritt 3: UDP-Datenbankserver-Suchanforderungen absetzen** Der SQL Anywhere-Client sendet UDP-Datenbankserver-Suchanforderungen nur aus, wenn die Verbindungszeichenfolge den `ServerName`-Verbindungsparameter enthält und der `Host`-Wert keinen Port angibt. UDP-Serversuchanforderungen werden an Port 2638 auf der angegebenen Adresse gesendet.

Standardmäßig warten alle Datenbankserver auf demselben Computer (außer bei Mac OS X) auf Port 2638 auf UDP-Pakete. Unter Mac OS X kann nur ein Server auf Port 2638 auf UDP-Pakete warten. Wenn ein Datenbankserver eine UDP-Serversuchanforderung empfängt, vergleicht der Datenbankserver seinen Namen mit dem angegebenen Namen in der UDP-Anforderung. Wenn die Namen übereinstimmen, sendet der Datenbankserver ein UDP-Antwortpaket zurück, das seine IP-Adresse und die Portnummer enthält. Nur der übereinstimmende Datenbankserver sendet ein Antwortpaket.

Standardmäßig wartet der Client bis zu fünf Sekunden auf eine UDP-Antwort. Wenn keine Antworten ankommen, werden die UDP-Pakete jede Sekunde erneut gesendet, bis bei diesem Prozess eine Zeitüberschreitung eintritt.

Wenn der Client das UDP-Antwortpaket empfängt, versucht der Client eine TCP/IP-Verbindung mit der Adresse und dem Port, die im Paket angegeben sind.

Wenn sich der Client mit einem Datenbankserver verbinden kann, kommt die Verbindung erfolgreich zustande. Der Client aktualisiert seine *sasrv.ini*-Datei.

#### Hinweis

UDP-Pakete können folgende Datenbankserver nicht finden:

- Einen Datenbankserver unter Mac OS X, der nicht am Port 2638 auf Verbindungen wartet. Siehe [„ServerPort-Protokolloption \(PORT\)“ auf Seite 416](#).
- Einen Datenbankserver, der mit der Option `-sb 0` gestartet wurde. Siehe [„Datenbankserveroption -sb“ auf Seite 278](#).
- Einen Datenbankserver, dessen UDP-Anforderungen durch eine Firewall, einen Router oder ein Gateway blockiert sind. Siehe [„Firewall-Verbindungen“ auf Seite 107](#).

In beiden Fällen müsste die Angabe des Ports des Datenbankservers im `Host`-Verbindungsparameter eine erfolgreiche Verbindung des Clients ermöglichen.

**Schritt 3: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152. Dies ist das erste Mal, dass sich der Client mit diesem Server verbindet, daher gibt es keine im Cache gespeicherte Adresse in seiner *sasrv.ini*-Datei.

Mit der Verbindungszeichenfolge `Host=kangaroo;ServerName=joey` hat der Client versucht, eine Verbindung über TCP/IP zu 10.25.13.5:2638 aufzunehmen und der Versuch ist fehlgeschlagen (Schritt 2). Da in der Verbindungszeichenfolge keine Portnummer angegeben wurde, sendet der Client

UDP-Serversuchanforderungen an die Adresse 10.25.13.5:2638. Der Datenbankserver joey wartet an der UDP-Adresse 10.25.13.5.2638 auf Verbindungen und antwortet mit der Adresse 10.25.13.5:49152. Der Client stellt eine Verbindung über TCP/IP mit 10.25.13.5:49152 her. Die Verbindung ist erfolgreich, daher aktualisiert der Client seine *sasrv.ini*-Datei.

## Fehlerbehandlung: Datenbankserver mithilfe des Verbindungsparameters "CommLinks=TCPIP" suchen

### Hinweis

Sie sollten den CommLinks-Verbindungsparameter (LINKS) nur dann verwenden, wenn Sie andere TCP/IP-Protokolloptionen als HOST oder ServerPort (PORT) angeben müssen. Verwenden Sie andernfalls den Host-Verbindungsparameter. Siehe „[Host-Verbindungsparameter](#)“ auf Seite 363.

Sie können nicht sowohl CommLinks als auch Host in der Verbindungszeichenfolge angeben.

Der Host-Verbindungsparameter unterscheidet sich von der HOST-Protokolloption. Die HOST-Protokolloption wird vom CommLinks-Verbindungsparameter verwendet. Siehe „[Host-Protokolloption \(IP\) \(nur clientseitig\)](#)“ auf Seite 399.

Ein SQL Anywhere-Client, der versucht, einen Server über TCP/IP unter Verwendung der CommLinks-Verbindungsparameter zu finden, führt dabei folgende Schritte aus:

1. [Schritt 1: Überprüfen Sie den Datenbankserver-Adressencache \(sasrv.ini\) auf Seite 90.](#)
2. [Schritt 2: Im LDAP-Server den Servernamen abfragen auf Seite 91.](#)
3. [Schritt 3: Versuchen, eine TCP/IP-Verbindung mit der/den in der HOST-Protokolloption angegebenen Adresse\(n\) herzustellen auf Seite 91.](#)
4. [Schritt 4: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 92.](#)

Wenn der Datenbankserver nicht gefunden wird, teilt das System in einer Meldung mit, dass der Server nicht gefunden wurde. Wenn ein anderer Fehler auftritt, schlägt der Verbindungsversuch fehl, ohne dass weitere Schritte versucht werden. Siehe „[Datenbankserver nicht gefunden](#)“ [[Fehlermeldungen](#)].

Wenn sich der Client mit dem Datenbankserver erfolgreich verbunden hat, versucht er, eine Verbindung mit der Datenbank herzustellen. Siehe „[Fehlerbehandlung: Datenbankserver suchen](#)“ auf Seite 94.

**Schritt 1: Überprüfen Sie den Datenbankserver-Adressencache (sasrv.ini)** Wenn die Verbindungszeichenfolge die HOST-Protokolloption, nicht aber den ServerName-Verbindungsparameter enthält, wird die LocalOnly-Protokolloption auf YES oder die DoBroadcast-Protokolloption auf NONE gesetzt. Danach versucht der SQL Anywhere-Client eine direkte TCP/IP-Verbindung. Das heißt, dass der SQL Anywhere-Client nicht den Datenbankserver-Adressencache oder den LDAP-Server verwendet. Siehe [Schritt 3: Versuchen, eine TCP/IP-Verbindung mit der/den in der HOST-Protokolloption angegebenen Adresse\(n\) herzustellen auf Seite 91.](#)

Der Client überprüft die *sasrv.ini*-Datei auf einen Eintrag, der mit dem Datenbankservernamen übereinstimmt, der vom Verbindungsparameter ServerName festgelegt wird. Wenn die

Verbindungszeichenfolge auch die HOST-Protokolloption enthält, muss der Cacheeintrag ebenfalls mit der angegebenen Hostadresse übereinstimmen.

Wenn kein übereinstimmender Cacheeintrag gefunden wird, versucht der Client, den Datenbankserver mit LDAP zu finden. Siehe [Schritt 2: Im LDAP-Server den Servernamen abfragen auf Seite 91](#).

Wenn ein entsprechender Cacheeintrag gefunden wird, versucht der Client eine TCP/IP-Verbindung mit der IP-Adresse, die im Cache gelistet ist.

- Wenn der Client eine Verbindung zum Datenbankserver über diese IP-Adresse aufnimmt und die VerifyServer-Protokolloption nicht aktiviert ist, kommt die Verbindung zustande. Siehe [„VerifyServerName-Protokolloption \(VERIFY\) \(nur clientseitig\)“ auf Seite 422](#).
- Wenn der Client eine Verbindung zum Datenbankserver über diese IP-Adresse aufnimmt und VerifyServer auf Ja gesetzt ist (Standardwert), vergleicht der Client den Datenbankservernamen mit dem von ServerName angegebenen Wert. Wenn der Datenbankservername übereinstimmt, kommt die Verbindung erfolgreich zustande. Wenn der Datenbankservername nicht übereinstimmt, entfernt der Client den Eintrag aus der *sasrv.ini*-Datei und der Client versucht, den Datenbankserver direkt über TCP/IP mit LDAP zu finden. Siehe [Schritt 2: Im LDAP-Server den Servernamen abfragen auf Seite 91](#).
- Wenn der Client keine Verbindung herstellen kann, entfernt er den Eintrag aus seiner *sasrv.ini*-Datei und versucht, den Datenbankserver mit LDAP zu finden. Siehe [Schritt 2: Im LDAP-Server den Servernamen abfragen auf Seite 91](#).

#### Hinweis

Der Dateiname für den Datenbankserver-Adressencache ist unter Unix *.sasrv.ini*. Siehe [„Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in sasrv.ini zwischenspeichern“ auf Seite 94](#).

**Schritt 1: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152.

Für die Verbindungszeichenfolge `CommLinks=TCPIP(Host=kangaroo);ServerName=joey` findet der Client einen Eintrag in seiner *sasrv.ini*-Datei, der mit dem Servernamen joey übereinstimmt. Die IP-Adresse im Cache ist 10.25.13.5:49152. Der Client vergleicht die Adresse des angegebenen Hostnamens mit 10.25.13.5. Die Adressen stimmen überein, sodass der Client eine Verbindung über TCP/IP mit 10.25.13.5:49152 einrichtet und dann prüft, ob der verbundene Server joey heißt. Die Verbindung ist erfolgreich.

**Schritt 2: Im LDAP-Server den Servernamen abfragen** Ein SQL Anywhere-Client fragt im LDAP-Server einen Eintrag ab, der mit dem ServerName-Verbindungsparameter übereinstimmt, wenn die Computer, auf denen der SQL Anywhere-Client und der Datenbankserver laufen, so konfiguriert sind, dass sie einen LDAP-Server verwenden. Siehe [„Verbindungen mit LDAP als Namensserver“ auf Seite 109](#).

**Schritt 3: Versuchen, eine TCP/IP-Verbindung mit der/den in der HOST-Protokolloption angegeben Adresse(n) herzustellen** Wenn die HOST-Protokolloption nicht angegeben ist, versucht

der SQL Anywhere-Client, den Server mithilfe von UDP-Serversuchanforderungen zu finden. Siehe [Schritt 4: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 92](#).

Der SQL Anywhere-Client versucht, eine Verbindung über TCP/IP mit den in der HOST-Protokolloption angegebenen Adressen herzustellen. Wenn mehrere Adressen angegeben sind, versucht der Client, sich mit jeder Adresse in der Reihenfolge zu verbinden, in der sie in der HOST-Protokolloption angegeben werden. Der Client versucht, Verbindungen herzustellen, bis eine Verbindung erfolgreich ist oder alle Adressen aufgebraucht sind.

Wenn die Verbindungszeichenfolge einen Port (in der HOST-Protokolloption oder in der ServerPort-Verbindungseigenschaft) enthält, versucht der Client, eine TCP/IP-Verbindung mit der angegebenen Adresse und Portnummer herzustellen. Wenn kein Port angegeben ist, versucht der Client eine TCP/IP-Verbindung an der angegebenen Adresse über den Standardport 2638.

- Wenn der Client eine Verbindung zum Datenbankserver über die angegebene IP-Adresse aufnimmt und die VerifyServer-Protokolloption nicht aktiviert ist, kommt die Verbindung zustande. Siehe [„VerifyServerName-Protokolloption \(VERIFY\) \(nur clientseitig\)“ auf Seite 422](#).
- Wenn der Client über die angegebene Adresse eine Verbindung mit dem Datenbankserver herstellt, vergleicht der Client den Namen des Datenbankservers mit dem von ServerName angegebenen Wert. Wenn der Datenbankservername übereinstimmt, kommt die Verbindung zustande und der Client aktualisiert seine *sasrv.ini*-Datei. Wenn der Datenbankservername nicht übereinstimmt, versucht der Client eine Verbindung über UDP-Serversuchanforderungen. Siehe [Schritt 4: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 92](#).
- Wenn der Client keine Verbindung herstellen kann und ein ServerName-Parameter angegeben ist, versucht der Client eine Verbindung über UDP-Serversuchanforderungen. Siehe [Schritt 4: UDP-Datenbankserver-Suchanforderungen absetzen auf Seite 92](#).
- Wenn der Client keine Verbindung herstellen kann und der ServerName-Parameter nicht angegeben wurde, schlägt die Verbindung fehl.

**Schritt 3: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152. Dies ist das erste Mal, dass sich der Client mit diesem Server verbindet, daher gibt es keine im Cache gespeicherte Adresse in seiner *sasrv.ini*-Datei.

Für die Verbindungszeichenfolge `CommLinks=TCPIP(Host=kangaroo:49152);ServerName=joey` verbindet sich der Client über TCP/IP mit 10.25.13.5:49152 und prüft dann, ob der verbundene Server joey heißt. Die Verbindung ist erfolgreich, daher aktualisiert der Client seine *sasrv.ini*-Datei.

**Schritt 4: UDP-Datenbankserver-Suchanforderungen absetzen** Der SQL Anywhere-Client sendet UDP-Datenbankserver-Suchanforderungen nur aus, wenn die Verbindungszeichenfolge den ServerName-Verbindungsparameter enthält und die DoBroadcast-Protokolloption auf DIRECT oder ALL eingestellt ist.

- Wenn "DoBroadcast=DIRECT" eingestellt ist oder die HOST-Protokolloption angegeben wurde, sendet der Client UDP-Serversuchpakete an die angegebene(n) Adresse(n). Wenn ein Port angegeben ist (in der HOST-Protokolloption oder der ServerPort-Protokolloption), wird die UDP-

Serversuchanforderung an den angegebenen Port gesendet. Andernfalls wird die Anforderung an den Standardport 2638 gesendet.

- Wenn "DoBroadcast=ALL" eingestellt ist und keine HOST-Protokolloption angegeben wurde, ermittelt der Client die Broadcast-Adresse des Subnetzes für jede IP-Adresse. Wenn die ServerPort-Protokolloption angegeben ist, sendet der Client UDP-Broadcast-Serversuchpakete an den angegebenen Port. Andernfalls werden die UDP-Broadcast-Pakete an den Standardport 2638 gesendet.

Außer wenn beim Start des Datenbankservers die Option -sb 0 Option angegeben wurde, warten alle Datenbankserver am Port 2638 auf UDP-Pakete. Wenn ein Datenbankserver eine UDP-Serversuchanforderung empfängt, vergleicht der Datenbankserver seinen Namen mit dem angegebenen Namen im Anforderungspaket. Wenn die Namen übereinstimmen, sendet der Datenbankserver ein UDP-Antwortpaket zurück, das seine IP-Adresse und die Portnummer enthält. Nur der übereinstimmende Datenbankserver sendet ein Antwortpaket.

Standardmäßig wartet der Client bis zu fünf Sekunden auf eine UDP-Antwort. Wenn keine Antworten ankommen, werden die UDP-Pakete jede Sekunde erneut gesendet, bis bei diesem Prozess eine Zeitüberschreitung eintritt.

Wenn der Client das UDP-Antwortpaket empfängt, versucht der Client eine TCP/IP-Verbindung mit der Adresse und dem Port, die im Paket angegeben sind.

Wenn sich der Client mit einem Datenbankserver verbinden kann, kommt die Verbindung erfolgreich zustande. Der Client aktualisiert seine *sasrv.ini*-Datei.

#### Hinweis

UDP-Pakete können folgende Datenbankserver nicht finden:

- Einen Datenbankserver, der sich in einem anderen Subnetz befindet. UDP-Serversuch-Broadcast-Pakete können den Datenbankserver nur finden, wenn das Broadcast Repeater-Dienstprogramm verwendet wird. Siehe „Broadcast Repeater-Dienstprogramm (dbns16)“ auf Seite 891.
- Einen Datenbankserver unter Mac OS X, der nicht am Port 2638 auf Verbindungen wartet. Siehe „ServerPort-Protokolloption (PORT)“ auf Seite 416.
- Einen Datenbankserver, der mit der Option -sb 0 gestartet wurde. Siehe „Datenbankserveroption -sb“ auf Seite 278.
- Einen Datenbankserver, dessen UDP-Anforderungen durch eine Firewall, einen Router oder ein Gateway blockiert sind. Siehe „Firewall-Verbindungen“ auf Seite 107.

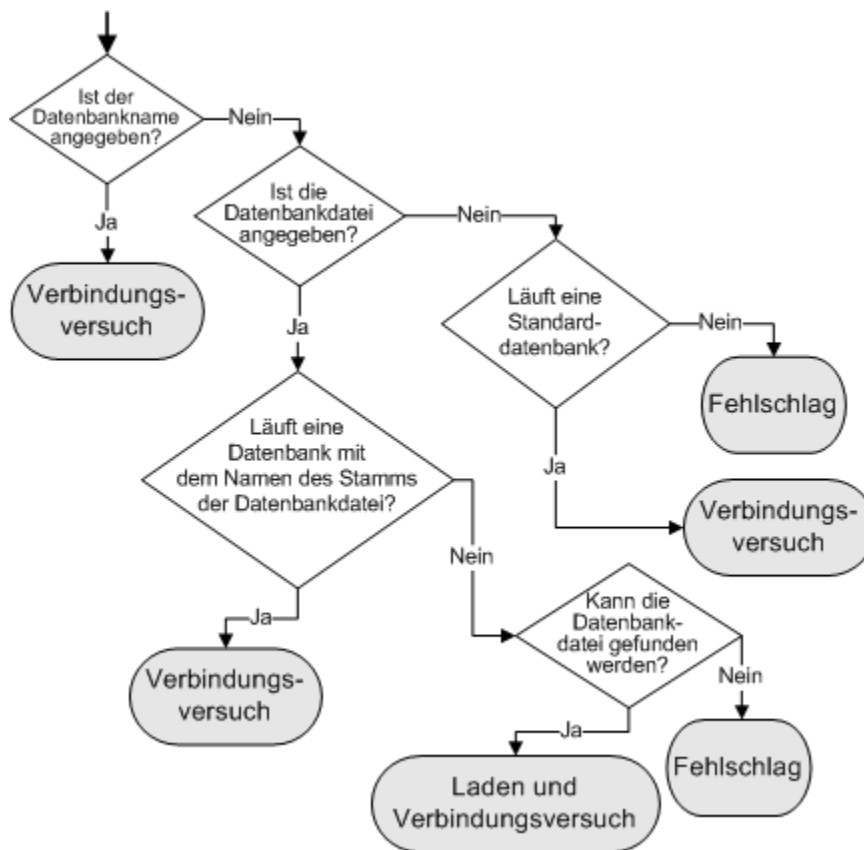
In beiden Fällen sollte die Angabe der Adresse des Datenbankservers (einschließlich der Portnummer) in der HOST-Protokolloption eine erfolgreiche Verbindung des Clients ermöglichen.

**Schritt 4: Beispiel** Angenommen, es gibt einen Computer mit dem Hostnamen kangaroo und der IP-Adresse 10.25.13.5. Ein Datenbankserver namens joey läuft auf diesem Computer auf Port 49152. Dies ist das erste Mal, dass sich der Client mit diesem Server verbindet, daher gibt es keine im Cache gespeicherte Adresse in seiner *sasrv.ini*-Datei. Die Verbindung wird von einem PC auf demselben Subnetz wie kangaroo versucht und die Broadcast-Adresse für dieses Subnetz ist 10.25.13.255.

Für die Verbindungszeichenfolge `CommLinks=TCPIP;ServerName=joeys` sendet der Client UDP-Server-Broadcast-Anforderungen an die Broadcast-Adresse 10.25.13.255:2638. Der Datenbankserver joeey wartet an der UDP-Adresse 10.25.13.5.2638 auf Verbindungen und antwortet mit der Adresse 10.25.13.5:49152. Der Client stellt eine Verbindung über TCP/IP mit 10.25.13.5:49152 her. Die Verbindung ist erfolgreich, daher aktualisiert der Client seine *sasrv.ini*-Datei.

## Fehlerbehandlung: Datenbankserver suchen

Nachdem ein Server gefunden wurde, versuchen SQL Anywhere-Programme, die Datenbank zu finden.



## Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in *sasrv.ini* zwischenspeichern

Wenn Sie die Host- oder CommLinks-Verbindungsparameter verwenden, kann die Aufnahme mehrerer TCP/IP-Verbindungen oder ein Broadcast über große Netzwerke zur Suche nach einem Datenbankserver eines bestimmten Namens sehr zeitraubend sein. Das Caching von Datenbankserveradressen im Cache durch Speichern der folgenden Informationen in der *sasrv.ini*-Datei für nachfolgende Verbindungen kann die Netzwerkverbindungen beschleunigen:

- Datenbankservername
- IP-Adresse des Datenbankservers

Die Cachedatei enthält Abschnitte, die jeweils folgendes Format haben:

```
[Server name]
LINK=TCPIP
Address=IP_address:port
```

#### Hinweis

Es ist von größter Wichtigkeit, dass jeder Datenbankserver einen eindeutigen Namen erhält. Wenn Sie mehreren Datenbankservern denselben Namen geben, kann es zu Identifizierungsproblemen kommen.

### Wie der Datenbankserver-Adressencache (*sasrv.ini*) verwendet wird

Eine Beschreibung der Verwendung der Datei *sasrv.ini* finden Sie unter [„Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen“](#) auf Seite 87 und [„Fehlerbehandlung: Datenbankserver mithilfe des Verbindungsparameters "CommLinks=TCPIP" suchen“](#) auf Seite 90.

### Speicherort der Datei *sasrv.ini*

Der Standardspeicherort der Datei *sasrv.ini* ist:

Betriebssystem	Standardspeicherort der <i>sasrv.ini</i>
Windows	%BENUTZERPROFILE%\Anwendungsdaten\SQL Anywhere 16
Windows Mobile	Das Verzeichnis der Programmdatei, die ausgeführt wird.
Unix	<i>\$HOME/.sqlanywhere16</i>  Unter Unix heißt die Datenbankserver-Cachedatei <i>.sasrv.ini</i> .

### Siehe auch

- [„Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in \*sasrv.ini\* zwischenspeichern“](#) auf Seite 94
- [„Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen“](#) auf Seite 87
- [„Fehlerbehandlung: Datenbankserver mithilfe des Verbindungsparameters "CommLinks=TCPIP" suchen“](#) auf Seite 90

## Fehlerbehandlung: Verbindungszeichenfolgen testen (dbping)

Verwenden Sie das Dienstprogramm dbping, um Fehler in Verbindungen zu suchen.

Sie können das Dienstprogramm dbping mit der Option -c verwenden, um Parameter von Verbindungszeichenfolgen zu testen. Standardmäßig stellt dbping keine Verbindung mit einer Datenbank her, sondern nur mit dem Server, wobei dieser aber nicht gestartet wird. Verwenden Sie das Dienstprogramm dbping mit der Option -d, um eine Verbindung mit der Datenbank herzustellen und, falls erforderlich, den Datenbankserver zu starten.

Beispiele

Beispiel: Ein Personal Server namens "demo16" führt die Beispieldatenbank aus (die mit dem Befehl `dbeng16 -n demo16 "%SQLANYAMP16%\demo.db"` gestartet werden kann). Der folgende Befehl gibt eine Meldung über erfolgreiches Pingen der Datenbank zurück, wenn auf dem lokalen Computer ein Datenbankserver namens demo16 läuft, der eine Datenbank namens demo ausführt:

```
dbping -d -c "Server=demo16;DBN=demo;UID=DBA;PWD=sql"
```

Mit dem folgenden Befehl wird geprüft, ob ein Datenbankserver namens demo16 mit der Datenbank namens demo läuft, und der Server und die Datenbank werden gestartet, falls sie nicht laufen:

```
dbping -d -c "Server=demo16;DBN=demo;DBF=c:\sa16\samples\demo.db;ASTOP=no;UID=DBA;PWD=sql"
```

Mit dem folgenden Befehl wird geprüft, ob ein Datenbankserver auf einem Computer mit dem Namen "Waterloo" am Standardport 2638 gefunden werden kann:

```
dbping -c "Host=Waterloo"
```

Mit dem folgenden Befehl wird geprüft, ob ein Standarddatenbankserver auf dem aktuellen Computer verfügbar ist.

```
dbping
```

Siehe auch

- [„Ping-Dienstprogramm \(dbping\)“ auf Seite 955](#)
- [„Fehlerbehandlung: Leistungsfähigkeit von Embedded SQL- und Netzwerkverbindung testen \(dbping\)“ auf Seite 96](#)

Fehlerbehandlung: Leistungsfähigkeit von Embedded SQL- und Netzwerkverbindung testen (dbping)

Sie können das Dienstprogramm Ping (dbping) verwenden, um Informationen über die Performance von Embedded SQL-Verbindungen und die Netzwerkperformance zu erhalten, indem Sie die Option -s oder -t angeben. Die folgenden Statistiken werden gesammelt:

Statistik	Beschreibung
DBLib-Verbindungsherstellung und Verbindungsabbruch	Die Zeit, um eine DBLib-Verbindungsherstellung und einen Verbindungsabbruch durchzuführen. Die Performance von Verbindungsherstellung und Verbindungsabbruch ist bei der Verwendung von anderen Schnittstellen (wie ODBC) üblicherweise langsamer als DBLib, weil mehr Anforderungen benötigt werden, um die Verbindungsherstellung abzuschließen.

Statistik	Beschreibung
Roundtrip - einfache Anforderung	Die erforderliche Zeit, um eine Anforderung vom Client an den Server zu senden, plus der erforderlichen Zeit, um eine Antwort vom Server zurück an den Client zu senden. Die Roundtrip-Zeit ist das Doppelte der durchschnittlichen Verarbeitungszeit (Latenz).
Durchsatz senden	Der Durchsatz, der auf der Übertragung von 100 kB von Daten bei jeder Wiederholung von "dbping" zum Datenbankserver basiert.
Durchsatz empfangen	Der Durchsatz, der auf der Übertragung von 100 kB von Daten bei jeder Wiederholung vom Datenbankserver zu "dbping" basiert.

Wenn Ihr Netzwerk sowohl hohe Roundtrip-Zeiten als auch einen hohen Durchsatz hat, wird der gemeldete Durchsatz aufgrund der hohen Roundtrip-Zeiten niedriger als Ihr tatsächlicher Netzwerkdurchsatz sein. Die Verwendung von "dbping -s" kann als Hinweis nützlich sein, ob eine Kommunikationskomprimierung die Performance steigern würde. Die Performancestatistiken sind angenäherte Statistiken. Sie sind genauer, wenn sowohl der Client- und der Servercomputer verhältnismäßig untätig sind. Die übertragenen Daten können auf ca. 25% ihrer Originalgröße komprimiert werden, wenn eine Kommunikationskomprimierung verwendet wird:

Das Folgende ist ein Beispiel für die Ausgabe von dbping -s für den dbping-Befehl:

```
dbping -s -c "UID=DBA;PWD=sql;Host=localhost;Server=demo16"
```

```
SQL Anywhere-Dienstprogramm Server-Ping, Version 16.0.0.1403
Verbunden mit SQL Anywhere 16.0.0.1403 Server "demo16" und Datenbank "demo".
Performancestatistik
```

	Nummer	Gesamtzeit	Mittel
-----	-----	-----	-----
DBLib - Verbinden u. Trennen	200 mal	512 ms	2 ms
Roundtrip/einfache Anforderung	22100 Anforderungen	1024 ms	<1 ms
Durchsatz senden	267500 KB	1024 ms	261230 KB/s
Durchsatz empfangen	230400 KB	1024 ms	225000 KB/s
Ping der Datenbank erfolgreich.			

#### Siehe auch

- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „Fehlerbehandlung: Verbindungszeichenfolgen testen (dbping)“ auf Seite 95

## Fehlerbehandlung: Kompatible Protokolloptionen für Client und Datenbankserver

Vergewissern Sie sich, dass der Client und der Datenbankserver dasselbe Protokoll verwenden.

- **Shared Memory-Protokoll** Wenn der Client und der Datenbankserver auf demselben Computer laufen, wird Shared Memory (Standardprotokoll) empfohlen.
- **TCP/IP-Protokoll** Wenn sich Client und Datenbankserver auf verschiedenen Computern befinden, müssen Sie TCP/IP verwenden. Der Netzwerkserver (dbsrv16) lässt standardmäßig TCP/IP-Verbindungen zu. Der Personal Server (dbeng16) lässt standardmäßig keine TCP/IP-Verbindungen

zu. Der Personal Server akzeptiert lokale (aber nicht entfernte) TCP/IP-Verbindungen, wenn Sie die Option `-x tcpip` angeben. Clients verwenden den Host- oder CommLinks-Verbindungsparameter, um TCP/IP-Verbindungen zum Datenbankserver herzustellen.

### Siehe auch

- „Datenbankserveroption `-x`“ auf Seite 305
- „Host-Verbindungsparameter“ auf Seite 363
- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345

## Fehlerbehandlung: Allgemeine Verbindungsprobleme und Lösungen

In der folgenden Liste finden Sie einige häufig auftretende Probleme und mögliche Lösungen.

Wenn Sie beim Verbindungsversuch eine Fehlermeldung erhalten, wonach der Datenbankserver nicht gefunden werden kann, konnte der Client den Datenbankserver im Netzwerk nicht finden.

Prüfen Sie folgende Bedingungen:

- Geben Sie den Servernamen in der Verbindungszeichenfolge an.

#### Hinweis

Auf Ihrem Computer wird eventuell Software ausgeführt, die einen eingebetteten SQL Anywhere-Server enthält. Es kann also sein, dass mehrere Server gleichzeitig ausgeführt werden, ohne dass Sie es wissen. Geben Sie daher immer den Servernamen an (`ServerName=Servername`).

- Bei entfernten Datenbankservern wird empfohlen, dass Sie den Host-Verbindungsparameter angeben und den TCP/IP-Hostnamen oder die Adresse des Computers übergeben, auf dem der Datenbankserver läuft. Prüfen Sie, ob die angegebene Adresse richtig ist. Wenn der Server einen anderen Port als den Standardport 2638 verwendet, müssen Sie möglicherweise `Host=TCPIP-Adresse:Portnummer` angeben.

Wenn Sie den erweiterten CommLinks-Verbindungsparameter verwenden, erreichen die für die Datenbankserverversuche verwendeten Pakete eventuell den Datenbankserver nicht. Es wird empfohlen, dass Sie den Host-Verbindungsparameter verwenden, außer wenn Sie andere TCP/IP-Protokolloptionen außer Host, ServerPort oder DoBroadcast benötigen. Wenn Sie den CommLinks-Verbindungsparameter ohne Angabe der HOST-Protokolloption verwenden, werden UDP-Broadcasts oder -Anforderungen möglicherweise auf das aktuelle Subnetz beschränkt oder durch einen Router, ein Gateway oder eine Firewall blockiert.

- Eine Firewall zwischen dem Client und dem Server kann die Verbindung behindern.
- Der Personal Server kann nur Verbindungen akzeptieren, die auf demselben Computer ausgeführt werden. Wenn sich Client und Server auf verschiedenen Computern befinden, müssen Sie den Netzwerkserver verwenden.
- Ihre Netzwerktreiber sind nicht richtig installiert, oder die Netzwerkverkabelung wurde nicht fachmännisch ausgeführt. Verwenden Sie das Ping-Dienstprogramm, um zu prüfen, ob der Clientcomputer mit dem Servercomputer kommunizieren kann.

- Der Server muss das TCP/IP-Protokoll verwenden, wenn Sie sich über jConnect oder Sybase Open Client verbinden.
- Wenn Sie ein Administrationstool, ODBC oder das OLE DB-Fenster **Verbinden** verwenden und eine Verbindung mit einem Datenbankserver auf Ihrem lokalen Computer herstellen möchten, klicken Sie im Fenster **Verbinden** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**. Sie können auf **Mit einer Datenbank auf einem anderen Computer verbinden** klicken, wenn Sie sich mit einem Datenbankserver verbinden möchten, der nicht auf Ihrem lokalen Computer läuft.

#### Siehe auch

- „Fehlerbehandlung: Verbindungen“ auf Seite 79
- „Fehlerbehandlung beim Datenbankserverstart“ auf Seite 1109
- „Datenbankserver nicht gefunden“ [*Fehlermeldungen*]
- „Host-Verbindungsparameter“ auf Seite 363
- „Firewall-Verbindungen“ auf Seite 107
- „Netzwerkprotokolloptionen“ auf Seite 388

## Verbundene Benutzer verwalten

In Sybase Central können Sie alle Benutzer überwachen, die eine Verbindung mit der Datenbank hergestellt haben. Sie können Eigenschaften dieser verbundenen Benutzer anzeigen und deren Verbindungen trennen.

#### Voraussetzungen

Sie müssen das Systemprivileg DROP CONNECTION, MONITOR oder SERVER OPERATOR haben.

#### Kontext und Bemerkungen

Sie können auch eine Liste aller mit einer Datenbank verbundenen Benutzer im **Verbindungen**-Widget im SQL Anywhere-Monitor anzeigen.

#### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Zeigen Sie eine Liste aller mit der Datenbank verbundenen Benutzer an.
  - a. Markieren Sie eine Datenbank im linken Fensterausschnitt und öffnen Sie die Registerkarte **Verbindungen** im rechten Fensterausschnitt.

Diese Registerkarte enthält alle Benutzer, die derzeit mit der Datenbank verbunden sind. Dies ist unabhängig von der für die Verbindung benutzten Anwendung (Sybase Central, Interactive SQL oder eine angepasste Clientanwendung).
3. Prüfen Sie die Eigenschaften für die Verbindung eines Benutzers mit einer Datenbank.
  - a. Rechtsklicken Sie auf der Registerkarte **Verbindungen** auf den Benutzer und klicken Sie dann auf **Eigenschaften**.

- b. Überprüfen Sie die Eigenschaften für den Benutzer und klicken Sie auf **OK**.

### Ergebnisse

Die Eigenschaften der verbundenen Benutzer werden überprüft.

### Nächste Schritte

Sie können die Verbindung eines Benutzers mit der Datenbank trennen.

### Siehe auch

- [„Widgets“ auf Seite 1127](#)

## Verbindungen mit Datenbanken trennen (Sybase Central)

In Sybase Central können Sie für sich selbst oder andere Benutzer die Verbindung mit einer Datenbank trennen.

### Voraussetzungen

Sie benötigen keine Privilegien, um Ihre Verbindung mit der Datenbank zu trennen.

Sie müssen das DROP CONNECTION-Systemprivileg haben, um Verbindungen anderer Benutzer zu trennen.

### Aufgabe

- Stellen Sie eine Verbindung mit der Datenbank her.

Option	Aktion
Verbindung des aktuellen Benutzers trennen	Klicken Sie auf <b>Datei » Trennen</b> .
Verbindungen anderer Benutzer trennen	Klicken Sie im rechten Fensterausschnitt auf die Registerkarte <b>Verbindungen</b> .  Rechtsklicken Sie auf einen Benutzer und klicken Sie dann auf <b>Verbindung trennen</b> .

### Ergebnisse

Die Verbindung des Benutzers mit der Datenbank wird getrennt.

### Siehe auch

- [„Verbindungen mit Datenbanken trennen \(SQL\)“ auf Seite 101](#)
- [„Verbindungen von Benutzern mit Datenbanken trennen \(Dienstprogramm dbconsole\)“ auf Seite 102](#)
- [„Schließen einer Verbindung mit dem Monitor“ auf Seite 1130](#)

## Verbindungen mit Datenbanken trennen (SQL)

Trennen Sie Ihre Verbindung mit einer Datenbank mithilfe der DISCONNECT-Anweisung bzw. die Verbindungen anderer Benutzer mithilfe der DROP CONNECTION-Anweisung.

### Voraussetzungen

Sie benötigen keine Privilegien, um Ihre Verbindung mit der Datenbank zu trennen.

Sie müssen das DROP CONNECTION-Systemprivileg haben, um Verbindungen anderer Benutzer zu trennen.

### Aufgabe

- Stellen Sie eine Verbindung mit der Datenbank her.

Option	Aktion
Verbindung des aktuellen Benutzers trennen	Führen Sie eine DISCONNECT-Anweisung aus.
Verbindungen anderer Benutzer trennen	Verwenden Sie die Systemprozedur "sa_conn_info", um die Verbindungs-ID des Benutzers zu ermitteln, dessen Verbindung Sie trennen wollen.  Führen Sie die Anweisung DROP CONNECTION aus.

### Ergebnisse

Die Verbindung des Benutzers mit der Datenbank wird getrennt.

### Beispiel

Mit der folgenden Anweisung wird die aktuelle Verbindung conn1 in Interactive SQL getrennt:

```
DISCONNECT conn1;
```

Die folgende Anweisung zeigt, wie DISCONNECT in Embedded SQL verwendet wird:

```
EXEC SQL DISCONNECT :conn-name
```

Mit der folgenden Anweisung wird Verbindung Nummer 4 getrennt:

```
DROP CONNECTION 4;
```

### Siehe auch

- „DISCONNECT-Anweisung [ESQL] [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP CONNECTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindungen mit Datenbanken trennen (Sybase Central)“ auf Seite 100
- „Verbindungen von Benutzern mit Datenbanken trennen (Dienstprogramm dbconsole)“ auf Seite 102
- „Schließen einer Verbindung mit dem Monitor“ auf Seite 1130
- „sa\_conn\_info-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Verbindungen von Benutzern mit Datenbanken trennen (Dienstprogramm dbconsole)

Sie können das SQL Anywhere-Konsolendienstprogramm (dbconsole) verwenden, um Verbindungen von Benutzern mit einer Datenbank zu trennen.

### Voraussetzungen

Sie müssen das DROP CONNECTION-Systemprivileg haben, um Verbindungen anderer Benutzer zu trennen.

### Aufgabe

1. Stellen Sie über das SQL Anywhere-Konsolendienstprogramm eine Verbindung zur Datenbank her.
2. Rechtsklicken Sie in der Spalte **Benutzer-ID** auf den Benutzer und klicken Sie auf **Verbindung trennen**.

Sie können die Spalten, die in der SQL Anywhere-Konsole angezeigt werden, im Fenster **Optionen** konfigurieren, das Sie durch Klicken auf **Datei » Optionen** öffnen können.

### Ergebnisse

Die Verbindung des Benutzers mit der Datenbank wird getrennt.

### Siehe auch

- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 877
- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 981
- „Verbindungen mit Datenbanken trennen (Sybase Central)“ auf Seite 100
- „Verbindungen mit Datenbanken trennen (SQL)“ auf Seite 101
- „Schließen einer Verbindung mit dem Monitor“ auf Seite 1130

## Kommunikationsprotokolle

Datenbankserver kommunizieren über eine Vielzahl von Protokollen. SQL Anywhere enthält zahlreiche Optionen für die Anpassung des Verhaltens von unterstützten Protokollen.

**Siehe auch**

- „SQL Anywhere als HTTP-Webserver“ [[SQL Anywhere Server - Programmierung](#)]
- „Zugriff auf Webdienste mithilfe von Webclients“ [[SQL Anywhere Server - Programmierung](#)]
- „Kommunikationsprotokolle der Interface-Bibliothek“ [[SQL Anywhere 16 - Einführung](#)]

## Hinweise zum Kommunikationsprotokoll

Die Kommunikation zwischen einer Clientanwendung und einem Datenbankserver benötigt ein Kommunikationsprotokoll. SQL Anywhere unterstützt Kommunikationsprotokolle für die Kommunikation im Netzwerk, aber auch für den Datenverkehr auf dem Computer selbst.

### Verfügbare Protokolle für den Personal Datenbankserver (dbeng16)

Standardmäßig lässt der Personal Datenbankserver nur Shared Memory-Verbindungen zu. Um auch das TCP/IP-Protokoll zu starten, verwenden Sie die Option -x.

- **Shared Memory** Dieses Protokoll wird für die Kommunikation auf demselben Computer verwendet und ist immer auf allen Plattformen verfügbar.

Für die Kommunikation auf einem einzigen Computer kann mit Shared Memory eine bessere Performance erzielt werden als mit TCP/IP.

Hinweise zur Sicherung von Shared Memory-Verbindungen unter Unix finden Sie unter [Setzen Sie die SATMP-Umgebungsvariable auf ein eindeutiges Verzeichnis \(Unix\) auf Seite 1407](#).

- **TCP/IP** Dieses Protokoll steht nur für die Kommunikation auf demselben Computer für Personal Server zur Verfügung. Sie müssen zusätzlich TCP/IP verwenden, wenn Sie TDS-Clients betreiben (Sybase Open Client oder jConnect JDBC-Treiber). Es steht auf allen Plattformen zur Verfügung.

Weitere Hinweise zu TDS-Clients finden Sie unter „[SQL Anywhere als Open Server](#)“ auf Seite 1569.

### Verfügbare Protokolle für den Netzwerk-Datenbankserver (dbsrv16)

Standardmäßig startet der Netzwerk-Datenbankserver mit den Shared Memory- und TCP/IP-Protokollen. Sie können die TCP/IP-Protokolloptionen bereitstellen oder das TCP/IP-Protokoll mit der Option -x deaktivieren.

- **Shared Memory** Dieses Protokoll wird für die Kommunikation auf demselben Computer verwendet und ist immer auf allen Plattformen verfügbar. Hinweise zur Sicherung von Shared Memory-Verbindungen unter Unix finden Sie unter [Setzen Sie die SATMP-Umgebungsvariable auf ein eindeutiges Verzeichnis \(Unix\) auf Seite 1407](#).
- **TCP/IP** Dieses Protokoll wird hauptsächlich für die Kommunikation zwischen verschiedenen Computern verwendet. Sie müssen TCP/IP verwenden, wenn Sie TDS-Clients (Sybase Open Client oder jConnect JDBC-Treiber) haben. Es steht auf allen Plattformen zur Verfügung. Weitere Hinweise zu TDS-Clients finden Sie unter „[SQL Anywhere als Open Server](#)“ auf Seite 1569.

### Von einem SQL Anywhere-Client verbinden

- **Shared Memory** Shared Memory ist das Standard-Kommunikationsprotokoll. Wenn Sie eine Shared Memory-Verbindung herstellen möchten, geben Sie in der Verbindungszeichenfolge des Clients nicht den Verbindungsparameter Host oder CommLinks (LINKS) an.
- **TCP/IP** Wenn Sie eine TCP/IP-Verbindung herstellen möchten, geben Sie entweder den Host-Verbindungsparameter oder den CommLinks-Verbindungsparameter (LINKS) an. Der Host-Verbindungsparameter wird empfohlen.

### Siehe auch

- „Datenbankserveroption -x “ auf Seite 305
- „Host-Verbindungsparameter“ auf Seite 363
- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „TCP/IP-Protokoll“ auf Seite 105
- „Netzwerkprotokolloptionen“ auf Seite 388
- „Verbindungsparameter“ auf Seite 337

## Hinweise zu Sitzung und Terminal für Shared Memory-Verbindungen

### Shared Memory, Dienste und Terminaldienste (Windows Vista oder höher)

Wenn Sie Datenbankserver und Clients als Dienste oder in Terminaldiensten ausführen:

- Jeder Client kann eine Shared Memory-Verbindung mit einem Datenbankserver herstellen, der als Dienst ausgeführt wird.
- Jeder Client kann eine Shared Memory-Verbindung zu einem Datenbankserver herstellen, der in derselben Sitzung läuft wie der Client. Wenn versucht wird, eine Shared Memory-Verbindung herzustellen, sucht ein Client zuerst nach einem Datenbankserver mit dem angegebenen Namen in derselben Sitzung wie der Client. Wenn keine gefunden wird, sucht der Client nach einem Dienst mit dem angegebenen Namen.
- Ein Client, der in einer Terminalsitzung läuft, kann über Shared Memory keine Verbindung mit einem Datenbankserver herstellen, der in einer anderen Terminalsitzung läuft. Verwenden Sie stattdessen TCP/IP.
- Ein Client, der als Dienst läuft, kann über Shared Memory keine Verbindung mit einem Datenbankserver herstellen, der in einer Terminalsitzung läuft. Verwenden Sie stattdessen TCP/IP.
- Ein Datenbankserver *kann nicht starten*, wenn bereits ein Datenbankserver mit demselben Namen in der aktuellen Sitzung läuft oder ein Dienst mit demselben Namen aktiv ist.
- Ein Datenbankserver *kann starten*, wenn ein Datenbankserver mit demselben Namen in einer anderen Sitzung läuft, sofern nicht ein Dienst mit demselben Namen läuft und die Datenbankserver nicht beide TCP/IP verwenden.

### Shared Memory, Dienste und Terminaldienste (Windows XP und 2003)

Wenn Sie Datenbankserver und Clients als Dienste oder in Terminaldiensten ausführen:

- Unter Windows XP laufen Dienste und der Primär-Desktop in derselben Sitzung. Diese Konfiguration wird als Primärsitzung bezeichnet.
- Ein Client kann eine Shared Memory-Verbindung zu einem Datenbankserver herstellen, der in derselben Sitzung wie der Client oder in der Primärsitzung läuft. Wenn versucht wird, eine Shared Memory-Verbindung herzustellen, sucht ein Client zuerst nach einem Datenbankserver mit dem angegebenen Namen in derselben Sitzung wie der Client, und dann in der Primärsitzung.
- Ein Client, der in einer Primärsitzung läuft, kann über Shared Memory keine Verbindung mit einem Datenbankserver herstellen, der nicht in einer Primärsitzung läuft. Ein Client, der in einer Nicht-Primärsitzung läuft, kann über Shared Memory keine Verbindung mit einem Datenbankserver herstellen, der in einer anderen Nicht-Primärsitzung läuft. Verwenden Sie stattdessen TCP/IP.
- Ein Datenbankserver *kann nicht* starten, wenn bereits ein Datenbankserver mit demselben Namen in der aktuellen Sitzung oder in der Primärsitzung läuft. Ein Datenbankserver, der auf dem Desktop (der Primärsitzung) läuft, verhindert eventuell den Start eines Dienstes mit demselben Namen. Da Dienste üblicherweise starten, wenn das System startet, tritt dieses Problem nur selten auf.
- Ein Datenbankserver *kann* mit Shared Memory starten, auch wenn ein Datenbankserver mit demselben Namen mit Shared Memory in einer anderen Nicht-Primärsitzung läuft, sofern nicht ein Datenbankserver mit demselben Namen in der Primärsitzung läuft.
- Ein Datenbankserver *kann nicht* mit TCP/IP starten, wenn ein Datenbankserver mit demselben Namen über TCP/IP in einer anderen Sitzung (Primär- oder Nicht-Primärsitzung) läuft.

**Siehe auch**

- [„Hinweise zum Kommunikationsprotokoll“ auf Seite 103](#)

## TCP/IP-Protokoll

SQL Anywhere verwendet TCP/IP für die Verbindung von Clients mit Datenbanken auf verschiedenen Computern.

Wenn Sie das TCP/IP-Protokoll verwenden, können Sie die Client/Server-Kommunikation mithilfe von Transportschichtssicherheit und RSA-Verschlüsselungstechnologie sichern. Siehe [„Verschlüsseln der Client/Server-Kommunikation über TCP/IP“ auf Seite 106](#).

**UDP**

UDP ist ein Transportschichtprotokoll, das auf IP aufgesetzt wird. SQL Anywhere kann UDP zur anfänglichen Auflösung von Servernamen verwenden und dann TCP für die Verbindung und Kommunikation nutzen.

UDP-Pakete, die vom Datenbankserver als Antwort auf Client-Broadcasts gesendet werden, enthalten keine sensitiven Daten. Die Daten in diesen Paketen sind auf folgende Informationen beschränkt:

- Datenbankservername
- Portnummer
- Datenbankserverversion
- Namen der Datenbanken, die auf dem Datenbankserver ausgeführt werden

Sie können Datenbanknamen vor Broadcast-UDP-Antworten verbergen, indem Sie die Datenbankoption `-dh` verwenden.

Sie können auch die Serveroption `-sb` angeben, um die UDP-Listener zu deaktivieren.

### TCP/IP mit Windows verwenden

Die TCP/IP-Implementierung für Datenbankserver verwendet auf allen Windows-Plattformen Winsock 2.2. Clients unter Windows Mobile verwenden den Winsock 1.1-Standard.

#### Siehe auch

- „Datenbankoption `-dh`“ auf Seite 326
- „Datenbankserveroption `-sb`“ auf Seite 278
- „Datenbankserveroption `-x`“ auf Seite 305
- „Host-Verbindungsparameter“ auf Seite 363
- „Broadcast-Protokolloption (BCAST)“ auf Seite 390
- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399
- „MyIP-Protokolloption (ME)“ auf Seite 414

## Verschlüsseln der Client/Server-Kommunikation über TCP/IP

Standardmäßig werden Kommunikationspakete nicht verschlüsselt und stellen so ein mögliches Sicherheitsrisiko dar. Sie können die Kommunikation zwischen Clientanwendungen und dem Datenbankserver über TCP/IP sichern, indem Sie einfache Verschlüsselung oder Transportschichtsicherheit verwenden. Die Transportschichtsicherheit bietet Serverauthentifizierung, starke Verschlüsselung mit RSA-Verschlüsselungstechnologie und weitere Funktionen zum Schutz der Datenintegrität.

#### Siehe auch

- „Transportschichtsicherheit“ auf Seite 1444

## IPv6-Unterstützung in SQL Anywhere

Auf Computern mit aktiviertem IPv6 wartet der Netzwerkdatenbankserver standardmäßig auf allen IPv4- und IPv6-Adressen auf Daten. IPv6 wird unter Windows CE nicht unterstützt.

Gewöhnlich sind keine Änderungen in der Datenbankserver-Startzeile erforderlich, um IPv6 zu verwenden. Wenn die Angabe einer IP-Adresse erforderlich ist, akzeptieren die Datenbankserver- und Clientbibliotheken IPv4- und IPv6-Adressen. Beispiel: Wenn auf einem Computer mehr als eine Netzwerkkarte aktiviert ist, hat er wahrscheinlich zwei IPv4- und zwei IPv6-Adressen. Bei IPv6-

Adressen, die eine Portnummer enthalten, müssen Sie die Adresse entweder in eckige Klammern oder in Klammern setzen. Wenn der Datenbankserver nur an einer der IPv6-Adressen warten soll, können Sie eine Adresse im folgenden Format angeben:

```
dbsrv16 -x tcpip(MyIP=fd77:55f:5a64:52a:202:5445:5245:444f) ...
```

Wenn eine Clientanwendung eine IP-Adresse eines Servers angeben muss, kann die Verbindungszeichenfolge oder ODBC-Datenquelle die Adresse im folgenden Format enthalten:

```
...HOST=fd77:55f:5a64::444f;...
```

Jede Schnittstelle erhält einen Schnittstellenbezeichner, der sich am Ende der IPv6-Adresse befindet. Beispiel: Wenn *ipconfig.exe* die Adresse `fd77:55f:5a64::444f` auflistet, ist der Schnittstellenbezeichner 7. Wenn Sie eine IPv6-Adresse auf einer Windows-Plattform angeben, sollten Sie den Schnittstellenbezeichner verwenden. Unter Unix können Sie entweder einen Schnittstellenbezeichner oder einen Schnittstellennamen angeben (der Schnittstellename ist der Name der von *ifconfig* angegebenen Schnittstelle). Beispiel: Der Schnittstellename in der folgenden IPv6-Adresse ist `eth1: fd77:55f:5a64::444f`. Der Schnittstellenbezeichner ist zur Angabe von IPv6-Adressen unter Linux (Kernel 2.6.13 und höher) erforderlich. Diese Einschränkung wirkt sich auf Werte aus, die wie folgt angegeben werden:

- „Host-Verbindungsparameter“
- „Broadcast-Protokolloption (BCAST)“
- „Host-Protokolloption (IP) (nur clientseitig)“
- „MyIP-Protokolloption (ME)“

## Beispiel

Beispiel: *ipconfig.exe* listet zwei Schnittstellen auf, eine mit dem Bezeichner "1" und die andere mit dem Bezeichner "2". Wenn Sie nach einem Datenbankserver suchen, der sich im Netzwerk befindet, das von Schnittstellennummer 2 verwendet wird, können Sie die Clientbibliothek anweisen, nur auf dieser Schnittstelle Broadcasts zu senden:

```
LINKS=tcpip(BROADCAST=ff02::1%2)
```

Die IPv6 link-local multicast-Adresse ist `ff02::1`.

## Firewall-Verbindungen

Es gibt Einschränkungen für Verbindungen, wenn sich die Clientanwendung auf der einen Seite einer Firewall und der Datenbankserver auf der anderen Seite befinden. Firewall-Software filtert unter Umständen Netzwerkpakete entsprechend dem Netzwerkport aus. Außerdem wird es UDP-Paketen oft verwehrt, eine Firewall zu passieren.

In der Regel können Sie eine Verbindung über eine korrekt konfigurierte Firewall mit dem Host-Verbindungsparameter und Übergabe von der Datenbankserveradresse und Port herstellen. Wenn der Datenbankserver den Standard-Port 2638 verwendet, ist die Angabe des Ports nicht erforderlich.

Das folgende Fragment einer Verbindungszeichenfolge stellt eine Verbindung mit einem Datenbankserver namens "myserver" her, der auf einem Computer an der Adresse "serverhost" mit dem Port "2020"

ausgeführt wird. Es werden keine UDP-Pakete verwendet, da der Host-Verbindungsparameter die TCP/IP-Adresse und den Port angibt.

```
Server=myserver;Host=serverhost:2020
```

### Firewalls, die nur bestimmte Clientports zulassen

Wenn die Firewall so konfiguriert werden muss, dass nur bestimmte Clientports zugelassen sind, müssen Sie den Verbindungsparameter CommLinks(LINKS) anstelle des Host-Verbindungsparameters verwenden. Die folgenden TCP/IP-Protokolloptionen sind erforderlich, wenn Sie den CommLinks-Verbindungsparameter verwenden:

- **Host** Setzen Sie diese Protokolloption auf den Hostnamen, auf dem der Datenbankserver läuft. Sie können die Kurzform "IP" verwenden.
- **ServerPort** Wenn Ihr Datenbankserver nicht den Standard-Port 2638 verwendet, müssen Sie den benutzten Port hier angeben. Sie können die Kurzform PORT verwenden.
- **ClientPort** Stellen Sie mit dieser Protokolloption den Wertebereich ein, den die Clientanwendung verwenden darf. Sie können die Kurzform CPORT verwenden.
- **DoBroadcast=NONE** Aktivieren Sie diese Protokolloption, damit bei der Verbindung mit einem Server UDP nicht genutzt wird. Sie können die Kurzform DOBROAD verwenden.

Die Firewall muss konfiguriert werden, um TCP/IP-Datenverkehr zwischen der Adresse des SQL Anywhere-Datenbankservers und allen Adressen der SQL Anywhere-Clients zu ermöglichen. Die Adresse des SQL Anywhere--Datenbankservers ist die IP-Adresse des Computers, auf dem der SQL Anywhere-Datenbankserver läuft (die HOST-Protokolloption), und die IP-Portnummer des SQL Anywhere-Datenbankservers (die ServerPort-Protokolloption, Standardwert 2638).

Verwenden Sie für jeden Clientcomputer einen Bereich mit mehr Ports als die maximale Anzahl von gleichzeitigen Verbindungen, da ein Timeout von mehreren Minuten verstreicht, bevor ein Clientport wieder verwendet werden kann. Der Bereich von Clients, der in der ClientPort-Protokolloption definiert wird, muss mit dem Bereich übereinstimmen, der über eine Firewall zugelassen wird.

### Siehe auch

- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „ClientPort-Protokolloption (CPORT) (nur clientseitig)“ auf Seite 395
- „ServerPort-Protokolloption (PORT)“ auf Seite 416
- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399
- „DoBroadcast-Protokolloption (DOBROAD)“ auf Seite 398

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge beschränkt die Clientanwendung auf die Ports 5050 bis 5060 und stellt eine Verbindung mit einem Datenbankserver namens myeng her, der auf dem Computer mit der Adresse myhost läuft, wobei der Serverport 2020 benutzt wird. Es wird wegen der auf NONE gesetzten DoBroadcast-Option kein UDP-Broadcast ausgeführt.

```
Server=myeng;LINKS=tcip(ClientPort=5050-5060;HOST=myhost;PORT=2020;DoBroadcast=NONE)
```

## DFÜ-Netzwerkverbindungen (CommLinks-Verbindungsparameter)

Zur Verbindung über eine DFÜ-Netzwerkverbindung müssen Sie den CommLinks-Verbindungsparameter verwenden.

Auf der Clientseite müssen Sie folgende Protokolloptionen verwenden:

- **Host** Sie müssen den Hostnamen oder die IP-Adresse des Datenbankservers mit der Host-Protokolloption (IP) angeben.
- **DoBroadcast** Wenn Sie die Host-Protokolloption (IP) angeben, ist es nicht erforderlich, per Broadcast nach dem Datenbankserver zu suchen. Benutzen Sie daher Direct Broadcasting.
- **MyIP** Sie müssen auf der Clientseite **MyIP=NONE** einschalten.
- **TIMEOUT** Legen Sie die Timeout-Protokolloption (TO) so fest, dass dem Client mehr Zeit für die Suche nach dem Server zur Verfügung steht.

### Beispiel

Nachstehend finden Sie ein Beispiel für einen typischen CommLinks-Verbindungsparameter (LINKS) für die Verbindung über eine DFÜ-Netzwerkverbindung:

```
LINKS=tcip(MyIP=NONE;DoBroadcast=DIRECT;HOST=server-ip); TIMEOUT=15)
```

### Siehe auch

- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399
- „DoBroadcast-Protokolloption (DOBROAD)“ auf Seite 398
- „MyIP-Protokolloption (ME)“ auf Seite 414
- „Timeout-Protokolloption (TO)“ auf Seite 420

## Verbindungen mit LDAP als Namensserver

Sie können einen zentralen LDAP-Server definieren, der alle Datenbankserver in einem Unternehmen verfolgt, wenn Sie unter Windows (außer Windows Mobile) oder Unix arbeiten. Wenn sich der Datenbankserver bei einem LDAP-Server anmeldet, können Clients den LDAP-Server abfragen und den gesuchten Datenbankserver finden, gleichgültig ob sie auf einem WAN bzw. LAN oder hinter einer Firewall liegen. Die LDAP-Namensserverversuche wird nicht von Clients genutzt, die die Datenbankserveradresse mit dem Host-Verbindungsparameter oder der HOST-Protokolloption angeben.

### Konfigurieren der Datei *saldap.ini*

Wenn Sie mit LDAP als Namensserver nach Datenbankservern suchen möchten, muss eine Datei, die Informationen zum Auffinden des LDAP-Servers und zum Verbinden mit dem LDAP-Server enthält, auf dem Datenbankservercomputer und auf jedem Clientcomputer erstellt werden. Standardmäßig ist der Name dieser Datei *saldap.ini*, Sie können sie aber umbenennen. Wenn Sie die Datei *saldap.ini* umbenennen, müssen Sie beim Verbinden mit dem Datenbankserver die LDAP-Protokolloption verwenden, um den Dateinamen anzugeben. Wenn diese Datei nicht vorhanden ist, wird die Unterstützung für den LDAP-Namensserver deaktiviert.

Mithilfe des Dienstprogramms zum Verschleiern von Dateien (dbfhide) können Sie einfache Verschlüsselung hinzufügen, um den Inhalt der Datei *saldap.ini* zu verschleiern.

Die Datei muss sich in demselben Verzeichnis befinden wie die SQL Anywhere-Programmdateien (z.B. *%SQLANY16%\bin32* unter Windows), wenn nicht mit der LDAP-Protokolloption ein kompletter Pfad angegeben wird. Die Datei muss folgendes Format haben:

```
[LDAP]
server=computer-running-LDAP-server
port=port-number-of-LDAP-server
basedn=Base-DN
authdn=Authentication-DN
password=password-for-authdn
search_timeout=age-of-timestamps-to-be-ignored
update_timeout=frequency-of-timestamp-updates
read_authdn=read-only-authentication-domain-name
read_password=password-for-authdn
```

**server** Der Name oder die IP-Adresse des Systems, auf dem der LDAP-Server läuft. Bei Unix muss dieser Wert angegeben werden. Wenn dieser Eintrag unter Windows fehlt, sucht Windows nach einem LDAP-Server auf dem lokalen Domänencontroller.

**port** Die vom LDAP-Server benutzte Portnummer. Der Standardwert ist 389.

**basedn** Der Domänenname der Unterstruktur, in der SQL Anywhere-Einträge gespeichert werden. Dieser Wert ist standardmäßig das Stammverzeichnis der Struktur.

**authdn** Der Name der Authentifizierungsdomäne. Der Domänenname muss ein bestehendes Benutzerobjekt im LDAP-Verzeichnis sein, das Schreibzugriff auf "basedn" hat. Dieser Parameter ist für den Datenbankserver erforderlich und wird vom Client ignoriert.

**password** Das Kennwort für "authdn". Dieser Parameter ist für den Datenbankserver erforderlich und wird vom Client ignoriert.

**search\_timeout** Das Alter, ab dem Zeitstempel vom Client bzw. dem Dienstprogramm für die Serverauflistung [dblocate] ignoriert werden. Der Wert "0" deaktiviert diese Option, sodass alle Einträge als "aktuell" eingestuft werden. Der Standardwert ist 600 Sekunden (10 Minuten).

**update\_timeout** Die Häufigkeit der Zeitstempelaktualisierungen im LDAP-Verzeichnis. Der Wert "0" deaktiviert die Option, sodass der Datenbankserver den Zeitstempel nie aktualisiert. Der Standardwert ist 120 Sekunden (2 Minuten).

**read\_authdn** Der schreibgeschützte Name der Authentifizierungsdomäne. Der Domänenname muss ein bestehendes Benutzerobjekt im LDAP-Verzeichnis sein, das Lesezugriff auf "basedn" hat. Dieser Parameter ist nur erforderlich, wenn der LDAP-Server eine nicht anonyme Bindung braucht, bevor der Suchprozess durchgeführt werden kann. Dieses Feld ist z.B. erforderlich, wenn Active Directory als der LDAP-Server verwendet wird. Wenn dieser Parameter fehlt, ist die Bindung anonym.

**read\_password** Das Kennwort für "authdn". Dieser Parameter ist auf dem Client nur erforderlich, wenn der Parameter read\_authdn angegeben ist.

## Verbindung herstellen

Wenn der Datenbankserver startet, prüft er, ob ein Eintrag mit demselben Namen in LDAP vorhanden ist. Ein eventuell gefundener Eintrag wird ersetzt, wenn die Speicherorteinträge in LDAP zu dem Datenbankserver passen, der gestartet werden soll, oder wenn der Wert des Zeitstempelfelds im LDAP-Eintrag jünger ist als der durch den `search_timeout`-Parameter festgelegte Wert.

Wenn ein anderer Datenbankserver mit demselben Namen wie der läuft, der zu starten versucht, startet die Datenbank nicht.

Um sicherzugehen, dass Einträge in LDAP aktuell sind, aktualisiert der Datenbankserver ein Zeitstempelfeld im LDAP-Eintrag alle 2 Minuten. Wenn der Zeitstempel eines Eintrags älter ist als 10 Minuten, ignorieren die Clients den LDAP-Eintrag. Beide Einstellungen sind konfigurierbar.

Auf dem Client wird das LDAP-Verzeichnis durchsucht, bevor der Client das UDP-Broadcasting ausführt. Wenn der Datenbankserver gefunden wird, werden keine UDP-Broadcasts gesendet. Die LDAP-Suche ist sehr schnell. Wenn sie fehlschlägt, kommt es zu keiner merklichen Verzögerung.

## LDAP-Server und das Dienstprogramm für die Serverauflistung (dblocate)

Das Dienstprogramm für die Serverauflistung (dblocate) benutzt ebenfalls LDAP - alle in LDAP aufgelisteten Datenbankserver werden der zurückgegebenen Liste der Server hinzugefügt. Damit kann das Dienstprogramm für die Serverauflistung (dblocate) Datenbankserver auflisten, die normalerweise nicht zurückgegeben werden, etwa solche, bei denen Broadcasts nicht ankommen. Einträge mit Zeitstempeln, die älter als 10 Minuten sind, sind nicht enthalten.

## Siehe auch

- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960

## Beispiel

Nachstehend finden Sie ein Beispiel für eine *saldap.ini*-Datei:

```
[LDAP]
server=ldapservers
basedn=dc=iAnywhere,dc=com
authdn=cn=SAserver,ou=iAnywhereASA,dc=iAnywhere,dc=com
password=secret
```

Die Einträge werden in einer Unterstruktur der "basedn" namens iAnywhereASA gespeichert. Dieser Eintrag muss erstellt werden, bevor SQL Anywhere LDAP benutzen kann. Um die Unterstruktur zu erstellen, können Sie das Dienstprogramm LDAPADD verwenden und folgende Informationen angeben:

```
dn: ou=iAnywhereASA,basedn
objectClass: organizationalUnit
objectClass: top
ou: iAnywhereASA
```

## Links erstellen im Verzeichnis */usr/lib* unter IBM AIX

Wenn Sie SQL Anywhere mit IBM AIX 6 verwenden möchten, müssen Sie entweder Links im Verzeichnis */usr/lib* erstellen oder sicherstellen, dass das Verzeichnis mit den LDAP-Bibliotheken im LIBPATH enthalten ist, um zu gewährleisten, dass die LDAP-Systembibliotheken gefunden werden.

### Voraussetzungen

LDAP wird nur mit TCP/IP und nur mit Netzwerk-Datenbankservern verwendet.

### Kontext und Bemerkungen

Das Dienstprogramm für die Serverauflistung (dblocate) kann den LDAP-Server verwenden, um andere derartige Server zu finden.

### Aufgabe

1. Erstellen Sie Links im Verzeichnis */usr/lib*, indem Sie die folgenden Befehle als Root-Benutzer ausführen:

```
cd /usr/lib
ln -s /opt/IBM/ldap/V6.1/lib64/libibmldap.a libibmldap64.a
ln -s /opt/IBM/ldap/V6.1/lib/libibmldap.a
```

2. (Optional) Stellen Sie sicher, dass das Verzeichnis mit den LDAP-Bibliotheken im LIBPATH enthalten ist.

Für 32-Bit-Bibliotheken:

```
export LIBPATH=/opt/IBM/ldap/V6.1/lib:$LIBPATH
```

Für 64-Bit-Bibliotheken:

```
export LIBPATH=/opt/IBM/ldap/V6.1/lib64:$LIBPATH
```

### Ergebnisse

Links werden in */usr/lib* erstellt.

### Siehe auch

- „LDAP-Protokolloption“ auf Seite 406
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960

## Komprimierungseinstellungen für die Kommunikation

Die Aktivierung der Komprimierung für eine oder alle Verbindungen und die Definition der Mindestgröße, mit der Pakete komprimiert werden, kann unter bestimmten Umständen die Performance von SQL Anywhere steigern. Daher sollten Sie eine Performance-Analyse für Ihr Netzwerk mit Ihren Anwendungen durchführen, um zu ermitteln, ob eine Änderung des Komprimierungsschwellenwerts vorteilhaft ist oder nicht.

Die Aktivierung der Komprimierung erhöht die in den Datenpaketen gespeicherte Datenmenge, wodurch die Anzahl der zur Übertragung einer bestimmten Datenmenge erforderlichen Pakete verringert wird. Eine geringere Paketanzahl bedeutet eine schnelle Datenübertragung.

Um bestimmen zu können, ob die Aktivierung der Komprimierung in Ihrer Situation hilfreich ist, wird Folgendes empfohlen: Führen Sie eine Performanceanalyse Ihres Netzwerks mit Ihrer Anwendung durch, bevor Sie die Kommunikationskomprimierung in einer Produktionsumgebung anwenden.

Sie können die Performance der Komprimierung wie folgt regeln:

**Komprimierung aktivieren** Die Aktivierung der Komprimierung für alle Verbindungen kann die Performance von SQL Anywhere unter bestimmten Bedingungen steigern:

- Beim Einsatz in einem langsamen Netzwerk (z. B. in bestimmten drahtlosen Netzwerken, Modems, seriellen Verbindungen oder WANs).
- Beim Einsatz mit SQL Anywhere-Verschlüsselung in einem langsamen Netzwerk mit integrierter Komprimierung, da Pakete komprimiert werden, bevor die Verschlüsselung erfolgt.

Die Aktivierung der Komprimierung kann allerdings manchmal auch die Performance verringern. Zum Beispiel:

- Die Kommunikationskomprimierung benötigt mehr Speicher und stärkere CPU-Nutzung. Sie kann eine geringere Performance vor allem bei LANs und anderen schnellen Netzwerken bewirken.
- Die meisten Modems und einige langsame Netzwerke haben bereits eine eingebaute Komprimierungsfunktion. In diesen Fällen wird die SQL Anywhere-Kommunikationskomprimierung keine zusätzlichen Vorteile bringen, wenn Sie die Daten nicht auch zusätzlich verschlüsseln.

Informationen zum Aktivieren oder Deaktivieren der Komprimierung finden Sie unter [„Verbindungsparameter Compress \(COMP\)“ auf Seite 347](#) und [„Datenbankserveroption - pc“ auf Seite 272](#).

### Komprimierungsschwellenwert ändern

#### Hinweis

Bei den meisten Netzwerkinstallation ist eine Änderung des Komprimierungsschwellenwerts nicht nötig. In seltenen Fällen können Sie den Schwellenwert für die Komprimierung anpassen, um die Performance von SQL Anywhere zu verbessern.

Um zu ermitteln, ob die Änderung des Schwellenwerts für die Komprimierung in Ihrem Fall sinnvoll ist, führen Sie eine Performance-Analyse Ihres Netzwerk mit Ihren Anwendungen durch, bevor Sie Anpassungen in einer Produktionsumgebung vornehmen.

Wenn die Komprimierung aktiviert ist, werden einzelne Pakete je nach ihrer Größe komprimiert oder nicht. SQL Anywhere komprimiert beispielsweise keine Pakete, die kleiner als der Komprimierungsschwellenwert sind, auch wenn die Kommunikationskomprimierung aktiviert ist.

Da CPU-Zeit erforderlich ist, um Pakete zu komprimieren, ist die versuchte Komprimierung kleiner Pakete im Endeffekt möglicherweise sogar ein Nachteil für die Performance.

Im Allgemeinen kann die Absenkung des Komprimierungsschwellenwerts die Performance in sehr langsamen Netzwerken verbessern, während die Erhöhung des Komprimierungsschwellenwerts die Performance erhöhen kann, indem die CPU-Nutzung verringert wird. Da allerdings das Absenken des Komprimierungsschwellenwerts die CPU-Nutzung auf dem Client und dem Server erhöht, sollte eine Performanceanalyse erfolgen, um zu ermitteln, ob eine Änderung des Komprimierungsschwellenwerts vorteilhaft ist.

### SQL Anywhere-Komprimierungseinstellungen anpassen

- Aktivieren Sie die Kommunikationskomprimierung.

Umfangreiche Datenübertragungen mit stark komprimierbaren Daten und größeren Paketen haben tendenziell die besten Komprimierungsraten.

- Passen Sie die Einstellung des Verbindungsparameters `CompressionThreshold` an.

Das Absenken des Komprimierungsschwellenwerts kann die Performance in sehr langsamen Netzwerken verbessern, während das Erhöhen des Komprimierungsschwellenwerts die Performance erhöhen kann, weil die CPU-Nutzung verringert wird.

### Siehe auch

- „Systemmonitor-Statistiken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „sa\_conn\_compression\_info-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindungsparameter Compress (COMP)“ auf Seite 347
- „Datenbankserveroption -pc“ auf Seite 272
- „Verbindungsparameter CompressionThreshold (COMPTH)“ auf Seite 348
- „Datenbankserveroption -pt“ auf Seite 273

## Praktische Einführung: SQL Anywhere-Datenbank erstellen

In dieser praktischen Einführung wird gezeigt, wie Sie eine einfache Datenbank erstellen können und dabei die Tabellen "Products", "SalesOrderItems", "SalesOrders" und "Customers" der SQL Anywhere-Beispieldatenbank als Vorlagen verwenden.

### Privilegien

In der neuen Datenbank müssen Sie das CREATE ANY OBJECT-Systemprivileg haben.

## Lektion 1: Datenbankdateien erstellen

Erstellen Sie eine Datenbankdatei für Ihre Daten. Die Datenbankdatei enthält Systemtabellen und andere Systemobjekte, die in allen Datenbanken gleich sind.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: SQL Anywhere-Datenbank erstellen“](#).

## Aufgabe

1. Starten Sie Sybase Central. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.
2. Starten Sie den **Assistenten zum Erstellen einer Datenbank**. Klicken Sie auf **Extras » SQL Anywhere 16 » Datenbank erstellen**.
  - a. Auf der Seite **Willkommen** klicken Sie auf **Weiter**.
  - b. Klicken Sie auf **Datenbank auf diesem Computer erstellen** und anschließend auf **Weiter**.
  - c. Im Feld **Haupt-Datenbankdatei in folgender Datei speichern** geben Sie `c:\temp\mysample.db` ein.

Wenn Sie ein anderes temporäres Verzeichnis verwenden als `c:\temp`, geben Sie den entsprechenden Pfad an.
  - d. Geben Sie auf der Seite **DBA-Benutzer und Kennwort angeben** die DBA-Benutzer-ID und das DBA-Kennwort an. Standardmäßig lautet die Benutzer-ID **DBA** und das Kennwort **sql**. Es wird jedoch empfohlen, dass Sie diese Einstellungen ändern, um die Sicherheit Ihrer Datenbank zu gewährleisten.
  - e. Klicken Sie auf **Fertig stellen** und anschließend auf **Schließen**.

Sie werden automatisch als DBA-Benutzer mit der Datenbank verbunden.

## Ergebnisse

Sie haben eine Datenbank erstellt und eine Verbindung mit ihr hergestellt.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 2: Tabellen zur Datenbank hinzufügen“](#) auf Seite 115.

## Siehe auch

- „SQL Anywhere-Beispieldatenbank“ [[SQL Anywhere 16 - Einführung](#)]
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbanken erstellen (Dienstprogramm dbinit)“ auf Seite 126
- „Datenbanken erstellen (Sybase Central)“ auf Seite 125

# Lektion 2: Tabellen zur Datenbank hinzufügen

Erstellen Sie Tabellen, um die Informationen in Ihrer Datenbank zu speichern.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankdateien erstellen](#)“ auf Seite 114.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: SQL Anywhere-Datenbank erstellen](#)“.

## Aufgabe

1. Starten Sie den **Assistenten zum Erstellen einer Tabelle**. Rechtsklicken Sie im linken Fensterausschnitt von Sybase Central auf **Tabellen** und klicken Sie auf **Neu » Tabelle**.
  - a. Im Feld **Wie lautet der Name der neuen Tabelle?** geben Sie **Products** ein.
  - b. Klicken Sie auf **Fertig stellen**.

Der Datenbankserver erstellt die Tabelle mit den Standardeinstellungen und zeigt dann im rechten Fensterausschnitt die Registerkarte **Spalten** an. Das Feld **Name** für die neue Spalte wird ausgewählt und Sie werden aufgefordert, einen Namen für die neue Spalte anzugeben.

2. Tippen Sie **ProductID** als Namen für die neue Spalte ein.

Da dies die erste Spalte in der Tabelle ist, wird **PSch** markiert, um anzuzeigen, dass die Spalte der Primärschlüssel für die Tabelle ist.

3. Klicken Sie in der Liste **Datentyp** auf **Integer**.
4. Klicken Sie auf die Schaltfläche ...
5. Klicken Sie auf die Registerkarte **Wert** und anschließend auf **Standardwert » Systemdefiniert » Autoincrement**.

Ein AUTOINCREMENT-Wert wird für jede zur Tabelle hinzugefügte Zeile erhöht. Dieser Wert gewährleistet, dass die Werte in der Spalte eindeutig sind, was für Primärschlüssel erforderlich ist.

6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Datei » Neu » Spalte**.
  - a. Im Feld **Name** geben Sie **ProductName** ein.
  - b. Klicken Sie in der Liste **Datentyp** auf **Char**.
  - c. Klicken Sie in der Liste **Größe** auf **15**.
8. Wiederholen Sie die vorherigen Schritte, um folgende Tabellen zu Ihrer Datenbank hinzuzufügen:
  - **Customers-Tabelle** Fügen Sie eine Tabelle mit dem Namen **Customers** hinzu, die folgende Spalten enthält:
    - **CustomerID** Die Identifizierungsnummer für jeden Kunden. Vergewissern Sie sich, dass **PSch** ausgewählt ist, und setzen Sie den **Datentyp** auf **Integer** und den **Standardwert** auf **Autoincrement**.

- **CompanyName** Der Name der jeweiligen Firma. Setzen Sie den **Datentyp** auf **Char** mit einer maximalen Länge von 35 Zeichen.
  - **SalesOrders-Tabelle** Fügen Sie eine Tabelle mit dem Namen **SalesOrders** hinzu, die folgende Spalten enthält:
    - **SalesOrderID** Die Identifizierungsnummer für jede Bestellung. Vergewissern Sie sich, dass **PSch** ausgewählt ist, und setzen Sie den **Datentyp** auf **Integer** und den **Standardwert** auf **Autoincrement**.
    - **OrderDate** Das Datum, an dem die Bestellung aufgegeben wurde. Setzen Sie den **Datentyp** auf **date**.
    - **CustomerID** Die Identifikationsnummer des Kunden, der die Bestellung aufgegeben hat. Setzen Sie den **Datentyp** auf **integer**.
  - **SalesOrderItems-Tabelle** Fügen Sie eine Tabelle mit dem Namen **SalesOrderItems** hinzu, die folgende Spalten enthält:
    - **SalesOrderItemsID** Die Identifikationsnummer der Bestellung, zu der das Element gehört. Vergewissern Sie sich, dass **PSch** ausgewählt ist, und setzen Sie den **Datentyp** auf **Integer**.
    - **LineID** Die Identifizierungsnummer für jede Bestellung. Vergewissern Sie sich, dass **PSch** ausgewählt ist, und setzen Sie den **Datentyp** auf **Integer**.
- Da **PSch** sowohl für SalesOrderItemsID als auch für LineID festgelegt ist, besteht der Primärschlüssel für die Tabelle aus den verketteten Werten dieser beiden Spalten.
- **ProductID** Die Identifizierungsnummer des bestellten Produkts. Setzen Sie den **Datentyp** auf **integer**.

9. Klicken Sie auf **Datei** » **Speichern**.

## Ergebnisse

Sie haben vier Tabellen für Ihre Datenbank erstellt.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: NOT NULL-Integritätsregel für eine Spalte festlegen](#)“ auf Seite 117.

## Siehe auch

- „Erstellen einer Tabelle“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Primärschlüssel“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Entity-Relationship-Diagramme anzeigen“ auf Seite 811

## Lektion 3: NOT NULL-Integritätsregel für eine Spalte festlegen

Fügen Sie einer Spalte eine NOT NULL-Integritätsregel hinzu, um zu verhindern, dass die Spalte NULL zulässt. Standardmäßig ist NULL für Spalten zulässig. Es ist jedoch empfehlenswert, Spalten als NOT NULL zu deklarieren, es sei denn, Sie haben einen bestimmten Grund, NULL zuzulassen.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankdateien erstellen](#)“ auf Seite 114.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: SQL Anywhere-Datenbank erstellen](#)“.

### Aufgabe

1. Doppelklicken Sie im linken Fensterausschnitt von Sybase Central auf **Tabellen**.
2. Klicken Sie auf **Products** und dann auf die Registerkarte **Spalten** im rechten Fensterausschnitt.
3. Klicken Sie auf die Spalte **ProductName**.
4. Klicken Sie auf **Datei » Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Integritätsregeln** und anschließend auf **Werte können nicht Null sein**.
6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Datei » Speichern**.

### Ergebnisse

Diese Integritätsregel bedeutet, dass für jede Zeile, die der Tabelle **Products** hinzugefügt wird, die Spalte **ProductName** einen Wert haben muss.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 4: Fremdschlüssel erstellen](#)“ auf Seite 118.

### Siehe auch

- „NULL-Spezialwert“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Hinweise zu Integritätsregeln“ auf Seite 125

## Lektion 4: Fremdschlüssel erstellen

Erstellen Sie Fremdschlüssel, um Beziehungen zwischen Tabellen zu erstellen.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankdateien erstellen](#)“ auf Seite 114.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: SQL Anywhere-Datenbank erstellen](#)“.

### Aufgabe

1. Doppelklicken Sie im linken Fensterausschnitt von Sybase Central auf **Tabellen**.
2. Klicken Sie auf die Tabelle **SalesOrdersItems**.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Integritätsregeln**.
4. Starten Sie den **Assistenten zum Erstellen eines Fremdschlüssels**. Klicken Sie auf **Datei » Neu » Fremdschlüssel**.
  - a. Klicken Sie in der Liste **Auf welche Tabelle soll sich dieser Fremdschlüssel beziehen?** auf die Tabelle **Products**.
  - b. Im Feld **Wie lautet der Name des neuen Fremdschlüssels?** geben Sie **ProductIDkey** ein.
  - c. Klicken Sie auf **Weiter**.
  - d. Klicken Sie im Feld **Soll dieser Fremdschlüssel den Primärschlüssel oder eine Eindeutigkeits-Integritätsregel referenzieren?** auf **Primärschlüssel**.
  - e. Klicken Sie in der Liste **Fremdspalte** auf **SalesOrderItemsID**.
  - f. Klicken Sie auf **Fertig stellen**.

### Ergebnisse

Sie haben einen Fremdschlüssel für die Tabelle **SalesOrderItems** erstellt.

Sie haben die praktische Einführung zum Erstellen einer Datenbank abgeschlossen.

### Nächste Schritte

Fügen Sie Informationen in Ihre Datenbank ein.

### Siehe auch

- „Fremdschlüssel“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Fremdschlüssel erstellen (Sybase Central)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Fremdschlüssel erstellen (SQL)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankdateitypen

Jeder einzelnen Datenbank werden die folgenden Dateien zugeordnet:

- **Die Datenbankdatei** Die Datei enthält den gesamten Inhalt Ihrer Datenbank. Eine einzelne Datei kann eine einzelne Datenbank enthalten; Sie können aber bis zu 12 DBSpaces hinzufügen (das sind zusätzliche Dateien, welche Teile derselben Datenbank enthalten). Sie wählen einen Speicherort für die Datenbankdatei und die DBSpaces aus. Die Datenbankdatei hat gewöhnlich die Erweiterung **.db**.

- **Das Transaktionslog** Diese Datei enthält eine Aufzeichnung der Änderungen in der Datenbankdatei und ist für die Synchronisation und Wiederherstellung von Daten in Ihrer Datenbank nach einem Systemausfall erforderlich. Das Transaktionslog hat üblicherweise die Erweiterung *.log*.
- **Die temporäre Datei** Der Datenbankserver benutzt die temporäre Datei während einer Datenbanksitzung, wenn SQL Anywhere mehr Platz benötigt, als im Cache für Vorgänge wie Sortieren und Bildung von Vereinigungen zur Verfügung steht. Wenn der Datenbankserver diesen Platz benötigt, nutzt er ihn gewöhnlich intensiv. Die gesamte Performance der Datenbank wird hochgradig abhängig von der Geschwindigkeit des Devices, auf dem sich die temporäre Datei befindet. Der Datenbankserver verwirft diese Datei, wenn die Datenbank heruntergefahren wird, auch wenn der Datenbankserver weiterläuft. Die temporäre Datei hat einen vom Server generierten Namen mit der Erweiterung *.tmp*.

Der Standort der temporären Datei kann beim Start des Datenbankservers mit der Serveroption *-dt* angegeben werden. Wenn Sie den Speicherort der temporären Datei beim Start des Datenbankservers nicht angeben, werden die folgenden Umgebungsvariablen in der angegebenen Reihenfolge überprüft:

- SATMP-Umgebungsvariable
- TMP-Umgebungsvariable
- TMPDIR-Umgebungsvariable
- TEMP-Umgebungsvariable

Wenn keine Umgebungsvariable definiert ist, platziert SQL Anywhere seine temporäre Datei unter Windows in das aktuelle Verzeichnis und unter Unix in das Verzeichnis */tmp*.

Der Datenbankserver erstellt, verwaltet und entfernt die temporäre Datei. Sie brauchen nur zu gewährleisten, dass ausreichend freier Speicherplatz für die temporäre Datei vorhanden ist. Sie können Informationen über den verfügbaren Speicherplatz für die temporäre Datei abrufen, indem Sie die Prozedur *sa\_disk\_free\_space* verwenden.

- **Vordefinierte DBSpace-Dateien** In diesen Dateien werden Ihre Daten und andere, von der Datenbank benutzte Dateien gespeichert.
- **DBSpace-Dateien** Sie können Ihre Daten auf mehrere separate Dateien aufteilen, zusätzlich zur Datenbankdatei.
- **Transaktionslog-Spiegeldateien** Zur Erhöhung der Sicherheit können Sie eine gespiegelte Kopie des Transaktionslogs erstellen. Diese Datei hat üblicherweise die Erweiterung *.mlg*.

### Siehe auch

- „Tipp: Verschiedene Dateien auf verschiedene Geräte platzieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „sa\_disk\_free\_space-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Das Transaktionslog“ auf Seite 135
- „Vordefinierte DBSpaces“ auf Seite 127
- „Zusätzliche Hinweise zu DBSpaces“ auf Seite 128
- „Transaktionslog-Spiegeldateien“ auf Seite 138

## Datenbankerstellung

Um eine Datenbank zu erstellen, müssen Sie zuerst die darin enthaltenen Tabellen (Entitäten), die Spalten in den einzelnen Tabellen (Attribute) und die Beziehungen zwischen den Tabellen (Schlüssel und Integritätsregeln) definieren.

Es wird empfohlen, ein konzeptionelles Datenbankmodell (Conceptual Database Model, CDM) für die neue Datenbank zu erstellen. Sie können mit CDM-Anwendungen wie Sybase PowerDesigner Ihr Datenbankdesign erstellen und validieren. Diese Tools erstellen SQL-Anweisungen, die in der Regel über die ODBC-Schnittstelle an den Datenbankserver übergeben werden. Wenn Sie eines dieser Tools verwenden, müssen Sie nicht selbst SQL-Anweisungen konstruieren, um Tabellen zu erstellen, Privilegien zu erteilen usw.

Weitere Hinweise zum Design von Datenbanken und zum Erstellen eines CDM finden Sie in der Sybase PowerDesigner Dokumentation unter <http://infocenter.sybase.com/help/index.jsp>.

Sie können auch Sybase Central, Interactive SQL oder die Befehlszeile verwenden, um eine Datenbank zu erstellen oder zu **initialisieren**. Nachdem Sie die Datenbank erstellt haben, können Sie sich mit ihr verbinden und Tabellen sowie andere Objekte hinzufügen.

### Transaktionslog

Wenn Sie eine Datenbank erstellen, müssen Sie entscheiden, wo das Transaktionslog gespeichert werden soll. In diesem Log werden alle Änderungen einer Datenbank in der Reihenfolge der Änderungen gespeichert. Wenn eine Datenbankdatei durch einen Datenträgerfehler in Mitleidenschaft gezogen wird, ist das Transaktionslog ausschlaggebend für die Wiederherstellung der Datenbank. Das Transaktionslog wirkt sich außerdem positiv auf die Produktivität Ihrer Arbeit aus. Standardmäßig wird das Transaktionslog in demselben Verzeichnis gespeichert wie die Datenbankdatei, jedoch wird diese Konfiguration für den Einsatz in der Produktion nicht empfohlen.

### Kompatibilität von Datenbankdateien

Eine Datenbank ist eine Betriebssystemdatei. Sie kann wie jede andere Datei an einen anderen Speicherort kopiert werden.

Datenbankdateien sind zwischen allen Betriebssystemen kompatibel, außer wenn das Dateisystem die Dateigröße beschränkt und die Unterstützung für große Dateien erwartet.

Eine Datenbank, die in einem Betriebssystem erstellt wurde, kann in einem anderen Betriebssystem verwendet werden, indem die Datei dorthin kopiert wird. Eine mit einem Personal Datenbankserver erstellte Datenbank kann daher auch mit einem Netzwerkserver benutzt werden. Datenbankserver können Datenbanken verwalten, die mit früheren Versionen der Software erstellt wurden, aber Server älterer Versionen können keine neueren Datenbanken verwalten.

### Siehe auch

- „Entity-Relationship-Diagramme anzeigen“ auf Seite 811
- SAP Sybase PowerDesigner – Physical Data Model [*SQL Anywhere 16 - Einführung*]
- „Tabellen, Ansichten und Indizes“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Das Transaktionslog“ auf Seite 135
- „SQL Anywhere-Einschränkungen von Größe und Anzahl“ auf Seite 791

## Hinweise zu Objektnamen

Verwenden Sie keine reservierten Wörter für die Benennung von Datenbankobjekten.

Spaltennamen müssen in Anführungszeichen gesetzt werden, wenn der Spaltenname:

- Andere Zeichen als Buchstaben, Ziffern oder Unterstriche enthält
- Nicht mit einem Buchstaben beginnt
- Mit einem Schlüsselwort identisch ist

### Siehe auch

- „Reservierte Wörter“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Hinweise zu Spalten-Datentypen

Die folgenden Datentypen sind verfügbar:

- Binärdatentypen
- Zeichendatentypen
- Datum- bzw. Uhrzeitdatentypen
- Dezimal-Datentypen
- Domänen (benutzerdefinierte Datentypen)
- Gleitkomma-Datentypen
- Ganzzahl-Datentypen
- Räumliche Datentypen

Jeder Datentyp mit Zeichenfolgen oder binären Zeichenfolgen wie CHAR, VARCHAR, LONG VARCHAR, NCHAR, BINARY, VARBINARY usw. kann zum Speichern großer Objekte wie etwa von Bildern, Textverarbeitungsdokumenten und Audiodateien verwendet werden.

### Siehe auch

- „Hinweise zu BLOBs“ auf Seite 123
- „SQL-Datentypen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## NULL- und NOT NULL-Spalten

Wenn der Spaltenwert für eine Zeile obligatorisch ist, definieren Sie die Spalte als NOT NULL. Andernfalls darf die Spalte den Wert NULL enthalten, was "keinen Wert" bedeutet. Standardmäßig ist NULL zulässig, aber Sie sollten die Spalten explizit als NOT NULL deklarieren, es sei denn, Sie haben einen bestimmten Grund, NULL zuzulassen.

Die Beispieldatenbank enthält eine Tabelle namens "Departments", die über die Spalten "DepartmentID", "DepartmentName" und "DepartmentHeadID" verfügt. Die Definition lautet folgendermaßen:

Spalte	Datentyp	Größe	NULL/NOT NULL	Integritätsregel
DepartmentID	integer	—	NOT NULL	Primärschlüssel
DepartmentName	char	40	NOT NULL	Keine
DepartmentHeadID	integer	—	NULL	Fremdschlüssel

Wenn Sie NOT NULL angeben, muss für jede Zeile in der Tabelle ein Spaltenwert angegeben werden.

#### Siehe auch

- „NULL-Spezialwert“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Suchbedingungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Hinweise zu BLOBs

Ein BLOB ist eine nicht interpretierte Folge von Bytes oder Zeichen, die als Wert in einer Spalte gespeichert wird. Beispiele für BLOBs sind Bild- oder Audiodateien. Obwohl BLOBs normalerweise groß sind, können Sie sie in jedem Datentyp für Zeichenfolgen oder binäre Zeichenfolgen wie etwa CHAR, VARCHAR, NCHAR, BINARY, VARBINARY usw. speichern. Wählen Sie den Datentyp und die Länge abhängig vom Inhalt und der Länge der BLOBs, die Sie speichern wollen.

#### Hinweis

Ein großes Zeichenobjekt (Character Large Object) wird gemeinhin als CLOB bezeichnet, ein großes Binärobjekt (Binary Large Object) als BLOB und die Kombination beider als LOB. In dieser Dokumentation wird nur das Akronym BLOB verwendet.

Wenn Sie eine Spalte zum Speichern von BLOB-Werten erstellen, können Sie einzelne Aspekte der Speicherung steuern. Sie können beispielsweise festlegen, dass BLOBs bis zu einer bestimmten Größe in der Zeile (inline) gespeichert werden, während größere BLOBs außerhalb der Zeile auf Tabellenerweiterungsseiten gespeichert werden. Zusätzlich können Sie festlegen, dass für BLOBs, die außerhalb der Zeile gespeichert werden, die ersten *n* Byte des BLOBs, die auch als Präfix bezeichnet werden, in der Zeile dupliziert werden sollen. Diese Aspekte der Speicherung werden durch die Einstellungen INLINE und PREFIX gesteuert, die in den Anweisungen CREATE TABLE und ALTER TABLE festgelegt werden. Die Werte, die Sie für diese Einstellungen angeben, können unvorhersehbare Auswirkungen auf die Performance oder die Plattenspeicheranforderungen haben.

Wenn weder INLINE noch PREFIX angegeben sind, oder wenn INLINE USE DEFAULT oder PREFIX USE DEFAULT angegeben ist, werden Standardwerte wie folgt angewendet:

- Bei Spalten vom Typ Zeichendaten wie CHAR, NCHAR, LONG VARCHAR und XML ist der Standardwert für INLINE 256 und der Standardwert für PREFIX 8.
- Bei Spalten vom Typ Binärdaten wie BINARY, LONG BINARY, VARBINARY, BIT, VARBIT, LONG VARBIT, BIT VARYING und UUID ist der Standardwert für INLINE 256 und der Standardwert für PREFIX 0.

Es wird empfohlen, die Werte für `INLINE` und `PREFIX` nicht festzulegen, es sei denn, es gibt bestimmte Anforderungen, die durch die Standardwerte nicht erfüllt werden. Die Standardwerte wurden ausgewählt, um die Performance und den Festplattenspeicherbedarf möglichst gut aneinander anzupassen. Die Performance bei der Zeilenverarbeitung kann sich z.B. verschlechtern, wenn Sie `INLINE` auf einen großen Wert setzen und alle BLOBs in der Zeile gespeichert werden. Wenn Sie `PREFIX` zu hoch einstellen, erhöhen Sie den erforderlichen Speicherplatz zum Speichern von BLOBs, da die `PREFIX`-Daten einen BLOB-Abschnitt duplizieren.

Wenn Sie sich dazu entscheiden, Werte für `INLINE` oder `PREFIX` festzulegen, darf die `INLINE`-Länge die Länge der Spalte nicht überschreiten. Ebenso darf die `PREFIX`-Länge die `INLINE`-Länge nicht überschreiten.

Die Präfixdaten für eine komprimierte Spalte werden nicht komprimiert gespeichert, daher ist keine Dekomprimierung erforderlich, wenn alle Daten, die zur Erfüllung einer Anforderung erforderlich sind, im Präfix gespeichert sind.

Informationen über die Standardwerte für die `INLINE`- und `PREFIX`-Klauseln finden Sie unter „[CREATE TABLE-Anweisung](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

### BLOBs gemeinsam nutzen

Falls ein BLOB die `INLINE`-Größe überschreitet und mehr als eine Datenbankseite für die Speicherung benötigt, speichert der Datenbankserver das BLOB so, dass es, falls möglich, durch andere Zeilen in derselben Tabelle referenziert werden kann. Dies wird als gemeinsame Nutzung von BLOBs bezeichnet. Die gemeinsame Nutzung von BLOBs wird intern abgewickelt und soll unnötige Duplizierungen von BLOBs in der Datenbank reduzieren.

BLOBs werden nur dann gemeinsam genutzt, wenn Sie die Werte einer Spalte den Werten einer anderen Spalte gleichsetzen. Zum Beispiel: `UPDATE t column1=column2;` Wenn "column2" in diesem Beispiel BLOBs enthält, werden diese in "column1" nicht dupliziert, sondern es werden Zeiger auf die Werte in "column2" benutzt.

Wenn ein BLOB gemeinsam genutzt wird, hält der Datenbankserver fest, wie viele andere Referenzen für dieses BLOB vorhanden sind. Sobald der Datenbankserver feststellt, dass ein BLOB innerhalb einer Tabelle nicht mehr referenziert wird, wird das BLOB entfernt.

Falls ein BLOB von zwei nicht komprimierten Spalten gemeinsam genutzt wird, dann aber eine der Spalten komprimiert wird, wird das BLOB nicht mehr gemeinsam genutzt.

## Hinweise zur Spaltenkomprimierung

Spalten des Typs `CHAR`, `VARCHAR` und `BINARY` können komprimiert werden, um Speicherplatz zu sparen. Sie können z.B. eine Spalte komprimieren, in der große BLOB-Dateien wie etwa BMPs oder TIFFs gespeichert sind. Die Komprimierung wird mithilfe des Deflate-Komprimierungsalgorithmus durchgeführt. Dabei handelt es sich um den gleichen Algorithmus wie bei der Funktion `COMPRESS`, der auch für ZIP-Dateien unter Windows benutzt wird.

Komprimierte Spalten können sich innerhalb von verschlüsselten Tabellen befinden. In einem solchen Fall werden die Daten zuerst komprimiert und dann verschlüsselt.

Wenn eine Zeichenfolge auf einen Wert komprimiert wird, der nicht um mindestens eine Seite kleiner ist als der ursprüngliche Wert, wird sie als nicht komprimiert gespeichert. Außerdem werden Zeichenfolgen nicht komprimiert, die kleiner sind als der Inline-Wert der Spalte.

Verwenden Sie zum Komprimieren von Spalten die COMPRESS-Klausel der Anweisungen CREATE TABLE und ALTER TABLE.

Mithilfe der Systemprozedur "sa\_column\_stats" können Sie ermitteln, welchen Vorteil Sie durch das Komprimieren einer Spalte erhalten.

#### Siehe auch

- „CREATE TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_column\_stats-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Tabellenverschlüsselung“ auf Seite 1437

## Hinweise zu Integritätsregeln

Obwohl der Datentyp einer Spalte die zulässigen Werte für diese Spalte einschränkt (z.B. nur Zahlen oder Datumsangaben), kann es sinnvoll sein, die zulässigen Werte noch weiter einzuschränken.

Sie können die Werte einer beliebigen Spalte einschränken, indem Sie eine CHECK-Integritätsregel angeben. Eine CHECK-Integritätsregel ist eine Einschränkung, die festgelegte Bedingungen für eine oder mehrere Spalten erzwingt. Sie können jede gültige Bedingung verwenden, die in einer WHERE-Klausel erscheinen kann, um die zulässigen Werte einzuschränken. Die meisten CHECK-Integritätsregeln verwenden die BETWEEN- bzw. die IN-Bedingung.

#### Siehe auch

- „Suchbedingungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenintegrität“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „CHECK-Integritätsregeln in Spalten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „CHECK-Integritätsregeln in Tabellen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbanken erstellen (Sybase Central)

Erstellen Sie eine Datenbank mit Sybase Central.

### Voraussetzungen

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gu geändert werden.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Datenbank erstellen**.
2. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen einer Datenbank**.

## Ergebnisse

Eine Datenbank wird erstellt.

## Siehe auch

- „Verbindungs-IDs“ auf Seite 30
- „Datenbanken erstellen (Dienstprogramm dbinit)“ auf Seite 126
- „Erstellen von Datenbanken für Windows Mobile“ auf Seite 441
- „Datenimport“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Erstellen einer Tabelle“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbanken erstellen (Dienstprogramm dbinit)

Verwenden Sie das Dienstprogramm dbinit, um eine Datenbank zu erstellen.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Mit diesem Dienstprogramm können Sie Befehlszeilenoptionen angeben, um unterschiedliche Einstellungen für die Datenbank festzulegen.

Ein Transaktionslog-Spiegel bietet zusätzlichen Schutz für kritische Daten. Er ermöglicht die vollständige Datenwiederherstellung, wenn ein Datenträgerfehler das Transaktionslog betrifft. Um beim Erstellen einer Datenbank einen Transaktionslog-Spiegel zu verwalten, geben Sie die Option -m an.

## Aufgabe

- Führen Sie einen dbinit-Befehl aus.

## Ergebnisse

Eine Datenbank wird erstellt.

## Beispiel

Um z.B. eine Datenbank namens *company.db* mit einer Seitengröße von 4 kB zu erstellen, geben Sie den folgenden Befehl ein:

```
dbinit -dba DBA,sql -p 4k company.db
```

Mit dem folgenden Befehl (der in einer Zeile eingegeben werden muss) wird eine Datenbank mit dem Namen *company.db* initialisiert, wobei das Transaktionslog auf einem anderen Gerät und ein Spiegel auf einem dritten Gerät gespeichert wird.

```
dbinit -dba DBA,sql -t d:\log-dir\company.log -m  
e:\mirr-dir\company.mlg c:\db-dir\company.db
```

**Siehe auch**

- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Verbindungs-IDs“ auf Seite 30
- „Erstellen von Datenbanken für Windows Mobile“ auf Seite 441
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Transaktionslog-Spiegeldateien“ auf Seite 138

## Vordefinierte DBSpaces

SQL Anywhere verwendet die folgenden DBSpaces für seine Datenbanken:

DBSpace	Name
Haupt-Datenbankdatei	system
Temporäre Datei	temporary oder temp
Transaktionslogdatei	translog
Transaktionslogspiegel	translogmirror

Es ist nicht möglich, benutzerdefinierte DBSpaces mit diesen Namen zu erstellen oder die vordefinierten DBSpaces zu löschen.

Wenn Sie ein Upgrade einer Datenbank der Version 10.0.0 oder früher durchführen, die benutzerdefinierte DBSpaces mit den vordefinierten DBSpace-Namen verwendet, wird angenommen, dass sich alle Referenzen auf diese DBSpaces in SQL-Anweisungen auf die benutzerdefinierten und nicht auf die vordefinierten DBSpaces beziehen. Die einzige Möglichkeit, auf die vordefinierten DBSpaces zu verweisen, besteht darin, die benutzerdefinierten DBSpaces zu löschen oder sie umzubenennen.

Die ALTER DBSPACE-Anweisung unterstützt die vordefinierten DBSpace-Namen, sodass Sie ihnen weiteren Speicherplatz zuordnen können.

Die DB\_EXTENDED\_PROPERTY-Funktion akzeptiert ebenfalls die vordefinierten DBSpace-Namen.

**Siehe auch**

- „ALTER DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DB\_EXTENDED\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Zusätzliche Hinweise zu DBSpaces

### Hinweis

Bei den meisten Datenbanken ist eine Datenbankdatei ausreichend. Für Benutzer von großen Datenbanken können jedoch manchmal zusätzliche Dateien erforderlich werden. Zusätzliche Datenbankdateien sind außerdem praktisch, um zusammengehörige Daten in eigenen Dateien zu gruppieren.

Wenn Sie eine Datenbank initialisieren, enthält sie eine Datenbankdatei. Die erste Datenbankdatei wird als **Hauptdatei** oder **System-DBSpace** bezeichnet. Standardmäßig werden alle Datenbankobjekte und alle Daten in der Hauptdatei gespeichert.

Ein **DBSpace** ist eine zusätzliche Datenbankdatei, die zusätzlichen Speicherplatz für Daten bereitstellt. Eine Datenbank kann in bis zu 13 verschiedenen Dateien gespeichert sein (einer Hauptdatei und 12 DBSpaces). Jede Tabelle muss zusammen mit ihren Indizes in einer Datenbankdatei enthalten sein. Die SQL-Anweisung CREATE DBSPACE fügt der Datenbank eine neue Datei hinzu.

Temporäre Tabellen werden nur im temporären DBSpace ("temporary") erstellt werden.

Es gibt mehrere Methoden, den DBSpace anzugeben, in dem eine Basistabelle oder ein anderes Datenbankobjekt erstellt wird. In der folgenden Aufzählung haben Speicherorte, die durch Methoden definiert werden, die in der Aufzählung zuerst angegeben sind, Vorrang vor den Methoden, die in der Aufzählung weiter unten stehen.

1. IN DBSPACE-Klausel (wenn angegeben)
2. default\_dbspace-Option (wenn eingestellt)
3. DBSpace "system"

Wenn ein DBSpace-Name einen Punkt enthält und nicht in Anführungszeichen steht, generiert der Datenbankserver einen Fehler für den Namen.

Jede Datenbankdatei hat eine zulässige Höchstgröße von  $2^{28}$  (ca. 268 Mio.) Datenbankseiten. So kann beispielsweise eine Datenbankdatei, die mit einer Datenbankseitengröße von 4 kB eingerichtet wurde, zu einer maximalen Größe von einem Terabyte ( $2^{28} \cdot 4$  kB) anwachsen. In der Praxis begrenzt jedoch die zulässige Dateigröße im physischen Dateisystem, in dem die Datei erstellt wurde, die maximale Dateigröße in erheblichem Maße.

Während einige ältere Dateisysteme die Dateigröße auf ein Maximum von 2 GB beschränken, kann in vielen Systemen, wie etwa in Windows unter Verwendung des NTFS-Dateisystems, die gesamte Datenbankdateigröße genutzt werden. Wenn die Datenmenge in der Datenbank die maximale Dateigröße überschreitet, ist es erforderlich, die Daten auf mehr als eine Datenbankdatei zu verteilen. Außerdem können auch aus anderen Gründen als der Dateigrößenbegrenzung mehrere DBSpaces eingerichtet werden, z.B. um zusammengehörige Objekte zu gruppieren.

Sie können die sa\_disk\_free-Systemprozedur verwenden, um Informationen über den für einen DBSpace verfügbaren Speicherplatz abzurufen.

Die SYSDBSPACE-Systemansicht enthält Informationen zu allen DBSpaces für eine Datenbank.

## Vorhandene Datenbanken aufteilen

Wenn Sie vorhandene Datenbankobjekte auf mehrere DBSpaces aufteilen möchten, müssen Sie Ihre Datenbank entladen und die generierte Skriptdatei (standardmäßig mit dem Namen *reload.sql*) ändern, um die Datenbank neu aufzubauen. Fügen Sie in der Datei *reload.sql* IN-Klauseln zu den CREATE TABLE-Anweisungen hinzu, um für alle Tabellen die DBSpaces anzugeben, die nicht in die Hauptdatei aufgenommen werden sollen.

## Siehe auch

- „SQL Anywhere-Einschränkungen von Größe und Anzahl“ auf Seite 791
- „sa\_disk\_free\_space-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SYSDBSPACE-Systemansicht“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Privilegien für DBSpaces

Für DBSpaces wird nur das CREATE-Privileg unterstützt. Das CREATE-Privileg ermöglicht es einem Benutzer, Datenbankobjekte im angegebenen DBSpace zu erstellen. Sie können das CREATE-Privileg für einen DBSpace erteilen, indem Sie eine GRANT CREATE ON-Anweisung ausführen.

Das CREATE-Privileg für DBSpaces verhält sich wie folgt:

- Ein Benutzer, der versucht, ein neues Objekt mit darunterliegenden Daten zu erstellen, muss das CREATE-Privileg für den DBSpace haben, in dem die Daten platziert werden.
- Auch wenn eine GRANT CREATE ON-Anweisung ausgegeben wurde, muss der Benutzer (Berechtigungsempfänger) das CREATE ANY OBJECT-Systemprivileg haben, um neue Datenbankobjekte erstellen zu können.
- Die aktuelle Liste der Objekte, die in spezifischen DBSpaces platziert werden können und das CREATE-Privileg erfordern, umfasst Tabellen, Indizes, Textindizes und materialisierte Ansichten. Objekte wie normale Ansichten und Prozeduren haben keine darunterliegenden Daten und erfordern nicht das CREATE-Privileg.
- Einem Benutzer kann das CREATE-Privileg direkt erteilt werden oder er kann das Privileg durch Mitgliedschaft in einer Rolle erben, der das Privileg erteilt wurde.
- Es ist möglich, PUBLIC das CREATE-Privileg für einen bestimmten DBSpace zu erteilen. In diesem Fall kann jeder Benutzer, der auch das CREATE ANY OBJECT-Systemprivileg hat, Objekte in dem DBSpace erstellen.
- Ein neu erstellter DBSpace erteilt PUBLIC automatisch das CREATE-Privileg für sich selbst.
- Es ist möglich, Privilegien zu entziehen, z.B. um einen DBSpace zu sichern. Privilegien für die internen DBSpaces "system" und "temporary" können ebenfalls verwaltet werden, um den Zugriff zu steuern.
- Das Erstellen von lokalen temporären Tabellen erfordert keine Privilegien. DBSpace-Privilegien wirken sich nicht auf die Erstellung von lokalen temporären Tabellen aus. Das Erstellen von globalen temporären Tabellen erfordert jedoch das CREATE ANY OBJECT-Systemprivileg und das CREATE-Privileg für den DBSpace "temporary".

### Siehe auch

- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DB\_EXTENDED\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „UNLOAD-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## DBSpace-Erstellung

Eine neue Datenbankdatei bzw. ein neuer DBSpace wird entweder von Sybase Central aus oder mithilfe der Anweisung CREATE DBSPACE eingerichtet. Die Datenbankdatei für den neuen DBSpace kann sich auf derselben Festplatte wie die Hauptdatei oder auf einem anderen Datenträger befinden.

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben, um DBSpaces zu erstellen.

Für jede Datenbank können Sie zusätzlich zum Haupt-DBSpace bis zu zwölf weitere DBSpaces einrichten. Ein neu erstellter DBSpace ist leer. Wenn Sie eine neue Tabelle oder einen neuen Index erstellen, können Sie sie oder ihn in einen bestimmten DBSpace platzieren, indem Sie eine IN-Klausel in der CREATE TABLE-Anweisung verwenden oder vor dem Erstellen der Tabelle die Option default\_dbspace setzen. Wenn Sie keine IN-Klausel angeben bzw. die Einstellung der Option default\_dbspace nicht ändern, wird die Tabelle im System-DBSpace erstellt.

Jede Tabelle ist zur Gänze in dem DBSpace enthalten, in dem sie erstellt wird. Standardmäßig erscheinen Indizes in demselben DBSpace wie ihre Tabelle, aber Sie können sie in einen anderen DBSpace setzen, indem Sie mit der CREATE-Anweisung eine IN-Klausel verwenden.

### Siehe auch

- „default\_dbspace-Option“ auf Seite 604
- „CREATE DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE INDEX-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## DBSpaces erstellen (Sybase Central)

Sie können einen DBSpace mit Sybase Central erstellen. Eine einzelne Datenbankdatei reicht für die meisten Datenbanken aus, aber zusätzliche DBSpaces können verwendet werden, um zusätzlichen Speicherplatz für Daten zu schaffen.

### Voraussetzungen

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.

2. Klicken Sie im linken Fensterausschnitt auf **DBSpaces**.
3. Rechtsklicken Sie auf den Ordner und klicken Sie auf **Neu » DBSpace**.
4. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen von DBSpaces**.

### Ergebnisse

Der neue DBSpace erscheint im Ordner **DBSpaces**.

### Siehe auch

- „CREATE DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „default\_dbpace-Option“ auf Seite 604
- „Tabellen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „CREATE INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## DBSpaces erstellen (SQL)

Sie können einen DBSpace mithilfe der CREATE DATABASE-Anweisung erstellen. Eine einzelne Datenbankdatei reicht für die meisten Datenbanken aus, aber zusätzliche DBSpaces können verwendet werden, um zusätzlichen Speicherplatz für Daten zu schaffen.

### Voraussetzungen

Sie müssen das **MANAGE ANY DBSPACE**-Systemprivileg haben.

### Aufgabe

- Führen Sie eine CREATE DBSPACE-Anweisung aus.

### Ergebnisse

Der DBSpace wird im selben Verzeichnis angezeigt wie die Hauptdatenbankdatei, sofern nicht anders angegeben.

### Beispiel

Mit dem folgenden Befehl wird ein neuer DBSpace mit dem Namen "MyLibrary" in der Datei *library.db* in demselben Verzeichnis erstellt, das auch die Hauptdatei enthält:

```
CREATE DBSPACE MyLibrary
AS 'library.db';
```

Mit dem folgenden Befehl wird eine Tabelle "LibraryBooks" erstellt und in den DBSpace "MyLibrary" platziert.

```
CREATE TABLE LibraryBooks (
  title CHAR(100),
  author CHAR(50),
  isbn CHAR(30)
) IN MyLibrary;
```

Der folgende Befehl erstellt einen neuen DBSpace mit Namen "MyLibrary", setzt den Standard-DBSpace auf den DBSpace "MyLibrary" und erstellt anschließend die Tabelle "LibraryBooks" im DBSpace "MyLibrary".

```
CREATE DBSPACE MyLibrary
AS 'e:\\dbfiles\\library.db';
SET OPTION default_dbspace = 'MyLibrary';
CREATE TABLE LibraryBooks (
    title CHAR(100),
    author CHAR(50),
    isbn CHAR(30),
);
```

### Siehe auch

- „CREATE DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „default\_dbspace-Option“ auf Seite 604
- „Tabellen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „CREATE INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Speicherplatz für Datenbankdateien vorab zuweisen (Sybase Central)

Wenn Sie eine neue Datenbankdatei erstellen, können Sie mit Sybase Central Speicherplatz für die Datenbankdatei vorab zuweisen. Durch die Vorabzuweisung von Speicherplatz können die Performance beim Laden großer Datenmengen und die zusammenhängende Speicherung von Datenbankdateien verbessert werden.

### Voraussetzungen

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben.

### Kontext und Bemerkungen

Während Sie die Datenbank verwenden, werden die Datenbankdateien automatisch nach Bedarf vergrößert. Häufiges Ändern von Datenbankdateien kann zu einer starken Dateifragmentierung und daraus resultierenden Performanceproblemen führen. Überdies sind viele kleinere Zuweisungen langsamer als eine große Zuweisung. Wenn Sie mit einer Datenbank mit hoher Änderungsrate arbeiten, können Sie in Sybase Central Festplattenspeicher für DBSpaces oder Transaktionslogs vorab zuweisen.

#### **Tipp**

Nachdem Sie den Festplattenspeicher vorbelegt haben, wird durch das Ausführen eines Dienstprogramms für die Defragmentierung von Festplatten gewährleistet, dass die Datenbankdatei nicht über mehrere unabhängige Bereiche der Festplatte fragmentiert ist. Die Performance kann darunter leiden, wenn die Datenbankdateien stark fragmentiert sind.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plugins her.

2. Klicken Sie im linken Fensterausschnitt auf **DBSpaces**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf den DBSpace und klicken Sie auf **Speicherplatz vorbelegen**.
4. Geben Sie den Umfang des Speicherplatzes an, den Sie DBSpace hinzufügen möchten. Sie können Speicherplatz in den Maßeinheiten Seiten, Byte, Kilobyte (kB), Megabyte (MB), Gigabyte (GB) oder Terabyte (TByte) hinzufügen.
5. Klicken Sie auf **OK**.

### Ergebnisse

Speicherplatz für die Datenbankdatei wird vorab zugewiesen.

### Siehe auch

- „DBSpace-Erstellung“ auf Seite 130
- „ALTER DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927

## Speicherplatz für Datenbankdateien vorab zuweisen (SQL)

Wenn Sie eine neue Datenbankdatei erstellen, können Sie Speicherplatz für die Datenbank vorab zuweisen, indem Sie die DATABASE SIZE-Klausel der CREATE DATABASE-Anweisung verwenden. Durch die Vorabzuweisung von Speicherplatz können die Performance beim Laden großer Datenmengen und die zusammenhängende Speicherung von Datenbankdateien verbessert werden.

### Voraussetzungen

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben.

### Kontext und Bemerkungen

Während Sie die Datenbank verwenden, werden die Datenbankdateien automatisch nach Bedarf vergrößert. Häufiges Ändern von Datenbankdateien kann zu einer starken Dateifragmentierung und daraus resultierenden Performanceproblemen führen. Überdies sind viele kleinere Zuweisungen langsamer als eine große Zuweisung. Wenn Sie mit einer umfangreichen Datenbank mit einer hohen Änderungsrate arbeiten, können Sie Festplattenspeicher für DBSpace bzw. für Transaktionslogs vorab zuweisen, und zwar entweder mit Sybase Central oder mit der ALTER DBSPACE-Anweisung.

#### Tipp

Nachdem Sie den Festplattenspeicher vorbelegt haben, wird durch das Ausführen eines Dienstprogramms für die Defragmentierung von Festplatten gewährleistet, dass die Datenbankdatei nicht über mehrere unabhängige Bereiche der Festplatte fragmentiert ist. Die Performance kann darunter leiden, wenn die Datenbankdateien stark fragmentiert sind.

### Aufgabe

1. Stellen Sie eine Verbindung mit einer Datenbank her.
2. Führen Sie eine ALTER DBSPACE-Anweisung aus.

### Ergebnisse

Speicherplatz für die Datenbankdatei wird vorab zugewiesen.

### Beispiel

Größe des system-DBSpaces um 200 Seiten erhöhen.

```
ALTER DBSPACE system  
ADD 200;
```

Größe des system-DBSpaces um 400 MB erhöhen:

```
ALTER DBSPACE system  
ADD 400 MB;
```

### Siehe auch

- „DBSpace-Erstellung“ auf Seite 130
- „ALTER DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927

## DBSpaces löschen (Sybase Central)

Sie können einen DBSpace mit Sybase Central löschen.

### Voraussetzungen

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben.

Bevor Sie einen DBSpace löschen können, müssen Sie alle Tabellen und Indizes löschen, die den DBSpace verwenden.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Öffnen Sie den Ordner **DBSpaces**.
3. Rechtsklicken Sie auf den DBSpace und klicken Sie auf **Löschen**.

### Ergebnisse

Der DBSpace wird gelöscht.

**Siehe auch**

- „DROP DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DROP TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DROP INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## DBSpaces löschen (SQL)

Sie können einen DBSpace mithilfe der DROP DBSPACE-Anweisung löschen.

**Voraussetzungen**

Sie müssen das MANAGE ANY DBSPACE-Systemprivileg haben.

Bevor Sie einen DBSpace löschen können, müssen Sie alle Tabellen und Indizes löschen, die den DBSpace verwenden.

**Aufgabe**

1. Stellen Sie eine Verbindung mit einer Datenbank her.
2. Führen Sie eine DROP DBSPACE-Anweisung aus.

**Ergebnisse**

Der DBSpace wird gelöscht.

**Siehe auch**

- „DROP DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DROP TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DROP INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Das Transaktionslog

Das **Transaktionslog** ist eine von der Datenbankdatei getrennte Datei. Sie speichert alle Änderungen an der Datenbank. Einfügungen, Aktualisierungen, Löschungen, Festschreibungen, Zurücksetzungen sowie Änderungen am Datenbankschema werden aufgezeichnet. Das Transaktionslog wird manchmal auch als **Vorwärts-Log** (Forward-Log) bzw. als **Redo-Log** bezeichnet.

Das Transaktionslog ist ein Hauptelement bei der Sicherung und Wiederherstellung und zudem ein wesentliches Element für die Datensynchronisation mit MobiLink oder für die Datenreplikation über SQL Remote.

Standardmäßig benutzen alle Datenbanken ein Transaktionslog. Die Verwendung eines Transaktionslogs ist optional, wird aber empfohlen, sofern Sie nicht bestimmte Gründe haben, darauf zu verzichten. Der Betrieb einer Datenbank mit einem Transaktionslog bietet einen größeren Schutz gegen Systemausfälle, bessere Performance und die Möglichkeit, die Daten zu replizieren.

Es wird empfohlen, dass Sie die Datenbankdatei und das Transaktionslog auf getrennten Datenträgern auf dem Computer speichern. Wenn sich der/die DBSpace(s) und das Transaktionslog auf demselben Datenträger befinden und der Datenträger ausfällt, gehen alle Daten verloren. Wenn hingegen die Datenbank und das Transaktionslog auf verschiedenen Datenträgern gespeichert sind, können die Daten nach einem Datenträgerausfall zumindest zum Großteil wiederhergestellt werden, weil Sie entweder über die komplette Datenbank oder über das Transaktionslog (aus dem die Datenbank wiederhergestellt werden kann) verfügen. Siehe „[Datenträgerfehler](#)“ auf Seite 1067.

Der Zeitstempel einer Datenbank oder Transaktionslogdatei wird nur aktualisiert, wenn die Datei wächst oder wenn sie geschlossen wird. Wenn die Vorgänge bewirken, dass die Transaktionslogdatei wächst, ohne dass die Größe der Datenbankdatei zunimmt, ist der Zeitstempel der Transaktionslogdatei neuer als der Zeitstempel der Datenbankdatei. Wenn die Datenbank heruntergefahren wird, werden die Zeitstempel der Transaktionslogdatei und der Datenbank aktualisiert.

### Vorsicht

Die Datenbankdatei und die Transaktionslogdatei müssen sich auf demselben physischen Computer wie der Datenbankserver befinden, oder es muss auf sie über eine SAN- bzw. iSCSI-Konfiguration zugegriffen werden. Wenn sich Datenbankdateien und Transaktionslogdateien in einem entfernten Netzwerkverzeichnis befinden, kann dies zu schlechter Performance, zur Beschädigung von Daten und zur Instabilität des Servers führen. Siehe <http://www.sybase.com/detail?id=1034790>.

## Änderung auf Festplatte schreiben

Wie die Datenbankdatei ist auch das Transaktionslog in **Seiten** strukturiert. Wenn im Transaktionslog eine Änderung registriert wird, erfolgt dies auf einer Seite im Speicher. Die Änderung wird auf die Festplatte geschrieben, sobald eine der folgenden Bedingungen eintritt:

- Die Seite ist voll.
- Eine COMMIT-Anweisung wird ausgeführt.

Damit ist gewährleistet, dass abgeschlossene Transaktionen auf der Festplatte gespeichert werden, die Performance hingegen durch fortdauernde Schreibvorgänge auf der Festplatte nicht beeinträchtigt wird.

Mit Konfigurationsoptionen können erfahrene Benutzer das Verhalten des Transaktionslogs präzise abstimmen. Siehe „[cooperative\\_commits-Option](#)“ auf Seite 596 und „[delayed\\_commits-Option](#)“ auf Seite 606.

### Siehe auch

- „[Hinweise zur Transaktionsloggröße](#)“ auf Seite 138
- „[Datenbankserveroption -m](#)“ auf Seite 265
- „[Datenbankoption -m](#)“ auf Seite 327
- „[sa\\_disk\\_free\\_space-Systemprozedur](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „[delete\\_old\\_logs-Option](#) [*SQL Remote*]“ auf Seite 607

## Speicherorte von Transaktionslogs ändern (Sybase Central)

Sie können den Speicherort eines Transaktionslogs mit Sybase Central ändern. Es kann beispielsweise notwendig sein, das Transaktionslog auf ein anderes Laufwerk auf demselben Computer zu verschieben.

## Voraussetzungen

Die Datenbank darf nicht laufen, während Sie den Speicherort des Transaktionslogs ändern.

### Vorsicht

Die Datenbankdatei und die Transaktionslogdatei müssen sich auf demselben physischen Computer wie der Datenbankserver befinden, oder es muss auf sie über eine SAN- bzw. iSCSI-Konfiguration zugegriffen werden. Wenn sich Datenbankdateien und Transaktionslogdateien in einem entfernten Netzwerkverzeichnis befinden, kann dies zu schlechter Performance, zur Beschädigung von Daten und zur Instabilität des Datenbankservers führen.

Weitere Hinweise finden Sie unter <http://www.sybase.com/detail?id=1034790>.

Die besten Ergebnisse werden erzielt, wenn das Transaktionslog nicht auf derselben Festplatte wie die Datenbankdateien gespeichert wird. Siehe „Das Transaktionslog“ auf Seite 135.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie auf **Extras » SQL Anywhere 16 » Einstellungen der Logdatei ändern**.
3. Befolgen Sie die Anweisungen im **Assistenten zum Ändern der Einstellungen der Logdatei**.

## Ergebnisse

Der Speicherort des Transaktionslogs wird geändert.

### Siehe auch

- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998
- „Das Transaktionslog“ auf Seite 135

## Speicherorte von Transaktionslogs ändern (Befehlszeile)

Sie können den Speicherort des Transaktionslogs mit dem Dienstprogramm dblog ändern. Es kann beispielsweise notwendig sein, das Transaktionslog auf ein anderes Laufwerk auf demselben Computer zu verschieben.

### Voraussetzungen

Die Datenbank darf nicht laufen, während Sie den Speicherort des Transaktionslogs ändern.

## Aufgabe

- Führen Sie den folgenden Befehl aus:

```
dblog -t new-transaction-log-file database-file
```

## Ergebnisse

Der Speicherort des Transaktionslogs wird geändert.

### Siehe auch

- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998
- „Das Transaktionslog“ auf Seite 135

## Hinweise zur Transaktionsloggröße

Die Größe des Transaktionslogs wirkt sich in der Regel auch auf die Zeiten für die Wiederherstellung aus. Sie können das Wachstum der Transaktionslogdatei steuern, indem Sie dafür sorgen, dass alle Tabellen Ihrer Datenbank kompakte Primärschlüssel haben. Wenn Sie Aktualisierungen oder Löschvorgänge in Tabellen durchführen, die keine Primärschlüssel enthalten oder eindeutige Indizes haben, die NULL nicht zulassen, wird der ganze Inhalt der betroffenen Zeile in das Transaktionslog eingetragen. Wenn ein Primärschlüssel definiert ist, muss der Datenbankserver nur die Primärschlüsselspaltenwerte speichern, um eine Zeile eindeutig zu identifizieren. Bei Tabellen mit vielen bzw. breiten Spalten werden die Transaktionslogseiten viel schneller angefüllt, wenn kein Primärschlüssel definiert wurde. Dadurch wird nicht nur mehr Festplattenplatz belegt, die zusätzlichen Schreibvorgänge beeinträchtigen auch die Performance.

Wenn kein Primärschlüssel vorhanden ist, sucht der Server nach einem UNIQUE NOT NULL-Index in der Tabelle (oder nach einer Eindeutigkeits-Integritätsregel). Ein eindeutiger Index, der NULL zulässt, ist nicht ausreichend.

### Siehe auch

- „Datenbankserveroption -m “ auf Seite 265
- „Datenbankoption -m “ auf Seite 327
- „sa\_disk\_free\_space-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „delete\_old\_logs-Option [SQL Remote]“ auf Seite 607

## Transaktionslog-Spiegeldateien

Eine **Transaktionslog-Spiegeldatei** ist eine identische Kopie des Transaktionslogs, die zeitgleich mit dem Haupt-Transaktionslog aktualisiert wird. Wenn eine Datenbank über eine Transaktionslog-Spiegeldatei verfügt, werden alle Änderungen an der Datenbank in das Transaktionslog und in die Transaktionslog-Spiegeldatei geschrieben. Standardmäßig haben Datenbanken keine Transaktionslog-Spiegeldateien.

Eine Transaktionslog-Spiegeldatei bietet zusätzlichen Schutz für kritische Daten. Sie ermöglicht die vollständige Datenwiederherstellung, wenn ein Datenträgerausfall für das Transaktionslog auftritt. Ein Transaktionslog-Spiegel ermöglicht einem Datenbankserver die automatische Validierung des Transaktionslogs beim Start der Datenbank.

Es wird empfohlen, eine Transaktionslog-Spiegeldatei zu verwenden, wenn hoher Datendurchsatz erwartet oder betriebskritische Anwendungen ausgeführt werden. Bei einer konsolidierten Datenbank in

einer SQL Remote-Installation basiert z.B. die Replikation auf dem Transaktionslog. Wenn das Transaktionslog beschädigt ist, kann dies zum Scheitern der Replikation führen.

Wenn Sie einen Transaktionslog-Spiegel verwenden und eine Fehlermeldung erhalten, während versucht wird, in eines der beiden Logs zu schreiben (z.B. weil die Festplatte voll ist), stoppt der Datenbankserver. Der Zweck der Transaktionslog-Spiegelung ist es, die vollständige Wiederherstellbarkeit im Fall eines Datenträgerfehlers auf einem der Logmedien zu gewährleisten. Dieser Zweck würde verfehlt, wenn der Server mit nur einem Transaktionslog weiterarbeiten würde.

Sie können die Option `-fc` beim Starten des Datenbankservers angeben, um eine Callback-Funktion zu implementieren, wenn der Datenbankserver Speichermangel im Dateisystem feststellt.

### **Wo das gespiegelte Transaktionslog gespeichert werden sollte**

Die Performance leidet natürlich unter dem Transaktionslog-Spiegel, da jeder Schreibvorgang in ein Datenbanklog zweimal ausgeführt werden muss. Der Grad der Verschlechterung der Performance hängt von Art und Umfang des Datenbank-Verkehrsaufkommens sowie von der physischen Konfiguration der Datenbank und der Logdatei ab.

Eine Transaktionslog-Spiegeldatei sollte nicht auf demselben Medium wie das Transaktionslog gespeichert werden. Damit wird die Performance verbessert und bei einem Datenträgerausfall enthält die andere Kopie des Logs die Daten für eine Wiederherstellung.

### **Alternativen zu einer Transaktionslog-Spiegeldatei**

Als Alternative zu einer Transaktionslog-Spiegeldatei können auch folgende Konfigurationen verwendet werden:

- Datenbankspiegelung.
- Ein Festplatten-Controller, der für die Hardwarespiegelung konfiguriert ist. Im Allgemeinen ist die Hardwarespiegelung zwar kostenträchtiger als die Softwarespiegelung auf der Betriebssystemebene, bringt aber Performancevorteile.
- Softwarespiegelung auf Betriebssystemebene unter Microsoft Windows.

Live-Sicherungen bieten zusätzliche Sicherheiten mit einigen Ähnlichkeiten zum Transaktionslog-Spiegel.

Informationen zum Erstellen einer Datenbank mit Transaktionslog-Spiegel.

Informationen zum Ändern einer vorhandenen Datenbank für die Verwendung eines Transaktionslog-Spiegels.

### **Siehe auch**

- „Datenbankserveroption `-fc`“ auf Seite 235
- „Datenbankspiegelung“ auf Seite 1467
- „Unterschiede zwischen Live-Sicherungen und Transaktionslogspiegeldateien“ auf Seite 1033
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998

## Transaktionslog-Spiegel für vorhandene Datenbanken starten (Sybase Central)

Verwenden Sie Sybase Central, um einen Transaktionslog-Spiegel für eine vorhandene Datenbank zu starten.

### Voraussetzungen

Sie müssen Zugriff auf die Verzeichnisse haben, in denen sich das Transaktionslog befindet.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie auf **Extras » SQL Anywhere 16 » Einstellungen der Logdatei ändern**.
3. Befolgen Sie die Anweisungen im **Assistenten zum Ändern der Einstellungen der Logdatei**.

### Ergebnisse

Ein Transaktionslog-Spiegel wird für die Datenbank gestartet.

### Siehe auch

- [„Transaktionslog-Dienstprogramm \(dblog\)“ auf Seite 998](#)

## Transaktionslog-Spiegel für vorhandene Datenbanken starten (Befehlszeile)

Mit dem Transaktionslog-Dienstprogramm können Sie den Transaktionslog-Spiegel für eine vorhandene Datenbank verwalten, wenn die Datenbank nicht läuft. Außerdem können Sie das Dienstprogramm dblog verwenden, um die Verwendung eines Transaktionslog-Spiegels durch eine Datenbank zu beenden.

### Voraussetzungen

Sie müssen Zugriff auf die Verzeichnisse haben, in denen sich das Transaktionslog befindet.

### Aufgabe

1. Vergewissern Sie sich, dass die Datenbank nicht läuft.
2. Führen Sie den folgenden Befehl aus:

```
dblog -m mirror-file database-file
```

### Ergebnisse

Ein Transaktionslog-Spiegel wird für die Datenbank gestartet.

**Siehe auch**

- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998

**Verbindungen mit ausstehenden Transaktionen ermitteln (SQL)**

Sie können eine Systemprozedur verwenden, um zu ermitteln, welcher Benutzer ausstehende Transaktionen hat.

**Voraussetzungen**

Sie müssen das Systemprivileg SERVER OPERATOR, MONITOR oder DROP CONNECTION haben.

**Kontext und Bemerkungen**

Wenn Sie eine Sicherung durchführen, bei der das Transaktionslog umbenannt oder gelöscht wird, werden unvollständige Transaktionen in das neue Transaktionslog übertragen.

**Aufgabe**

1. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her.
2. Führen Sie die sa\_conn\_info-Systemprozedur aus:

```
CALL sa_conn_info;
```

**Ergebnisse**

Überprüfen Sie die Spalte **UncommitOps** im Fensterausschnitt **Ergebnisse**, um zu sehen, welche Verbindung nicht festgeschriebene Vorgänge aufweist.

**Nächste Schritte**

Wenn nötig, können Sie die Verbindung des betreffenden Benutzers mit einer DROP CONNECTION-Anweisung trennen.

**Siehe auch**

- „sa\_conn\_info-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 981
- „DROP CONNECTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Checkpoints**

Ein **Checkpoint** ist ein Zeitpunkt, an dem alle nicht festgeschriebenen Seiten (Dirty Pages) auf die Festplatte geschrieben werden und der daher einen bekannten konsistenten Zustand der Datenbank auf der Festplatte darstellt. Nachdem ein Checkpoint gesetzt wurde, wird der Inhalt des Checkpoint-Logs bereinigt. Die leeren Checkpoint-Logseiten bleiben während der laufenden Sitzung im Checkpoint-Log und können für neue Checkpoint-Logdaten wiederverwendet werden. Wenn das Checkpoint-Log größer wird, ist dies auch bei der Datenbankdatei der Fall.

Wenn ein Checkpoint gesetzt wird, befinden sich alle Daten in der Datenbank auf der Festplatte in der Datenbankdatei. Die Informationen in der Datenbankdatei entsprechen denen des Transaktionslogs. Während der Wiederherstellung wird die Datenbank erst bis zum jüngsten Checkpoint wiederhergestellt, danach werden die Änderungen nach diesem Checkpoint übernommen.

Am Ende jeder Sitzung wird ein Protokoll der Checkpoint-Log-Verwendung in der Datenbank geprüft und dazu verwendet, eine geeignete Größe für das Checkpoint-Log bei der nächsten Sitzung zu ermitteln.

Der Datenbankserver kann einen Checkpoint initiieren und während seines Ablaufs andere Vorgänge ausführen. Wenn jedoch bereits ein Checkpoint durchgeführt wird, müssen alle Anweisungen, die einen neuen Checkpoint auslösen, auf den Abschluss des aktuellen Checkpoints warten und können erst danach ausgeführt werden.

### Anweisungen, die implizite oder explizite Checkpoints auslösen

- ALTER INDEX REBUILD-Anweisung. Siehe „ALTER INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- ALTER TABLE-Anweisung - außer wenn die ALTER TABLE-Anweisung eine nullwertfähige Spalte oder eine Integritätsregel zur Erhaltung der referenziellen Integrität hinzufügt und die Seiten der Tabelle nicht physisch verändert. Siehe „ALTER TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- BACKUP-Anweisung. Siehe „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- CHECKPOINT-Anweisung. Siehe „CHECKPOINT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- COMMIT-Anweisung - wenn die Datenbank nicht über ein Transaktionslog verfügt. Siehe „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- CREATE DBSPACE-Anweisung. Siehe „CREATE DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- CREATE INDEX-Anweisung - bei Verwendung zum Erstellen eines Indexes für eine Funktion (einer impliziten berechneten Spalte). Siehe „CREATE INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- DROP DBSPACE-Anweisung. Siehe „DROP DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- DROP TABLE-Anweisung und DROP MATERIALIZED VIEW-Anweisung - nur wenn die Tabelle oder Ansicht mindestens eine Zeile enthält. Siehe „DROP TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)] und „DROP MATERIALIZED VIEW-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- LOAD TABLE-Anweisung. Siehe „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

- REFRESH MATERIALIZED VIEW-Anweisung. Siehe „REFRESH MATERIALIZED VIEW-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- REORGANIZE TABLE-Anweisung. Siehe „REORGANIZE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

#### Siehe auch

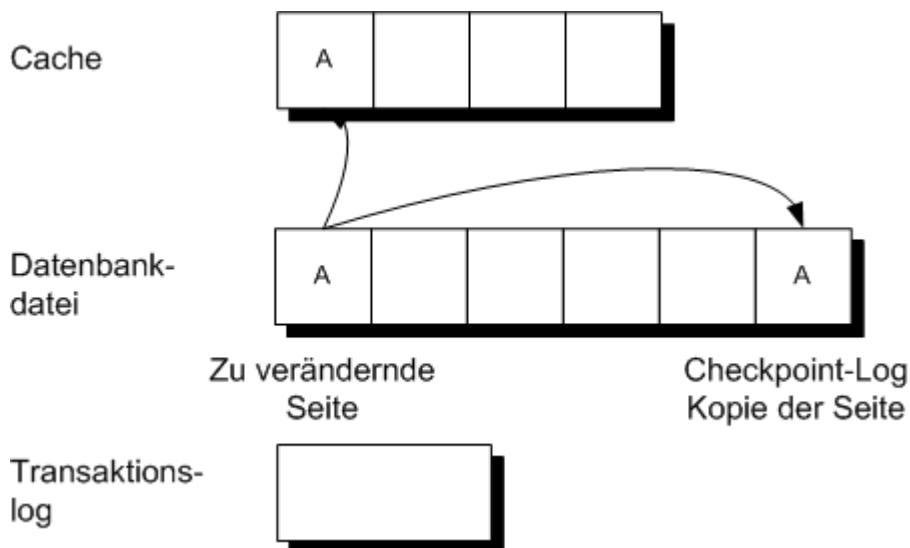
- „Einschränkungen für die Sicherung und Wiederherstellung von Daten“ auf Seite 1036
- „Sicherungskomponenten“ auf Seite 1076
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077
- „Checkpoint-Logs“ auf Seite 143

## Checkpoint-Logs

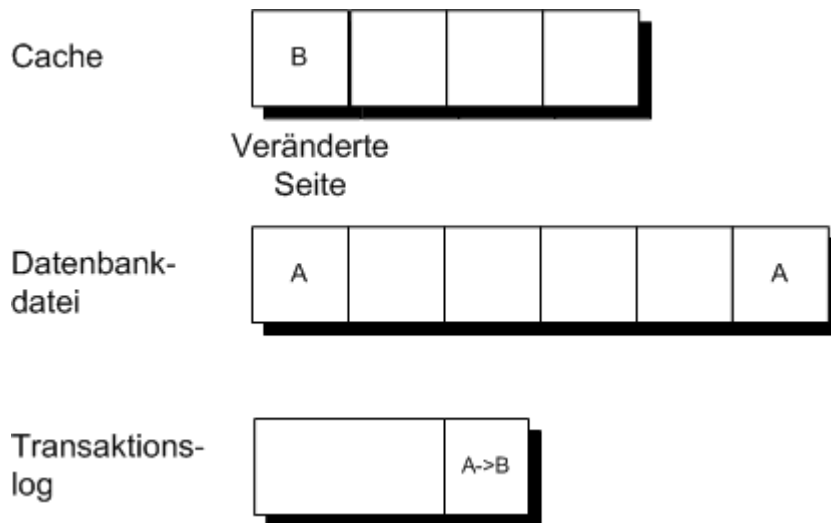
Die Datenbankdatei besteht aus Seiten. Diese Seiten sind Abschnitte der Festplatte mit fester Größe. Das **Checkpoint-Log** befindet sich am Ende der Datenbankdatei und wird im System-DBSpace gespeichert. Seiten werden erforderlichenfalls dem Checkpoint-Log während einer Sitzung hinzugefügt. Am Ende der Sitzung wird ein Protokoll der Checkpoint-Log-Verwendung in der Datenbank gespeichert. Dieses Protokoll wird verwendet, um eine geeignete Größe für das Checkpoint-Log in zukünftigen Sitzungen zu bestimmen.

Bevor eine Seite aktualisiert (somit **dirty**) wird, führt der Datenbankserver immer folgende Maßnahmen durch:

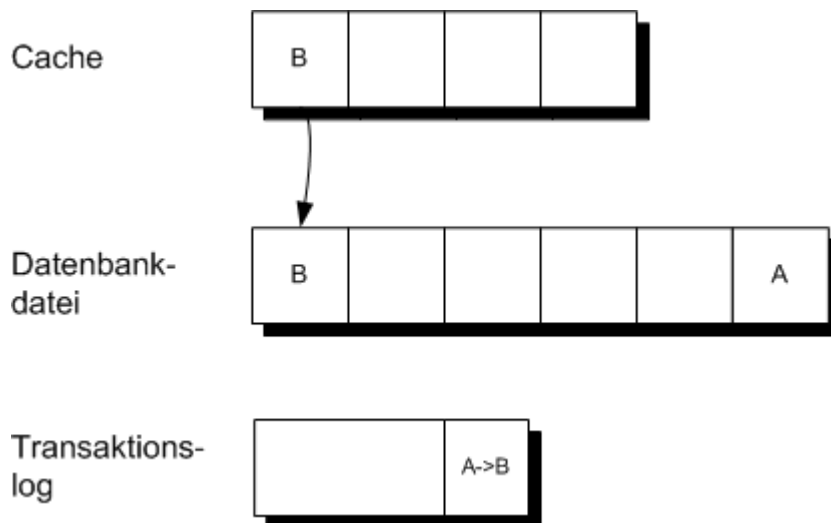
- Er liest die Seite in den Speicher, wo sie im Datenbankcache untergebracht wird.
- Er stellt eine Kopie der Originalseite her. Diese kopierten Seiten sind das Checkpoint-Log.



Änderungen der Seite werden in die Kopie im Cache eingetragen. Aus Performancegründen werden sie nicht sofort in die Datenbankdatei auf der Festplatte geschrieben.



Wenn der Cache voll ist, kann die geänderte Seite auf die Festplatte geschrieben werden. Die Kopie im Checkpoint-Log bleibt aber unverändert.



#### Siehe auch

- „Einschränkungen für die Sicherung und Wiederherstellung von Daten“ auf Seite 1036
- „Sicherungskomponenten“ auf Seite 1076
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077
- „Checkpoints“ auf Seite 141

## Die Dienstprogrammdatenbank

Bei der **Dienstprogrammdatenbank** handelt es sich um eine Phantomdatenbank, die physisch nicht vorhanden ist. Die Dienstprogrammdatenbank hat keine Datenbankdatei und kann deshalb keine Daten enthalten. Diese Funktion ermöglicht Ihnen Folgendes:

- Sie können Anweisungen zur Datenbankdateiverwaltung ausführen, z.B. CREATE DATABASE, ohne eine Verbindung mit einer vorhandenen physischen Datenbank herstellen zu müssen.
- Sie können Werte von Verbindungseigenschaften und Servereigenschaften mithilfe der Dienstprogrammdatenbank abrufen.
- Sie können eine Verbindung mit einem laufenden Datenbankserver herstellen, wenn es nicht möglich ist, eine Verbindung mit der Datenbank herzustellen. Beispiel: In einem Spiegelungssystem können Sie eine Verbindung mit der Dienstprogrammdatenbank herstellen, um einen Spiegelungsserver zu stoppen oder zu erzwingen, dass eine bestimmte Datenbank zum Primärserver wird.

Die Dienstprogrammdatenbank heißt **utility\_db**. Wenn Sie versuchen, eine Datenbank mit diesem Namen zu erstellen oder zu starten, schlägt der Vorgang fehl.

Die Dienstprogrammdatenbank hat einen Benutzer namens **DBA**. Das Kennwort für den DBA-Benutzer wird mit der Datenbankserveroption -su festgelegt. Sie können die Datenbankserveroption -su verwenden, um das Kennwort zur Dienstprogrammdatenbank für den DBA-Benutzer festzulegen oder um Verbindungen mit der Dienstprogrammdatenbank zu deaktivieren. Wenn die Option -su nicht beim Starten der Dienstprogrammdatenbank angegeben wird, unterscheiden sich die Anforderungen für die Benutzer-ID und das Kennwort beim Personal Server und beim Netzwerkserver.

Sie können die Dienstprogrammdatenbank auf einem Datenbankserver starten, indem Sie beim Herstellen der Verbindung mit dem Server utility\_db als Datenbanknamen angeben.

## Zulässige Anweisungen für die Dienstprogrammdatenbank

Nur die folgenden Anweisungen können ausgeführt werden, wenn Sie mit der Dienstprogrammdatenbank verbunden sind:

- ALTER DATABASE *Datenbankdatei* ALTER TRANSACTION LOG.
- ALTER DATABASE *Datenbankname* FORCE START
- CREATE DATABASE-Anweisung.
- CREATE DECRYPTED DATABASE-Anweisung.
- CREATE DECRYPTED FILE-Anweisung.
- CREATE ENCRYPTED DATABASE-Anweisung.
- CREATE ENCRYPTED FILE-Anweisung.
- DROP DATABASE-Anweisung.
- CREATE USER DBA IDENTIFIED BY *neues\_Kennwort*.
- RESTORE DATABASE-Anweisung.
- REVOKE CONNECT FROM DBA.
- SET TEMPORARY OPTION progress\_messages = [ OFF | RAW | FORMATTED ].
- SELECT-Anweisung ohne FROM- oder WHERE-Klausel.
- START DATABASE-Anweisung.
- STOP DATABASE-Anweisung.
- STOP SERVER-Anweisung.

## Beispiele

Nachdem Sie eine Verbindung mit der Dienstprogrammdatenbank hergestellt haben, wird durch die folgende Anweisung eine Datenbank namens *new.db* im Verzeichnis *c:\temp* erstellt.

```
CREATE DATABASE DBA USER 'DBA' DBA PASSWORD 'sql' 'c:\\temp\\new.db';
```

Wenn Sie die folgende Anweisung in der Dienstprogrammdatenbank ausführen, wird die Standardkollationssequenz zurückgegeben, die beim Erstellen einer Datenbank verwendet wird:

```
SELECT PROPERTY( 'DefaultCollation' );
```

## Die Datei *util\_db.ini* und Netzwerk-Datenbankserver (nicht mehr empfohlen)

### Hinweis

Die Datei *util\_db.ini* wird nicht mehr empfohlen. Sie sollten die Serveroption `-su` verwenden, um das Kennwort für den Benutzer DBA der Dienstprogrammdatenbank anzugeben. Siehe [„Datenbankserveroption -su“ auf Seite 289](#).

Die Verwendung der *util\_db.ini*-Datei hängt von der physischen Sicherheit des Host-Computers für den Datenbankserver ab, da die Datei *util\_db.ini* problemlos mit einem Texteditor gelesen werden kann.

Beim Netzwerkserver können Sie sich nur mit der Dienstprogrammdatenbank verbinden, wenn Sie `-su` angeben oder *util\_db.ini* verwenden. Wenn Sie *util\_db.ini* verwenden, enthält die Datei das Kennwort und ist im selben Verzeichnis wie die Datenbankserver-Programmdatei gespeichert. Sie enthält folgenden Text:

```
[UTILITY_DB]
PWD=password
```

Um den Inhalt der Datei *util\_db.ini* vor zufälligem Direktzugriff zu schützen, können Sie Dateien mithilfe des Dienstprogramms zum Verschleiern der Befehlsdatei (dbfhide) mit einer einfachen Verschlüsselung versehen. Sie können auch Betriebssystemfunktionen verwenden, um den Zugriff auf das Serverdateisystem zu begrenzen.

Weitere Informationen zur Verschleierung von .ini-Dateien finden Sie unter [„Inhalte von .ini-Dateien verbergen“ auf Seite 489](#).

### Siehe auch

- „Einen Datenbankserver in einem Spiegelungssystem stoppen“ auf Seite 1490
- „Fehlerbehandlung: Primärserver kann nicht neu gestartet werden“ auf Seite 1500
- „Datenbankserveroption -gu “ auf Seite 255

## Verbindung mit der Dienstprogrammdatenbank herstellen

Über eine Verbindung mit der Dienstprogrammdatenbank können Sie Anweisungen zur Datenbankdateiverwaltung ausführen, Verbindungs- und Servereigenschaften abfragen sowie eine Verbindung mit einem laufenden Datenbankserver herstellen, wenn es nicht möglich ist, eine Verbindung mit der Datenbank herzustellen.

### Voraussetzungen

Die Datenbankserveroption -su gibt das Kennwort für die Dienstprogrammdatenbank an. Um eine Verbindung mit einer Dienstprogrammdatenbank auf einem Server herzustellen, der mit der Option -su gestartet wurde, benötigen Sie das durch die Option -su festgelegte Kennwort.

Wenn die Datenbankserveroption -su für einen Netzwerkserver nicht angegeben wurde, können Sie keine Verbindung mit der Dienstprogrammdatenbank herstellen.

Wenn die Datenbankserveroption -su für einen Personal Server nicht angegeben wurde, können Sie eine Verbindung mit der Dienstprogrammdatenbank herstellen und Sie benötigen kein Kennwort.

### Kontext und Bemerkungen

Sie haben einen laufenden Datenbankserver und Sie möchten eine Verbindung mit dessen Dienstprogrammdatenbank herstellen.

Wenn es sich bei dem Datenbankserver um einen Netzwerkserver (dbsrv16) handelt, wurde er mit der Option -su gestartet und Sie haben das entsprechende Kennwort.

```
dbsrv16 -n server-name -su password
```

Wenn es sich bei dem Datenbankserver um einen Personal Server (dbeng16) handelt, wurde er entweder mit der Option -su gestartet und die Dienstprogrammdatenbank hat ein Kennwort oder er wurde ohne die Option -su gestartet und die Dienstprogrammdatenbank hat kein Kennwort.

```
dbeng16 -n server-name
```

**Aufgabe**

1. Starten Sie Interactive SQL oder Sybase Central.
2. Geben Sie im Fenster **Verbinden** die folgenden Daten an.
  - a. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - b. Im Feld **Kennwort** geben Sie Folgendes ein:

Option	Aktion
Personal Server (dbeng16)	Wenn die Option -su nicht angegeben wurde, geben Sie ein beliebiges nicht leeres Kennwort ein. Das Kennwort selbst wird nicht geprüft, aber das Feld darf nicht leer sein.  Wenn die Option -su angegeben wurde, geben Sie das festgelegte Kennwort ein.
Netzwerkserver (dbsrv16)	Geben Sie das durch die Option -su angegebene Kennwort ein.

- c. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**.
3. Im Feld **Datenbankname** geben Sie **utility\_db** ein.
4. Im Feld **Servername** geben Sie *Servername* ein.
5. Klicken Sie auf **Verbinden**.

**Ergebnisse**

Interactive SQL stellt eine Verbindung mit der Dienstprogrammdatenbank auf dem Personal Server bzw. Netzwerkserver her.

Wenn Sie mit der Dienstprogrammdatenbank verbunden sind und REVOKE CONNECT FROM DBA ausführen, werden zukünftige Verbindungen mit der Dienstprogrammdatenbank deaktiviert. Das bedeutet, dass keine weiteren Verbindungen mit der Dienstprogrammdatenbank hergestellt werden können, es sei denn, Sie verwenden eine Verbindung, die vor dem Ausführen von REVOKE CONNECT bestanden hat, oder Sie starten den Datenbankserver neu.

**Siehe auch**

- „Datenbankverbindungen“ auf Seite 5
- „Datenbankserveroption -su “ auf Seite 289
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Einen Datenbankserver in einem Spiegelungssystem stoppen“ auf Seite 1490
- „Fehlerbehandlung: Primärserver kann nicht neu gestartet werden“ auf Seite 1500
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbanken löschen (Sybase Central)

Wenn Sie eine Datenbank mit Sybase Central löschen, werden alle Tabellen und Daten von der Festplatte gelöscht, einschließlich des Transaktionslogs, in dem Änderungen an der Datenbank erfasst werden. Alle Datenbankdateien sind schreibgeschützt, damit ein irrtümliches Ändern oder Löschen von Datenbankdateien verhindert wird.

### Voraussetzungen

Die zu löschende Datenbank darf nicht laufen, wenn der **Assistent zum Löschen einer Datenbank** verwendet wird.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Datenbank löschen**.
2. Befolgen Sie die Anweisungen des Assistenten.

### Ergebnisse

Die Datenbank wird gelöscht.

### Siehe auch

- „Datenbankserveroption -gu “ auf Seite 255
- „Löschen-Dienstprogramm (dberase)“ auf Seite 916
- „DROP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindung mit der Dienstprogrammdatenbank herstellen“ auf Seite 147
- „Windows Mobile-Datenbanken über die Benutzeroberfläche des Geräts löschen“ auf Seite 450

## Datenbanken löschen (Dienstprogramm dberase)

Wenn Sie eine Datenbank mit dem Dienstprogramm dberase löschen, werden alle Tabellen und Daten von der Festplatte gelöscht, einschließlich des Transaktionslogs, in dem Änderungen an der Datenbank erfasst werden. Alle Datenbankdateien sind schreibgeschützt, damit ein irrtümliches Ändern oder Löschen von Datenbankdateien verhindert wird.

### Voraussetzungen

Die zu löschende Datenbank darf nicht laufen, wenn das Dienstprogramm dberase verwendet wird.

### Kontext und Bemerkungen

Das Dienstprogramm dberase löscht keine DBSpaces. Verwenden Sie zum Löschen von DBSpaces die DROP DBSPACE-Anweisung.

### Aufgabe

- Führen Sie das Dienstprogramm dberase aus.

### Ergebnisse

Die Datenbank wurde gelöscht.

### Nächste Schritte

Verwenden Sie ggf. die DROP DBSPACE-Anweisung.

### Beispiel

Mit dem folgenden Befehl wird die Datenbank "temp" gelöscht.

```
dberase c:\temp\temp.db
```

### Siehe auch

- „Datenbankserveroption -gu“ auf Seite 255
- „Löschen-Dienstprogramm (dberase)“ auf Seite 916
- „DROP DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindung mit der Dienstprogrammdatenbank herstellen“ auf Seite 147
- „Windows Mobile-Datenbanken über die Benutzeroberfläche des Geräts löschen“ auf Seite 450

## SQL Anywhere-Datenbankserver

### SQL Anywhere-Datenbankserver

Es gibt zwei Versionen des SQL Anywhere-Datenbankservers: **Personal Server** (dbeng16) und **Netzwerkserver** (dbsrv16). Eine mit einem Personal Datenbankserver erstellte Datenbank kann mit einem Netzwerk-Datenbankserver benutzt werden und umgekehrt. Die Engine für die Verarbeitung von Anforderungen ist beim Personal Server und Netzwerkserver identisch und beide unterstützen genau die gleiche SQL-Sprache und viele identische Datenbankfunktionen. Allerdings bestehen auch einige Unterschiede zwischen den beiden Servern.

- **Der Personal Datenbankserver** Diese Programmdatei wird für Einzelbenutzer auf demselben Computer bereitgestellt, z. B. als eingebetteter Datenbankserver. Sie unterstützt keine Client/Server-Kommunikation über ein Netzwerk.

Unter Windows-Betriebssystemen mit Ausnahme von Windows Mobile lautet der Name der Programmdatei des Personal Servers *dbeng16.exe*. Unter Unix-Betriebssystemen lautet der Name *dbeng16*. Der Personal Server wird unter Windows Mobile nicht unterstützt.

- **Der Netzwerk-Datenbankserver** Dieses Programm unterstützt Client/Serverkommunikation über ein Netzwerk und ist für den Mehrbenutzerbetrieb vorgesehen.

Unter Windows-Betriebssystemen einschließlich Windows Mobile lautet der Name der Programmdatei des Netzwerkserver *dbsrv16.exe*. Unter Linux- und Unix-Betriebssystemen lautet der Name *dbsrv16*.

## Anforderungen an die Netzwerksoftware

Wenn Sie einen SQL Anywhere-Netzwerk-Datenbankserver einsetzen, muss die betreffende Netzwerksoftware installiert sein und ausgeführt werden.

Der SQL Anywhere-Netzwerkserver ist für die Betriebssysteme Windows, Linux, Unix und Mac OS X verfügbar.

SQL Anywhere unterstützt das TCP/IP-Netzwerkprotokoll.

## Siehe auch

- „Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203
- „Unterschiede zwischen Netzwerkserver und Personal Server“ auf Seite 151

## Unterschiede zwischen Netzwerkserver und Personal Server

Die folgende Tabelle enthält eine Liste der gängigen Datenbankserverfunktionen und der Unterschiede zwischen Personal Server und Netzwerkserver.

Funktion	Netzwerk-Datenbankserver (dbsrv16)	Personal Datenbankserver (dbeng16)
Checkpoints	Das CHECKPOINT-Systemprivileg ist erforderlich, um die CHECKPOINT-Anweisung verwenden zu können.	Es sind keine Systemprivilegien erforderlich, um die CHECKPOINT-Anweisung verwenden zu können.
Komprimierung von Kommunikationspaketen	Unterstützt.	Nicht unterstützt.
Verbindung mit der Dienstprogramm-datenbank herstellen	Standardmäßig werden keine Verbindungen zur Dienstprogramm-Datenbank zugelassen. Sie müssen die Option -su verwenden, um das Kennwort für die Verbindung mit der Dienstprogramm-datenbank anzugeben. Siehe „Datenbankserveroption -su“ auf Seite 289.	Standardmäßig sind Verbindungen zur Dienstprogramm-datenbank mit der Benutzer-ID DBA und einem Kennwort zulässig.
Verbindungsarten	Über gemeinsam genutzten Speicher und TCP/IP standardmäßig.	Über gemeinsam genutzten Speicher standardmäßig. Verwenden Sie zum Verbinden mit dem TCP/IP-Protokoll die Option -x. Siehe „Datenbankserveroption -x“ auf Seite 305.

Funktion	Netzwerk-Datenbankserver (dbsrv16)	Personal Datenbankserver (dbeng16)
Datenbankspiegelung	Unterstützt. Siehe „Datenbankspiegelung“ auf Seite 1467.	Nicht unterstützt.
LDAP als Namensserver	Kann nur mit RSA-Verschlüsselung verwendet werden. Siehe „Verbindungen mit LDAP als Namensserver“ auf Seite 109.	Nicht unterstützt. Nicht zu wechseln mit der LDAP-Benutzerauthentifizierung, die unterstützt wird.
Optimierung der Multiprogramming-Stufe	Unterstützt. Siehe „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175.	Nicht unterstützt.
Netzwerk-kommunikation	Unterstützt.	Nicht unterstützt.
Anzahl von Verbindungen	Begrenzt durch die Lizenz. Siehe „Editionen und Lizenzierung“ [SQL Anywhere 16 - Einführung].	Maximum von zehn gleichzeitigen Verbindungen.
Anzahl der CPUs	Begrenzt durch die Lizenz.	Maximal vier Prozessorkerne auf einer CPU.
Scale-Out mit Schreibschutz	Unterstützt. Siehe „SQL Anywhere-Scale-Out mit Schreibschutz“ auf Seite 1536.	Nicht unterstützt.
Windows Mobile	Unterstützt. Siehe „SQL Anywhere für Windows Mobile“ auf Seite 423.	Nicht unterstützt.

### Server- und Datenbankoptionen

Die folgenden Server- und Datenbankoptionen werden *nur* vom Netzwerk-Datenbankserver unterstützt.

- „Datenbankserveroption -gna “
- „Datenbankserveroption -gnh “
- „Datenbankserveroption -gnl “
- „Datenbankserveroption -gns “
- „Datenbankserveroption -pc “
- „Datenbankserveroption -pt “
- „Datenbankoption -sm (nicht mehr empfohlen)“
- „Datenbankoption -sn “
- „Datenbankserveroption -xa “
- „Datenbankserveroption -xf “
- „Datenbankoption -xp“

## Datenbankservereigenschaften

Die folgenden Datenbankservereigenschaften werden *nur* vom Netzwerk-Datenbankserver unterstützt.

- [AutoMultiProgrammingLevel-Servereigenschaft](#)
- [AutoMultiProgrammingLevelStatistics-Servereigenschaft](#)
- [MaxMultiProgrammingLevel-Servereigenschaft](#)
- [MinMultiProgrammingLevel-Servereigenschaft](#)
- [UniqueClientAddresses-Servereigenschaft](#)

## Datenbankserver starten

Wie Sie den Datenbankserver starten, richtet sich nach dem von Ihnen benutzten Betriebssystem. Sie können Befehle auch auf unterschiedliche Weise eingeben, je nachdem welches Betriebssystem Sie benutzen:

- Führen Sie den Befehl an einer Eingabeaufforderung aus.
- Legen Sie den Befehl in einem Tastenkürzel oder in einer Verknüpfung auf dem Desktop ab.
- Führen Sie den Befehl in einer Batchdatei aus.
- Sie können den Befehl als StartLine-Verbindungsparameter (START) in eine Verbindungszeichenfolge einbeziehen.

Je nach Plattform gibt es leichte Unterschiede, wie Sie Basisbefehle angeben.

### Hinweis

- Wenn nicht anders angegeben, starten diese Befehle den Netzwerkserver (**dbsrv16**). Wenn Sie einen Personal Server starten möchten, ersetzen Sie **dbsrv16** durch **dbeng16**.
- Wenn sich die Datenbankdatei im Startverzeichnis für den Befehl befindet, brauchen Sie keinen *path* anzugeben.
- Wenn Sie mit *Datenbankdatei* keine Dateierweiterung angeben, wird die Erweiterung *.db* angenommen.

## Nachfolgend finden Sie Beispiele zum Starten eines Datenbankservers

Befehl	Kommentare
Klicken Sie unter Windows auf <b>Start » Programme » SQL Anywhere 16 » SQL Anywhere 16 » Personal Server</b>	Das Fenster <b>Startoptionen für den Server</b> erscheint. Dort können Sie angeben, dass ein Personal Datenbankserver (Programm dbeng16) gestartet werden soll. Sie können auch eine Datenbank auf dem Datenbankserver starten.

Befehl	Kommentare
Klicken Sie unter Windows auf <b>Start » Programme » SQL Anywhere 16 » SQL Anywhere » Netzwerkservers</b>	Das Fenster <b>Startoptionen für den Server</b> erscheint. Dort können Sie Informationen für den Start eines Netzwerk-Datenbankservers (Programm dbsrv16) eingeben. Sie können auch eine Datenbank auf dem Datenbankserver starten.
<code>dbsrv16 demo</code>	Verwenden Sie einen Datenbankdatei-Namen in der Verbindungszeichenfolge.  Führen Sie diesen Befehl in dem Verzeichnis aus, in dem sich <i>demo.db</i> befindet, um sowohl einen Netzwerkserver als auch die Datenbank <i>demo.db</i> zu starten:
<code>dbsrv16 path  \database-file</code>	Dieser Befehl startet den Datenbankserver unter Windows Mobile.  Wenn Sie keine Datenbankdatei angeben, wird das Fenster <b>Startoptionen für den Server</b> geöffnet, in dem Sie mit <b>Durchsuchen</b> eine Datenbankdatei auswählen können.

**Siehe auch**

- „Verbindungsparameter StartLine (START)“ auf Seite 385
- „Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203
- „Netzwerkprotokolloptionen“ auf Seite 388
- „SQL-Skriptdateien“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Fehlerbehandlung beim Datenbankserverstart“ auf Seite 1109

## Datenbankserver stoppen

Sie können den Datenbankserver folgendermaßen stoppen:

- Klicken Sie im Meldungsfenster des Datenbankservers auf **Herunterfahren**.
- Das Dienstprogramm dbstop verwenden.  
Das Dienstprogramm dbstop ist in Batchdateien sinnvoll, oder wenn Sie einen Server auf einem anderen Computer stoppen wollen. Es benötigt eine Verbindungszeichenfolge in seinem Befehl.
- Standardmäßig automatisch herunterfahren, wenn die Anwendung die Verbindung trennt.
- Q drücken, wenn das Meldungsfenster des Datenbankservers unter Unix aktiv ist.

## Datenbankserver stoppen (Dienstprogramm dbstop)

Sie können einen Datenbankserver mit dem Dienstprogramm dbstop stoppen.

## Voraussetzungen

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption `-gk` geändert werden.

## Kontext und Bemerkungen

Das Dienstprogramm `dbstop` ist in Batchdateien sinnvoll, oder wenn Sie einen Server auf einem anderen Computer stoppen wollen. Es benötigt eine Verbindungszeichenfolge in seinem Befehl.

## Aufgabe

- Führen Sie an einer Eingabeaufforderung eine Anweisung ähnlich der folgenden mit dem Dienstprogramm `dbstop` aus, wobei *server-name* der Name des Servers ist, den Sie stoppen möchten, und *user-ID* und *password* die Verbindungsparameter sind:

```
dbstop -c "Server=server-name;UID=user-ID;PWD=password"
```

## Ergebnisse

Der Datenbankserver wird gestoppt.

## Beispiel

Starten Sie einen Datenbankserver. Führen Sie den folgenden Befehl im SQL Anywhere-Installationsverzeichnis aus, um einen Server namens Ottawa mit der Beispieldatenbank zu starten:

```
dbsrv16 -n Ottawa "%SQLANYAMP16%\demo.db"
```

Stoppen Sie den Server mit `dbstop`:

```
dbstop -c "Server=Ottawa;UID=DBA;PWD=sql"
```

## Siehe auch

- „Datenbankserveroption `-gk`“ auf Seite 242
- „Serverstopp-Dienstprogramm (`dbstop`)“ auf Seite 984

## Wer kann einen Datenbankserver stoppen?

Wenn Sie einen Datenbankserver starten, können Sie mithilfe der Option `-gk` festlegen, welche Privilegien Benutzer benötigen, um den Server mit `dbstop` stoppen zu können. Bei Personal Datenbankservern ist der Standardwert "all". Standardmäßig ist für Netzwerk-Datenbankserver das SERVER OPERATOR-Systemprivileg erforderlich, aber Sie können den Wert auch auf "all" oder "none" setzen. (Allerdings kann jeder am Computer auf **Herunterfahren** im Meldungsfenster des Datenbankservers klicken.)

## Siehe auch

- „Datenbankserveroption `-gk`“ auf Seite 242

## Herunterfahren der Betriebssystemsitzung

Wenn Sie eine Betriebssystemsitzung schließen, in der ein Datenbankserver läuft, oder wenn Sie einen Betriebssystembefehl benutzen, um den Datenbankserver zu stoppen, fährt der Server zwar herunter, jedoch nicht sauber. Wenn die Datenbank das nächste Mal geladen wird, ist eine Wiederherstellung erforderlich, die automatisch durchgeführt wird.

Schließen Sie daher den Datenbankserver, bevor Sie eine Betriebssystemsitzung schließen.

Nachstehend finden Sie Beispiele für Befehle, die einen Server nicht ordnungsgemäß herunterfahren:

- Prozess im Windows Task-Manager stoppen
- Einen Unix-Befehl "Abbrechen" ("slay" bzw. "kill") verwenden

### Siehe auch

- [„Sicherung und Datenwiederherstellung“ auf Seite 1027](#)

## Datenbanken starten und stoppen

Ein Datenbankserver kann mit mehreren gleichzeitig geladenen Datenbanken betrieben werden. Sie können Datenbanken und den Datenbankserver folgendermaßen zur selben Zeit starten:

```
dbsrv16 demo sample
```

### Vorsicht

Die Datenbankdatei muss sich auf demselben Computer wie der Datenbankserver befinden. Das Verwalten einer Datenbankdatei, die auf einem Netzlaufwerk liegt, kann zu einer Beschädigung der Datei führen.

### Datenbank auf einem laufenden Server starten

Sie können Datenbanken auch starten, nachdem ein Server gestartet wurde. Dazu gibt es folgende Möglichkeiten:

- Stellen Sie bei bestehender Verbindung zu einem Server mit dem DatabaseFile-Verbindungsparameter (DBF) eine Verbindung mit einer Datenbank her. Über den Verbindungsparameter DatabaseFile (DBF) wird die für eine neue Verbindung zu verwendende Datenbankdatei angegeben. Die Datenbankdatei wird auf dem aktuellen Server geladen.
- Verwenden Sie die START DATABASE-Anweisung.
- Wählen Sie in Sybase Central einen Server aus und klicken Sie auf **Datei » Datenbank starten**.

### Einschränkungen

- Der Server hält Datenbank-Informationen im Speicher, indem er Seiten einer feststehenden Größe benutzt. Wenn ein Server gestartet wurde, können Sie keine Datenbank starten, die eine größere Seitengröße hat als der Server.

- Die Serveroption -gd bestimmt, welche Privilegien zum Starten und Stoppen von Datenbanken erforderlich sind.

**Siehe auch**

- „Verbindungen mit eingebetteten Datenbanken“ auf Seite 28
- „Verbindungsparameter DatabaseFile (DBF)“ auf Seite 351
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Hinweise zur maximalen Seitengröße“ auf Seite 160

## Datenbanken ohne Verbinden starten (Sybase Central)

Mit Sybase Central können Sie eine Datenbank starten, ohne sich mit ihr zu verbinden.

**Voraussetzungen**

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gd geändert werden.

**Aufgabe**

1. Stellen Sie in Sybase Central eine Verbindung mit einer anderen Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Wählen Sie im linken Fensterausschnitt den Datenbankserver aus und klicken Sie dann auf **Datei » Datenbank starten**.
3. Geben Sie im Fenster **Datenbank starten** die erforderlichen Werte ein, um eine andere Datenbank zu starten, ohne sich mit ihr zu verbinden.

**Ergebnisse**

Die Datenbank erscheint unter dem Datenbankserver als getrennte Datenbank.

**Siehe auch**

- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL Anywhere-Datenbankserver“ auf Seite 150

## Datenbanken starten, ohne Verbindungen herzustellen (SQL)

Mithilfe der START DATABASE-Anweisung können Sie eine Datenbank starten, ohne sich mit ihr zu verbinden.

**Voraussetzungen**

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gd geändert werden.

### Aufgabe

1. Stellen Sie eine Verbindung mit einer anderen Datenbank her.
2. Führen Sie eine START DATABASE-Anweisung aus.

### Ergebnisse

Die Datenbank wird gestartet.

### Beispiel

Starten Sie die Datenbankdatei `c:\temp\temp.db` auf dem aktuellen Datenbankserver.

```
START DATABASE 'c:\\temp\\temp.db'  
AS tempdb  
AUTOSTOP OFF;
```

Der AUTOSTOP OFF-Verbindungsparameter verhindert, dass die Datenbank automatisch gestoppt wird, nachdem alle Verbindungen getrennt wurden.

### Siehe auch

- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL Anywhere-Datenbankserver“ auf Seite 150

## Datenbanken nach dem Trennen der Verbindung stoppen (Sybase Central)

Sie können keine Datenbank stoppen, mit der Sie verbunden sind. Sie müssen zuerst die Verbindung mit der Datenbank trennen und dann die Datenbank stoppen.

### Voraussetzungen

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption `-gd` geändert werden.

Sie müssen mit einer anderen Datenbank auf demselben Datenbankserver verbunden sein, um eine Datenbank stoppen zu können.

### Aufgabe

1. Stellen Sie sicher, dass Sie mit einer anderen Datenbank auf demselben Datenbankserver verbunden sind. Falls auf dem Datenbankserver keine andere Datenbank läuft, können Sie eine Verbindung mit der Dienstprogrammdatei herstellen.
2. Wählen Sie in Sybase Central die zu stoppende Datenbank aus und klicken Sie auf **Datei » Datenbank stoppen**.

## Ergebnisse

Wenn die Verbindung zur Datenbank getrennt wurde, verschwindet die Datenbank möglicherweise aus dem linken Fensterausschnitt. Dies kommt vor, wenn Ihre Verbindung die letzte verbleibende Verbindung war, und wenn beim Start der Datenbank AutoStop angegeben wurde. Durch AutoStop wird die Datenbank automatisch gestoppt, wenn die letzte Verbindung getrennt wird.

### Siehe auch

- „Datenbankserver stoppen“ auf Seite 154
- „Verbindungsparameter AutoStop (ASTOP)“ auf Seite 342
- „STOP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindung mit der Dienstprogrammdatenbank herstellen“ auf Seite 147

## Datenbanken nach dem Trennen der Verbindung stoppen (SQL)

Wenn Sie eine Datenbank stoppen möchten, mit der Sie verbunden sind, müssen Sie die Verbindung trennen und anschließend die Datenbank mit der STOP DATABASE-Anweisung stoppen. Datenbanken, die mit dem AUTOSTOP-Verbindungsparameter gestartet wurden, werden automatisch gestoppt, wenn die Verbindung des letzten Benutzers getrennt wird.

### Voraussetzungen

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gd geändert werden.

Sie müssen mit einer anderen Datenbank auf demselben Datenbankserver verbunden sein, um eine Datenbank stoppen zu können.

### Aufgabe

1. Stellen Sie sicher, dass Sie mit einer anderen Datenbank auf demselben Datenbankserver verbunden sind. Falls auf dem Datenbankserver keine andere Datenbank läuft, können Sie eine Verbindung mit der Dienstprogrammdatenbank herstellen.
2. Führen Sie eine STOP DATABASE-Anweisung aus.

### Ergebnisse

Die Datenbank wird gestoppt.

### Beispiel

Die folgenden Anweisungen stellen eine Verbindung mit der Dienstprogrammdatenbank her und stoppen die Datenbank tempdb.

```
CONNECT to 'TestEng' DATABASE utility_db
AS conn2
USER 'DBA'
IDENTIFIED BY 'sql';
STOP DATABASE tempdb;
```

### Siehe auch

- „Datenbankserver stoppen“ auf Seite 154
- „Verbindungsparameter AutoStop (ASTOP)“ auf Seite 342
- „STOP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindung mit der Dienstprogrammdatei herstellen“ auf Seite 147

## Datenbankserverkonfiguration

- Sie können zahlreiche Optionen benutzen, um bestimmte Funktionen festzulegen, etwa wie viel Speicher als Cache benutzt werden soll, wie viele CPUs einbezogen werden sollen (bei Mehrprozessorcomputern, die einen Netzwerk-Datenbankserver ausführen) und welche Netzwerkprotokolle verwendet werden (nur beim Netzwerkserver). Optionen stellen die wichtigste Möglichkeit zur Steuerung des Verhaltens und der Performance von SQL Anywhere dar. Siehe „[Syntax des SQL Anywhere-Datenbankservers](#)“ auf Seite 203.
- Sie können den Server als Windows-Dienst betreiben. Wenn Sie einen Datenbankserver als einen Dienst ausführen, läuft er weiter, auch wenn Sie sich vom Computer abmelden. Siehe „[Datenbankserver als Dienst oder Daemon ausführen](#)“ auf Seite 180.
- Sie können den Personal Server aus einer Anwendung starten und wieder herunterfahren, wenn die Anwendung ihre Verarbeitung abgeschlossen hat. Diese Konfiguration ist sinnvoll, wenn der Datenbankserver als eingebettete Datenbank verwendet wird. Siehe „[Verbindungen mit eingebetteten Datenbanken](#)“ auf Seite 28.

### Siehe auch

- „Datenbankserver starten“ auf Seite 153

## Hinweise zur maximalen Seitengröße

Der Cache des Datenbankservers ist in **Seiten** aufgebaut - also Speicherbereichen mit feststehender Größe. Da der Datenbankserver während der Betriebszeit (also bis er heruntergefahren wird) nur einen einzigen Cache verwendet, müssen alle Seiten dieselbe Größe haben.

Eine Datenbankdatei ist ebenfalls in Seiten aufgebaut, deren Größe beim Erstellen der Datenbank angegeben wird. Jede Datenbankseite muss auf eine Cacheseite passen. Standardmäßig wird die Datenbankserver-Seitengröße auf die maximale Seitengröße der Datenbanken gesetzt, die beim Starten des Datenbankservers angegeben wurden. Wenn ein Datenbankserver gestartet wurde, können Sie keine Datenbank starten, die eine größere Seitengröße hat als der Datenbankserver.

Wenn Sie wollen, dass nach dem Start des Datenbankservers auch Datenbanken gestartet werden können, die größere Seiten verwenden, können Sie den Datenbankserver mit der Option `-gp` zwingen, mit einer bestimmten Seitengröße zu starten. Denken Sie daran, die Cachegröße zu erhöhen, falls Sie größere Seiten verwenden. Ein unveränderter Cache nimmt nur einen Bruchteil der größeren Seiten auf, was zu Flexibilitätseinbußen bei der Anordnung des Speicherplatzes führt.

Der folgende Befehl startet einen Datenbankserver, der einen 64-MByte-Cache reserviert und Datenbanken enthalten kann, die Seitengrößen bis zu 8192 Byte verwenden.

```
dbsrv16 -gp 8192 -c 64M -n myserver
```

**Siehe auch**

- „Datenbankserveroption -gp“ auf Seite 249

## Datenbankservernamen und Datenbanknamen

Sie können -n als Datenbankserveroption (zum Benennen des Datenbankservers) oder als Datenbankoption (zum Benennen der Datenbank) verwenden.

Clientanwendungen können Verbindungsparameter verwenden, die den Namen für den Datenbankserver und den Datenbanknamen angeben, wenn sie eine Verbindung zu einer Datenbank herstellen. Der Name des Datenbankservers erscheint auf dem Desktop-Symbol und in der Titelleiste des Meldungsfensters des Datenbankservers.

Der Name utility\_db ist für die Dienstprogrammdatenbank reserviert. Deshalb dürfen Sie keine Datenbank mit diesem Namen erstellen und keinen Datenbankserver mit diesem Namen starten.

**Datenbankserver benennen**

Wenn Sie einen Namen für den Datenbankserver vergeben, können Sie Konflikte mit anderen Datenbankservernamen im Netzwerk vermeiden. Den Benutzern der Clientanwendungen wird damit ein aussagekräftiger Name geboten. Der Datenbankserver behält seinen Namen während seiner gesamten Anwendungsdauer (bis er heruntergefahren wird). Wenn Sie keinen Datenbankservernamen vergeben, erhält der Datenbankserver den Namen der ersten gestarteten Datenbank.

Sie können den Datenbankserver benennen, indem Sie die Option -n vor die erste Datenbankdatei setzen. Der folgende Befehl startet z.B. einen Datenbankserver, der die Beispieldatenbank ausführt, und gibt ihm den Namen "Cambridge":

```
dbsrv16 -n Cambridge "%SQLANYSAMPl6%\demo.db"
```

Wenn Sie einen Datenbankservernamen eingeben, können Sie einen Datenbankserver starten, ohne eine Datenbank zu laden. Der folgende Befehl startet einen Datenbankserver namens "Galt", ohne eine Datenbank zu starten:

```
dbsrv16 -n Galt
```

Datenbankservernamen müssen gültige Bezeichner sein. Lange Datenbankservernamen werden je nach Protokoll auf unterschiedliche Längen gekürzt. Für Datenbankservernamen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola, Schrägstriche (/) oder Backslashes (\) enthalten.
- Sie dürfen nicht länger sein als 250 Byte.
- Sie dürfen keine Leerstellen enthalten, wenn sie unter Unix laufen.

### Hinweis

Unter Windows und Unix können sich Clients der Version 9.0.2 und früher nicht mit Datenbankservern der Version 10.0.0 und höher verbinden, die längere Namen als die folgenden Längen haben:

- 40 Byte bei Shared Memory unter Windows
- 31 Byte bei Shared Memory unter Unix
- 40 Byte bei TCP/IP

### Datenbanken benennen

Sie können für die Benutzer einer Clientanwendung einen aussagekräftigen Datenbanknamen verwenden. Die Datenbank ist durch diesen Namen identifiziert, bis sie gestoppt wird. Die maximale Länge für einen Datenbanknamen beträgt 250 Byte.

Wenn Sie keinen Datenbanknamen vergeben, wird der Standardname aus dem Hauptteil des Namens der Datenbankdatei gebildet (dem Dateinamen ohne die Erweiterung *.db*). Im folgenden Befehl z.B. ist die erste Datenbank "mydata" benannt, und die zweite "mysales".

```
dbsrv16 c:\mydata.db c:\sales\mysales.db
```

Sie können Datenbanken benennen, indem Sie die Option `-n` hinter die Datenbankdatei setzen. Mit dem folgenden Befehl wird beispielsweise die Beispieldatenbank gestartet und "MyDB" genannt:

```
dbsrv16 "%SQLANY16%\demo.db" -n MyDB
```

### Groß-/Kleinschreibung

Datenbankservernamen und Datenbanknamen berücksichtigen Groß- und Kleinschreibung nicht, wenn ein Einbyte-Zeichensatz verwendet wird.

### Siehe auch

- „Die Dienstprogrammdateiabank“ auf Seite 145
- „Datenbanken starten und stoppen“ auf Seite 156
- „Verbindungszeichenfolgen und Zeichensätze“ auf Seite 503

## Konfigurationsdateien und Datenbankserver-Startoptionen

Sie können die Gruppe von Optionen für das Starten eines Datenbankservers in einer Konfigurationsdatei speichern und diese Datei in einer Datenbankserver-Befehlszeile aufrufen. Die Konfigurationsdatei kann Optionen in mehreren Zeilen enthalten. Die folgende Konfigurationsdatei startet beispielsweise einen Datenbankserver und die Beispieldatenbank. Der Cache wird auf 10 MB eingestellt und diese Instanz des Personal Servers erhält den Namen **Elora**. Zeilen mit dem Rautenzeichen (#) als erstem Zeichen in der Zeile werden als Kommentar behandelt.

```
# Configuration file for server Elora
-n Elora
-c 10M
"%SQLANY16%\demo.db"
```

Wenn Sie die Datei mit diesen Optionen *sample.cfg* nennen, können Sie die Datei folgendermaßen verwenden:

```
dbsrv16 @sample.cfg
```

#### Siehe auch

- „@data -Datenbankserveroption“ auf Seite 214
- „Konfigurationsdateien“ auf Seite 882
- „Bedingte syntaktische Analyse in Konfigurationsdateien“ auf Seite 883

## Protokollieren von Datenbankserver-Aktionen

Das **Datenbankserver-Meldungslog** enthält informative Meldungen, Fehler, Warnungen und Meldungen von der MESSAGE-Anweisung. Diese Meldungen können an folgenden Standorten angezeigt werden:

- Im Meldungsfenster des Datenbankservers (ein Symbol in der Taskleiste unter Windows)
- Im Fensterausschnitt **Servermeldungen und ausgeführte SQL** in Sybase Central
- Im SQL Anywhere-Konsolendienstprogramm
- In der Datenbankserver-Meldungslogdatei
- In einem Eingabeaufforderungsfenster oder einer Shell, wenn der Datenbankserver als eine Befehlszeilenanwendung ausgeführt wird
- Im Unix-Syslog

#### Siehe auch

- „Datenbankserveroption -o “ auf Seite 268
- „Datenbankserveroption -oe “ auf Seite 269
- „Datenbankserveroption -on “ auf Seite 269
- „Datenbankserveroption -os “ auf Seite 270
- „Datenbankserveroption -ot “ auf Seite 271

## Datenbankservermeldungen in einer Datei protokollieren

Standardmäßig werden Datenbankservermeldungen an das Meldungsfenster des Datenbankservers gesendet. Mithilfe der Befehlszeilenoption -o können Sie die Ausgabe in eine Logdatei schreiben. Führen Sie den folgenden Befehl aus, um die Ausgabe in eine Logdatei mit dem Namen *mydbserver\_messages.txt* zu schreiben:

```
dbsrv16 -o mydbserver_messages.txt -c ...
```

Sie können die Größe der Datenbankserver-Meldungslogdatei steuern und festlegen, was geschehen soll, wenn eine Datei die Maximalgröße erreicht:

- Verwenden Sie die Option -o um festzulegen, dass eine Datenbankserver-Meldungslogdatei verwendet werden soll und um einen Namen anzugeben.
- Verwenden Sie die Option -ot, um festzulegen, dass eine Datenbankserver-Meldungslogdatei verwendet werden soll, und um einen Namen anzugeben, wenn der vorherige Inhalt der Datei gelöscht werden soll, bevor neue Meldungen an sie gesendet werden.

- Verwenden Sie zusätzlich zur Option -o oder -ot die Option -on, um die Größe anzugeben, bei der die Logdatei mit der Erweiterung *.old* umbenannt und eine neue Datei mit dem ursprünglichen Namen gestartet wird.
- Zusätzlich zu den Optionen -o oder -ot legen Sie mit der Option -os die Größe fest, bei der eine neue Datenbankserver-Meldungslogdatei mit einem neuen Namen gestartet wird, der auf dem Datum und einer sequenziellen Nummer basiert.

Sie können eine separate Datei zur Protokollierung von Startfehlern, schwerwiegenden Fehlern und Assertierungen angeben, indem Sie die Option -oe verwenden.

Es wird empfohlen, dass Sie den Namen der Datenbankserver-Nachrichtenlogdatei nicht mit *.log* abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

### Siehe auch

- „Datenbankserveroption -o “ auf Seite 268
- „Datenbankserveroption -oe “ auf Seite 269
- „Datenbankserveroption -on “ auf Seite 269
- „Datenbankserveroption -os “ auf Seite 270
- „Datenbankserveroption -ot “ auf Seite 271

## SQL-Anweisungen protokollieren

Während Sie in Sybase Central mit einer Datenbank arbeiten, generiert die Anwendung automatisch SQL-Anweisungen entsprechend Ihren Aktionen. Sie können diese Anweisungen in einem separaten Fensterausschnitt verfolgen, der **Servermeldungen und ausgeführte SQL** heißt, oder die Informationen in einer Datei speichern.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Der Fensterausschnitt **Servermeldungen und ausgeführte SQL** hat eine Registerkarte für jede Datenbank und jeden Datenbankserver. Die Registerkarte für Datenbankserver enthält dieselben Informationen wie das Meldungsfenster des Datenbankservers.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Protokollieren Sie von Sybase Central generierte SQL-Anweisungen im Fensterausschnitt **Servermeldungen und ausgeführte SQL**.
  - a. Klicken Sie auf **Ansicht » Servermeldungen und ausgeführte SQL**.

- b. Klicken Sie im Abschnitt **Servermeldungen und ausgeführte SQL** auf die Registerkarte mit dem Datenbanksymbol.
  - c. Rechtsklicken Sie und klicken Sie im Dropdown-Menü auf **Optionen**.
  - d. Bearbeiten Sie die Protokollierungsoptionen.
  - e. Klicken Sie auf **Speichern**.
3. Protokollieren Sie von Sybase Central generierte SQL-Anweisungen in einer Datei (Sybase Central).
  - a. Rechtsklicken Sie im linken Fensterausschnitt auf die Datenbank und klicken Sie auf **Protokollierung von Datenbankänderungen starten**.
  - b. Geben Sie einen Dateinamen an und klicken Sie auf **Speichern**.

### Ergebnisse

Datenbankänderungen werden protokolliert.

### Siehe auch

- [„Anweisungen in Interactive SQL protokollieren“ auf Seite 826](#)

## Protokollierung von Datenbankänderungen stoppen

Sie können die Protokollierung von Datenbankänderungen mit Sybase Central stoppen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf die Datenbank.
3. Klicken Sie auf **Protokollierung von Datenbankänderungen stoppen**.

### Ergebnisse

Datenbankänderungen werden nicht mehr protokolliert.

## Meldungen unter Unix mithilfe einer Facility-ID in eine Datei umleiten

Unter Unix können Sie Datenbankservermeldungen in eine Datei umleiten, die für die Systemadministratoren verfügbar ist.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Die folgenden Schritte zeigen, wie Meldungen unter Solaris umgeleitet werden. Dies ist jedoch auch unter Linux IBM AIX und Mac OS X möglich. Auf anderen Plattformen, z.B. HP-UX, befindet sich die Datei *syslog.conf* an einem anderen Speicherort. Sie können die */var/adm/sqlanywhere*-Datei an einen beliebigen Ort platzieren.

### Aufgabe

1. Wählen Sie eine eindeutige Facility-ID, die noch von keiner anderen auf Ihrem System laufenden Anwendung verwendet wird.

Dafür können Sie in der Datei */etc/syslog.conf* nachsehen, ob die Facility-IDs *localn* referenziert werden.

2. Bearbeiten Sie die Datei */etc/syslog.conf* und fügen Sie die folgende Zeile hinzu, wobei *localn* die Facility-ID ist, die Sie in Schritt 1 gewählt haben:

```
localn.err;localn.info;localn.notice /var/adm/sqlanywhere
```

3. Erstellen Sie die Datei */var/adm/sqlanywhere*:

```
touch /var/adm/sqlanywhere
```

4. Teilen Sie dem Prozess "syslogd" mit, dass Sie die Datei *syslog.conf* geändert haben, indem Sie nach der Prozesskennung von "syslogd" suchen:

```
ps -ef | grep syslogd
```

Führen Sie anschließend den folgenden Befehl aus, wobei *pid* die Prozesskennung von "syslogd" ist:

```
kill -HEAP pid
```

5. Starten Sie Ihren Datenbankserver mit dem folgenden Befehl, wobei **localn** die Facility-ID ist, die Sie in Schritt 1 gewählt haben:

```
dbsrv16 -s localn ...
```

### Ergebnisse

Alle Meldungen, die der Datenbankserver an Syslog weitergibt, werden in die Datei */var/adm/sqlanywhere* umgeleitet.

### Siehe auch

- „Datenbankserveroption -s“ auf Seite 278

## Windows-Ereignisprotokollmeldungen unterdrücken

Sie können Windows-Ereignisprotokolleinträge unterdrücken, indem Sie einen Registrierungseintrag verwenden. Der Registrierungseintrag lautet *Software\Sybase\SQL Anywhere\16.0*. Dieser Eintrag kann in den Eintrag HKEY\_CURRENT\_USER oder HKEY\_LOCAL\_MACHINE platziert werden.

Einträge des Ereignisprotokolls können Sie steuern, indem Sie den EventLogMask-Schlüssel festlegen. Es handelt sich dabei um den Typ REG\_DWORD. Der Wert ist eine Bitmaske, die die Bitwerte für die verschiedenen Typen von Ereignismeldungen enthält:

errors	EVENTLOG_ERROR_TYPE	0x0001
warnings	EVENTLOG_WARNING_TYPE	0x0002
information	EVENTLOG_INFORMATION_TYPE	0x0004

Wenn Sie die Einstellung des EventLogMask-Schlüssels ändern, müssen Sie den Datenbankserver neu starten, damit die Änderung in Kraft tritt.

### Beispiel

Wenn zum Beispiel der Schlüssel für EventLogMask auf 0 gesetzt wurde, erscheinen keine Meldungen. Wenn Sie diesen Schlüssel auf 1 setzen, werden keine informativen oder Warnmeldungen, dafür aber Fehler angezeigt. Die Standardeinstellung (kein Eintrag vorhanden) gibt an, dass alle Meldungstypen angezeigt werden.

### Siehe auch

- „Netzwerkprotokolloptionen“ auf Seite 388

## Performance und Speicher steuern

Im Folgenden werden einige der Einstellungen genannt, die sich auf die Datenbankserver-Performance auswirken können:

- **Cachegröße** Die Menge des für den Datenbankserver verfügbaren Cachespeichers kann ein Hauptfaktor für die Performance sein. Je mehr Speicher dem Datenbankserver zur Verfügung steht, desto schneller arbeitet er. Im Cache werden Daten gehalten, die häufiger abgerufen werden. Der Zugriff auf die Informationen im Cache ist schneller als der Festplattenzugriff. Die anfängliche Standardgröße des Caches wird auf Basis der Größe des physischen Speichers, des Betriebssystems und der Größe der Datenbankdateien berechnet. Der Datenbankserver passt automatisch die erforderliche Cachegröße an. Siehe „Dynamische Cachedimensionierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

Im Meldungsfenster des Datenbankservers wird die Größe des Caches beim Start angezeigt und Sie können die folgende Anweisung benutzen, um die aktuelle Größe des Caches abzurufen:

```
SELECT PROPERTY( 'CurrentCacheSize' );
```

Weitere Informationen zur Optimierung der Performance finden Sie unter „Tools für Performanceüberwachung und Diagnose“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

Die folgende Tabelle gibt einen Überblick über die Optionen des Datenbankservers für die Steuerung des Cache.

Cachefunktion	Datenbankserveroption	Verwendung	Siehe:
Cachegröße	-c	Legt die anfängliche Speichergöße für den Cache des Datenbankservers fest	„Datenbankserveroption -c “ auf Seite 217
	-ca 0	Erzwingt eine statische Cachegröße	„Datenbankserveroption -ca “ auf Seite 219
	-ch	Legt die maximale Cachegröße für automatische Cachegrößenveränderung fest	„Datenbankserveroption -ch “ auf Seite 221
	-chx	Legt die maximale Cachegröße für automatische Cachegrößenveränderung fest, ohne Adressraum für Nicht-Cache (nur 32-Bit-Datenbankserver)	„Datenbankserveroption -chx “ auf Seite 222
	-cl	Legt die minimale Cachegröße für die automatische Cachegrößenveränderung fest	„Datenbankserveroption -cl “ auf Seite 224
	-cs	Zeigt Statistiken der dynamischen Cachegrößenänderungen im Meldungsfenster des Datenbankservers an	„Datenbankserveroption -cs “ auf Seite 227
Cachevorwarnung	-cc	Sammelt Informationen über Datenbankseiten, die zur Cache-Vorwarnung eingesetzt werden können, wenn die Datenbank erneut gestartet wird	„Datenbankserveroption -cc “ auf Seite 220
	-cr	Bereitet den Cache mit Datenbankseiten vor	„Datenbankserveroption -cr “ auf Seite 226
	-cv	Zeigt die Cachenutzung im Meldungsfenster des Datenbankservers an	„Datenbankserveroption -cv “ auf Seite 227

- **Multiprogramming-Stufe** Die Multiprogramming-Stufe des Datenbankservers gibt die maximale Anzahl von Datenbankserveraufgaben an, die gleichzeitig durchgeführt werden können. Im Allgemeinen erhöht eine höhere Multiprogramming-Stufe den Gesamtdurchsatz des Datenbankservers, weil eine größere Anzahl von Anforderungen ausgeführt werden kann. Wenn die Anforderungen die gleichen Ressourcen benötigen, kann eine Erhöhung der Multiprogramming-Stufe zu zusätzlichen Konflikten führen und die Transaktionsantwortzeit verlängern.

Standardmäßig passt SQL Anywhere automatisch die Multiprogramming-Stufe des Datenbankservers an. In einigen Fällen können Sie den Durchsatz des Systems durch eine Erhöhung der Multiprogramming-Stufe verringern. Mit den folgenden Optionen können Sie die Multiprogramming-Stufe des Datenbankservers manuell steuern:

Datenbankserveroption	sa_server_option-Wert	Beschreibung
<a href="#">„Datenbankserveroption - gn“ auf Seite 244</a>	CurrentMultiProgramming-Level	Setzt die Multiprogramming-Stufe des Datenbankservers.
<a href="#">„Datenbankserveroption - gna“ auf Seite 245</a>	AutoMultiProgramming-Level	Aktiviert und deaktiviert die dynamische Optimierung der Multiprogramming-Stufe des Datenbankservers.
<a href="#">„Datenbankserveroption - gnh“ auf Seite 246</a>	MaxMultiProgramming-Level	Legt die maximale Anzahl von Aufgaben fest, die der Datenbankserver gleichzeitig ausführen kann
<a href="#">„Datenbankserveroption - gnl“ auf Seite 247</a>	MinMultiProgramming-Level	Legt die minimale Anzahl von Aufgaben fest, die der Datenbankserver gleichzeitig ausführen kann.
<a href="#">„Datenbankserveroption - gns“ auf Seite 248</a>	AutoMultiProgramming-LevelStatistics	Steuert, ob statistische Daten über die automatischen Änderungen in der Multiprogramming-Stufe in die Meldungslogdatei des Datenbankservers geschrieben werden.
<a href="#">„Datenbankserveroption - gta“ auf Seite 252</a>	ProcessorAffinity	Weist den Datenbankserver unter Windows oder Linux an, welche logischen Prozessoren verwendet werden sollen.

Weitere Informationen zur Multiprogramming-Stufe in SQL Anywhere finden Sie unter [„Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175](#).

- **Anzahl von Prozessoren** Wenn Sie den Server auf einem Computer mit mehreren Prozessoren ausführen, können Sie mit der Option -gt die Anzahl der Prozessoren festlegen. Siehe [„Datenbankserveroption -gt“ auf Seite 251](#) und [„SQL Anywhere-Threading“ auf Seite 171](#).

Die Anzahl der CPUs, die der Datenbankserver benutzen kann, hängt unter Umständen auch von Ihrer SQL Anywhere-Edition ab. Siehe „[Editionen und Lizenzierung](#)“ [*SQL Anywhere 16 - Einführung*].

- **Andere Optionen im Zusammenhang mit der Performance** Für die Optimierung der Netzwerkleistung stehen einige zusätzliche Optionen zur Verfügung, z.B.: -gb (Datenbank-Prozesspriorität) oder -u (gepufferte I/O-Vorgänge). Siehe „[Syntax des SQL Anywhere-Datenbankservers](#)“ auf Seite 203.

### Siehe auch

- „[sa\\_server\\_option-Systemprozedur](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Privilegien über die Befehlszeile steuern

Einige Optionen steuern, welche Privilegien zum Ausführen bestimmter globaler Vorgänge erforderlich sind. Dazu gehören die Privilegien zum Starten und Stoppen von Datenbanken, zum Laden und Entladen von Daten sowie zum Erstellen und Löschen von Datenbankdateien.

### Siehe auch

- „[Allgemeine Sicherheitstipps](#)“ auf Seite 1406

## Spezielle Betriebsmodi

Sie können SQL Anywhere in speziellen Modi ausführen.

- **Schreibgeschützt** Sie können Datenbanken im schreibgeschützten Modus ausführen, indem Sie die Option -r verwenden. Datenbanken mit aktiviertem Auditing können nicht im schreibgeschützten Modus gestartet werden.
- **In-Memory-Modus** Sie können Datenbanken vollständig im Speicher ausführen, indem Sie die Option -im angeben. Wenn Sie nur im Checkpoint-Modus (-im c) ausführen, verwendet der Datenbankserver kein Transaktionslog, aber die Datenbank kann bis zum letzten Checkpoint wiederhergestellt werden. Wenn Sie die Datenbank im Never-Write-Modus (-im nw) ausführen, werden festgeschriebene Transaktionen nicht in die Datenbankdatei auf der Festplatte geschrieben und alle Änderungen gehen verloren, wenn Sie die Datenbank herunterfahren. Bei beiden In-Memory-Modi kann Ihre Anwendung dennoch Änderungen an der Datenbank durchführen oder auf sie zugreifen, während die Datenbank aktiv ist.

#### Hinweis

Für den In-Memory-Modus benötigen Sie eine separate Lizenz. Siehe „[Getrennt lizenzierbare Komponenten](#)“ [*SQL Anywhere 16 - Einführung*].

- **Große Datenmengen laden** Dies ist nützlich, wenn Sie mit der INPUT-Anweisung von Interactive SQL große Datenmengen in eine Datenbank laden. Verwenden Sie die Option -b nicht, wenn Sie LOAD TABLE zum Laden großer Datenmengen benutzen.

- **Ohne Transaktionslog starten** Der Datenbankparameter -f wird für die Wiederherstellung benutzt, entweder um den Datenbankserver zu zwingen, nach dem Verlust eines Transaktionslogs neu zu starten, oder mit einem Transaktionslog zu starten, das er sonst nicht finden würde. -f ist eine Datenbankoption und keine Serveroption.

Wenn die Wiederherstellung abgeschlossen ist, sollten Sie Ihren Server stoppen und ohne die Option -f erneut starten.

- **Im stillen Modus arbeiten** Der Datenbankserver unterstützt den dialogfreien Betrieb. Sie können selbst festlegen, wie dialogfrei der Server betrieben wird: Sie können Meldungen unterdrücken, das Symbol aus dem Systeminformationsbereich entfernen und den Server vollkommen unmerklich arbeiten lassen. Um unter Windows einen vollständig dialogfreien Datenbankserverbetrieb auszuführen, geben Sie die Optionen -qi, -qs und -qw an. Wenn diese Optionen aktiviert sind, gibt es keine sichtbaren Anzeichen, dass der Server läuft, da alle Symbole und alle Startmeldungen unterdrückt werden. Wenn Sie den Datenbankserver im dialogfreien Betrieb laufen lassen, können Sie die Optionen -o oder -oe verwenden, um Fehler zu diagnostizieren.

Die Optionen -qi und -qs unterdrücken nicht die Fenster, die durch die Serveroptionen -v (Version) und -ep (Aufforderung zur Eingabe des Kennworts für die Datenbankverschlüsselung) angezeigt werden.

- „Datenimport und -export“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -r“ auf Seite 277
- „Datenbankoption -r“ auf Seite 329
- „Datenbankserveroption -im“ auf Seite 257
- „Datenbankserveroption -b“ auf Seite 216
- „Datenbankserver-Wiederherstellungsoption -f“ auf Seite 234
- „Datenbankserveroption -qi“ auf Seite 273
- „Datenbankserveroption -qn“ auf Seite 274
- „Datenbankserveroption -qs“ auf Seite 275
- „Datenbankserveroption -qw“ auf Seite 276

## SQL Anywhere-Threading

Um das SQL Anywhere- Thread-Modell zu verstehen, müssen Sie auch die grundlegende Terminologie und die Konzepte von Threads bzw. der Anforderungsverarbeitung verstehen.

- **Anforderung** Eine Anforderung ist eine Arbeitseinheit, wie z.B. eine Abfrage oder eine SQL-Anweisung, die an den Datenbankserver über eine Verbindung gesendet wird. Die Aktivitätszeit einer Anforderung reicht vom Zeitpunkt, an dem die Anforderung erstmals vom Datenbankserver empfangen wird, bis zu dem Zeitpunkt, an dem die letzten Ergebnisse zurückgegeben werden, Cursor geschlossen werden oder die Anforderung abgebrochen wird.
- **Aufgabe** Eine Aufgabe ist die Einheit einer Aktivität, die im Datenbankserver durchgeführt wird, und die kleinste Arbeitseinheit, die vom Datenbankserver geplant wird. Im Datenbankserver wird jede Benutzeranforderung zu zumindest einer Aufgabe, und möglicherweise zu mehreren, wenn die abfrageinterne Parallelität verwendet wird. Zusätzlich zu Benutzeranforderungen kann der Datenbankserver auch seine eigenen Aufgaben planen, um interne Aufgaben durchzuführen, wie z.B.

den Datenbank-Cleaner auszuführen oder Timer zu verarbeiten. Die maximale Anzahl von aktiven Aufgaben, die gleichzeitig ausgeführt werden können, richtet sich nach der Größe des Worker-Pools innerhalb des System-Kernels. Wenn eine Benutzeranforderung auf dem Datenbankserver ankommt und ihr ein Worker-Thread zugeordnet wird, wird die ActiveReq-Serveigenschaft um 1 erhöht. Wenn die Anforderung abgeschlossen ist, wird die ActiveReq-Serveigenschaft um 1 verringert. Wenn jedoch keine Worker-Threads zum Ausführen der Benutzeranforderung verfügbar sind, wird die Aufgabe in die Warteschlange gestellt und die UnschReq-Serveigenschaft wird um 1 erhöht. Wenn die Aufgabe aus der Warteschlange genommen wird, weil nun ein Worker-Thread verfügbar ist, wird die UnschReq-Serveigenschaft um 1 verringert und die ActiveReq-Eigenschaft wird um 1 erhöht.

- **Worker-Thread** Ein Worker-Thread ist eine Abstraktion eines ausführenden **Steuerungs-Threads** innerhalb des Datenbankserver-Kernels. Unter Windows und Linux sind Worker-Threads unter Verwendung von Lightweight-Threads implementiert, die als **Fasern** bezeichnet werden. Auf anderen Plattformen werden Worker-Threads unter Verwendung von Betriebssystem-Threads implementiert. Worker-Threads führen Aufgaben aus, die ihnen vom Datenbankserver-Kernel zugeordnet sind. Der Datenbankserver verwendet einen Worker-Thread-Pool variabler Größe für die Verarbeitung der Arbeitslast des Servers. Die Größe des Pools entspricht der Multiprogramming-Stufe des Datenbankservers.

Personal Server wie auch Netzwerkeserver unter Windows Mobile haben einen Pool fester Größe. Für diese Server wird die Anzahl von Worker-Threads, die beim Start des Datenbankservers erstellt wird, mit der Option -gn gesteuert. Für alle anderen Netzwerkeserver erstellt der Datenbankserver die Anzahl der Worker-Threads, die mit der Option -gnh angegeben wird. Nur die Anzahl der von der Multiprogramming-Stufe des Servers festgelegten Worker-Threads darf jedoch Aufgaben verarbeiten. Standardmäßig wird die Größe des Worker-Pools dynamisch vom Kernel und abhängig von den Änderungen der Datenbankserver-Arbeitslast abgestimmt. Sie kann zwischen den mit den Optionen -gnl und -gnh festgelegten Unter- und Obergrenzen schwanken.

Aufgaben werden Worker-Threads auf First-In-First-Out-Basis (FIFO) zugewiesen. Die Priorität jeder Aufgabe wird basierend auf der Verbindung gesetzt, die die Aufgabe generiert hat. Wenn eine Aufgabe einem Worker-Thread zur Ausführung zugewiesen wurde, berücksichtigt der Scheduler des Kernels die Priorität der Aufgabe bei der Zuweisung von CPU-Zeit für den Worker-Thread. Wenn eine Aufgabe während der Verarbeitung aus irgendeinem Grund blockiert werden muss, wie etwa während des Wartens auf eine Sperre oder auf die Beendigung eines I/O-Vorgangs, bleibt der Worker-Thread an diese Aufgabe gekoppelt. Erst wenn die Aufgabe abgeschlossen wurde, wird der Worker-Thread für die Ausführung von anderen Aufgaben verfügbar.

- **Thread** Ein Thread bzw. ein Verarbeitungs-Thread ist ein Betriebssystemkonstrukt, das die gleichzeitige Verarbeitung innerhalb eines einzelnen Prozesses ermöglicht. Jeder Betriebssystemprozess, einschließlich des Datenbankservers, wird von zumindest einem, aber möglicherweise von vielen Treads ausgeführt. Ein Thread wird außerhalb der Anwendung vom Betriebssystem geplant, und letztendlich wird die gesamte Ausführung einer Anwendung durch Threads durchgeführt. Unter Windows und Linux erstellt der Datenbankserver eine bestimmte Anzahl von Threads: einen Betriebssystem-Thread pro CPU-Kern, der von der Option -gtc gesteuert wird. Auf anderen Plattformen entspricht die Anzahl der erstellten Betriebssystem-Threads der Größe des Worker-Thread-Pools. Sie wird von den gleichen Mechanismen gesteuert, die für die Steuerung der Worker-Poolgröße verwendet werden.

Die Anzahl der Threads ist unabhängig von der Anzahl der Verbindungen zur Datenbank und der Datenbankserver stellt keinen Thread für eine bestimmte Verbindung bereit. Stattdessen wird Aufgaben, die zur Ausführung in den Datenbankserver gelangen, aus einem Pool fester Größe mit Server Threads dynamisch ein Thread zugewiesen. Wenn eine Aufgabe einem Thread zugewiesen ist, verarbeitet der Thread die Aufgabe, bis sie abgeschlossen ist oder abgebrochen wird.

#### Siehe auch

- [UnschReq-Servereigenschaft auf Seite 763](#)
- [ActiveReq-Servereigenschaft auf Seite 745](#)
- [„Threading-Verhalten“ auf Seite 174](#)
- [„Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175](#)
- [„Datenbankserveroption -gn “ auf Seite 244](#)
- [„Datenbankserveroption -gnl “ auf Seite 247](#)
- [„Datenbankserveroption -gnh “ auf Seite 246](#)
- [„Datenbankserveroption -gtc “ auf Seite 253](#)
- [„sa\\_clean\\_database-Systemprozedur“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [„Transaktion blockieren und Deadlock“ \[\*SQL Anywhere Server - SQL-Benutzerhandbuch\*\]](#)

## Worker-Threads unter Unix

Unter Unix wird ein Worker-Thread unter Verwendung eines Betriebssystem-Threads implementiert. Die zeitliche Verteilung von Aufgaben wird daher vom Betriebssystem-Scheduler gesteuert und das Betriebssystem kann zu jedem beliebigen Zeitpunkt wählen, die Ausführung eines Threads vorab festzulegen. Diese präventive Zeitplanung wirkt sich auf die Aufgabenverarbeitung nicht sichtbar aus - wenn ein Thread erneut zugeordnet wird, wird die Aufgabe an dem Punkt entgegengenommen, an dem die Verarbeitung unterbrochen wurde. Aufgabenprioritäten, die von einer Datenbankverbindung geerbt werden, haben keine Auswirkung auf die Ausführungsplanung für diese Aufgaben. Stattdessen werden alle Aufgaben auf derselben Prioritätsstufe ausgeführt, weil alle Betriebssystem-Thread-Prioritäten gleichwertig sind.

## Worker-Threads unter Windows und Linux

Unter Windows und Linux werden Worker-Threads unter Verwendung von Lightweight-Threads ausgeführt, die auch als **Fasern** ("fibers") bezeichnet werden. Eine Implementierung, die Fasern verwendet, gestattet es Worker-Threads, die Abfolgeplanung kooperativ untereinander festzulegen, anstatt sie mit dem Betriebssystem-Scheduler vorab festzulegen. Das Ergebnis ist, dass ein Kontextwechsel zwischen Fasern genauer gesteuert werden kann. Der Datenbank-Kernel erstellt den Zeitplan für die Fasern, um die Prozessoraffinität zu maximieren und die Ausführungspriorität jedes Worker-Threads genau zu steuern.

Da Fasern nicht vom Betriebssystem-Scheduler abhängen, muss eine Faser die Kontrolle an eine andere Faser explizit übergeben, wenn sie auf den Abschluss einer anderen Aktivität wartet. Wenn z.B. eine auf einer Faser ausgeführte Aufgabe blockiert, während sie auf den Abschluss eines I/O-Vorgangs wartet, übergibt sie die Kontrolle an eine andere Faser. Der Thread, der die ursprüngliche Faser ausführt, kann unmittelbar eine andere Faser entgegennehmen und ihre Ausführung ohne einen Kernel-Kontextwechsel beginnen. Wenn eine Faser blockiert und die Kontrolle nicht übergibt, blockiert sie den Thread, der sie

beherbergt, und hindert damit andere Fasern daran, auf diesem Thread zu laufen. Wenn mehr als ein Thread Fasern beherbergt, wird nur der Thread, der die wartende Faser beherbergt, blockiert: Andere Threads können weiterhin Fasern verarbeiten.

Auf Windows- und Linux-Plattformen werden zumindest so viele Fasern erstellt, wie es die Einstellung für die maximale Parallelität des Netzwerk-Datenbankservers erfordert (durch die Option `-gnh` angegeben). Der Netzwerk-Datenbankserver verwendet eine Teilmenge dieser Fasern während der Serverausführung, entsprechend der aktuellen Multiprogramming-Stufe des Servers. Für jede Faser muss das Betriebssystem Adressraum für ihren Stack reservieren. Der für jede Faser erforderliche Stackbereich hängt von der Einstellung der Serveroption `-gss` ab.

Der von einem Netzwerkserver benötigte Adressraum für Ausführungsstacks ist proportional zur maximalen Multiprogramming-Stufe.

### Siehe auch

- „Datenbankserveroption `-gss`“ auf Seite 250
- „Datenbankserveroption `-gn`“ auf Seite 244

## Threading-Verhalten

Es gibt mehrere Faktoren, die das Thread-Verhalten steuern und die jeweils durch eine Serveroption gesteuert werden. Nicht alle diese Optionen werden auf jeder Plattform unterstützt.

- **Multiprogramming-Stufe (Serveroption `-gn`)** Die Option `-gn` steuert die Multiprogramming-Stufe des Datenbankservers. Dieser Wert legt die maximale Anzahl der Aufgaben fest, die gleichzeitig aktiv sein können. Jede Datenbank Anforderung verursacht die Erstellung von zumindest einer und möglicherweise mehreren Aufgaben, wenn die abfrageinterne Parallelität verwendet wird. Zusätzlich plant der Server gelegentlich Aufgaben, um interne Aktivitäten durchzuführen. Wenn die Anzahl der Aufgaben im Server die Multiprogramming-Stufe überschreitet, müssen ausstehende Aufgaben warten, bis eine derzeit ausgeführte bzw. eine aktive Aufgabe abgeschlossen ist.
- **Stackgröße pro internem Ausführungs-Thread (Serveroption `-gss`)** Sie können die Stackgröße pro Worker-Thread im Datenbankserver mit der Option `-gss` festlegen. Die Option `-gss` gestattet es, die Adressraumanforderungen jedes Worker-Threads innerhalb des Datenbankservers herabzusetzen, was in Umgebungen mit begrenztem Speicherplatz nützlich sein kann.
- **Anzahl der Prozessoren (Serveroption `-gt`)** Die Option `-gt` steuert die Anzahl der Prozessoren, die der Datenbankserver verwendet.
- **Prozessoren-Parallelität (Serveroption `-gtc`)** Die Option `-gtc` gibt die Anzahl der logischen Prozessoren (Kerne) an, die der Datenbankserver verwendet.

### Prozessornutzung und Thread-Beispiel

Das folgende Beispiel zeigt, wie der Datenbankserver, basierend auf den Einstellungen von `-gt` und `-gtc`, CPUs auswählt. Für die folgenden Beispiele wird ein System mit 4 Prozessoren und 2 Kernen pro Prozessor vorausgesetzt. Die physischen Prozessoren werden mit Buchstaben und die Kerne mit Zahlen gekennzeichnet, wodurch das System die Verarbeitungseinheiten A0, A1, B0, B1, C0, C1, D0 und D1 enthält.

Szenario	Einstellungen des Netzwerk-Datenbankservers
Eine einzelne CPU-Lizenz oder -gt 1 angegeben	<ul style="list-style-type: none"> <li>• -gt 1</li> <li>• -gtc 2</li> </ul> <p>Threads können auf A0 und A1 ausgeführt werden.</p>
Keine Lizenz einschränkungen auf der CPU mit angegebenem -gtc 5	<ul style="list-style-type: none"> <li>• -gt 4</li> <li>• -gtc 5</li> </ul> <p>Threads können auf A0, A1, B0, C0 und D0 ausgeführt werden.</p>
Ein Datenbankserver mit einer 3-CPU-Lizenz und -gtc 5 angegeben	<ul style="list-style-type: none"> <li>• -gt 3</li> <li>• -gtc 5</li> </ul> <p>Threads können auf A0, A1, B0, B1 und C0 ausgeführt werden.</p>
Keine Lizenz einschränkungen auf der CPU mit angegebenem -gtc 1	<ul style="list-style-type: none"> <li>• -gt 4</li> <li>• -gtc 1</li> </ul> <p>Threads können nur auf A0 ausführen.</p>

#### Siehe auch

- [„Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175](#)
- [„Datenbankserveroption -gn “ auf Seite 244](#)
- [„Datenbankserveroption -gss “ auf Seite 250](#)
- [„Datenbankserveroption -gt “ auf Seite 251](#)
- [„Datenbankserveroption -gtc “ auf Seite 253](#)

## Datenbankserverkonfiguration der Multiprogramming-Stufe

Die **Multiprogramming Stufe** des Datenbankservers ist die maximale Anzahl der Aufgaben, die gleichzeitig aktiv sein können. Wenn eine clientseitige Anforderung auf dem Datenbankserver eintrifft, wird die Aufgabe, die für diese Anforderung erstellt wurde, einem Worker-Thread zugewiesen, sofern einer zur Verfügung steht. Eine Anforderung, die einem Worker-Thread zugewiesen ist, wird als **aktive Anforderung** bezeichnet. Wenn alle verfügbaren Worker-Threads belegt sind, wird die Anforderung in eine speziellen Warteschlange, der Warteschlange für nicht geplante Anforderungen, gestellt. Die Anforderung wird damit als nicht geplante Anforderung klassifiziert. Eine aktive Aufgabe ist eine Aufgabe, die derzeit von einem Worker-Thread verarbeitet wird. Eine aktive Aufgabe kann einen Zugriffsplan-Operator oder eine andere Funktion ausführen, kann aber auch beim Warten auf eine Ressource (wie z.B. auf einen I/O-Vorgang oder auf eine Zeilensperre) blockiert sein. Eine ungeplante Aufgabe ist eine Aufgabe, die für die Ausführung bereit ist, aber auf einen verfügbaren Worker-Thread wartet. Die Anzahl der aktiven Aufgaben, die gleichzeitig ausgeführt werden können, hängt von der Anzahl der Server-Threads und der Anzahl der logischen Prozessoren ab, die im System verwendet werden.

In SQL Anywhere können Datenbankadministratoren wählen, ob der Datenbankserver die Multiprogramming-Stufe aufgrund des Serverdurchsatzes dynamisch optimieren soll (Standardwert) oder ob die Multiprogramming-Stufe manuell konfiguriert werden soll. Sie haben zwei Möglichkeiten, die Einstellungen der Multiprogramming-Stufe zu konfigurieren: Wenn Sie einen Netzwerk-Datenbankserver starten, geben Sie Datenbankserveroptionen (-gna, -gnl und -gnh) an. Wenn der Datenbankserver dagegen bereits läuft, verwenden Sie für die sa\_server\_option-Systemprozedur die Eigenschaften MinMultiProgrammingLevel, MaxMultiProgrammingLevel und CurrentMultiProgrammingLevel.

Die folgende Tabelle gibt einen Überblick über die Befehlszeilen- und Serveroptionen für die Steuerung der Multiprogramming-Stufe des Datenbankservers:

Datenbankserver-Option (Datenbankserver starten)	sa_server_option-Wert (laufende Datenbankserver)	Beschreibung
-gn	CurrentMultiProgrammingLevel	Setzt die Multiprogramming-Stufe des Datenbankservers.
-gna	AutoMultiProgrammingLevel	Aktiviert und deaktiviert die dynamische Optimierung der Multiprogramming-Stufe des Netzwerk-Datenbankservers.
-gnh	MaxMultiProgrammingLevel	Legt die maximale Anzahl von Aufgaben fest, die der Netzwerk-Datenbankserver gleichzeitig ausführen kann.
-gnl	MinMultiProgrammingLevel	Legt die minimale Anzahl von Aufgaben fest, die der Netzwerk-Datenbankserver gleichzeitig ausführen kann.

### Multiprogramming-Stufe optimieren

SQL Anywhere-Netzwerkserver unterstützen sowohl die dynamische als auch die manuelle Optimierung der Multiprogramming-Stufe des Servers.

- Multiprogramming-Stufe dynamisch optimieren** SQL Anywhere-Netzwerkserver können den Durchsatz des Datenbankservers automatisch überwachen und ermitteln, wie die Multiprogramming-Stufe entsprechend der aktuellen Arbeitslast angepasst werden sollte. Der Netzwerk-Datenbankserver verwendet einen Bergsteigeralgorithmus sowie einen Parabelnäherungswert, um zu entscheiden, welche Änderungen vorgenommen werden sollen. Wenn eine Erhöhung der Multiprogramming-Stufe zu einer Erhöhung der Durchsatzstufe des Netzwerk-Datenbankservers führt, nimmt der Netzwerk-Datenbankserver die Erhöhung vor. Wenn die Erhöhung der Multiprogramming-Stufe zu einer Verschlechterung des Durchsatzes führt, senkt der Netzwerk-Datenbankserver die Multiprogramming-Stufe. Der Netzwerk-Datenbankserver überwacht die Durchsatzstufe kontinuierlich und ändert die Multiprogramming-Stufe, um den Serverdurchsatz zu verbessern. Bestehen die Arbeitslasten aus einer kurzzeitig hohen Anzahl von Anforderungen, denen lange Leerlaufperioden folgen, ist es am besten, die minimale Multiprogramming-Stufe auf die maximal erwartete Stufe für Mehrbenutzerbetrieb

festzulegen. Diese Konfiguration gewährleistet, dass der Netzwerk-Datenbankserver während der kurzen Stoßzeiten auf alle Anforderungen reagiert.

Die dynamische Optimierung der Multiprogramming-Stufe ist standardmäßig aktiviert (-gna 1). Die Netzwerk-Datenbankserveroptionen -gnl und -gnh legen die Mindest- und Höchstwerte der vom dynamischen Optimierungsalgorithmus verwendeten Multiprogramming-Stufe fest. Wenn die dynamische Optimierung aktiviert ist, versucht der Netzwerk-Datenbankserver außerdem, Thread-Deadlock-Probleme durch eine automatische Erhöhung der Multiprogramming-Stufe zu beheben. Der Netzwerk-Datenbankserver erhöht die Multiprogramming-Stufe kontinuierlich bis zum zulässigen MaxMultiprogrammingLevel-Wert. Wenn der MaxMultiprogrammingLevel-Wert erreicht wird, meldet der Netzwerk-Datenbankserver Thread-Deadlock-Probleme an die Clientanwendungen.

- **Multiprogramming-Stufe manuell optimieren** Sie können die Multiprogramming-Stufe erst manuell anpassen, wenn Sie die dynamische Optimierung deaktiviert haben. Es wird empfohlen, dass Sie die Arbeitslast Ihrer Anwendung testen, um die Auswirkungen der Multiprogramming-Stufe des Datenbankservers auf den Serverdurchsatz und die Anforderungsantwortzeiten zu analysieren. Hierzu können Sie das Verhalten der Datenbankserver analysieren, entweder mit dem Windows-Systemmonitor oder unter Unix mit dem Dienstprogramm für Performance-Statistiken (dbstats). Performance-Statistiken können mithilfe der Funktionen PROPERTY, DB\_PROPERTY und CONNECTION PROPERTY abgefragt werden.

Beobachten Sie bei dieser Analyse die Systemindikatoren, die sich auf aktive und ungeplante Anforderungen beziehen. Siehe [ActiveReq-Servereigenschaft auf Seite 745](#) und [UnschReq-Servereigenschaft auf Seite 763](#).

Wenn die Anzahl der aktiven Anforderungen stets niedriger als der Wert der Datenbankoption -gn ist, können Sie ein Herabsetzen der Multiprogramming-Stufe in Betracht ziehen, aber Sie müssen auch die Auswirkung der abfrageinternen Parallelität bedenken, die den Ausführungswarteschlangen des Datenbankservers zusätzliche Aufgaben hinzufügt. Wenn die abfrageinterne Parallelität marginal ist, kann die Multiprogramming-Stufe unbedenklich herabgesetzt werden, ohne den Gesamtdurchsatz des Systems abzusenken. Wenn allerdings die Anzahl aller Anforderungen (aktiv + ungeplant) häufig größer als der mit -gn angegebene Wert ist, ist möglicherweise eine Erhöhung der Multiprogramming-Stufe empfehlenswert. Wägen Sie erst die Vor- und Nachteile einer Erhöhung der Multiprogramming-Stufe für die Performance ab, bevor Sie sie ändern.

#### Siehe auch

- [ThreadDeadlocksAvoided-Servereigenschaft auf Seite 763](#)
- [Die Multiprogramming-Stufe erhöhen auf Seite 178](#)
- [„Datenbankserveroption -gn “ auf Seite 244](#)
- [„Datenbankserveroption -gna “ auf Seite 245](#)
- [„Datenbankserveroption -gnh “ auf Seite 246](#)
- [„Datenbankserveroption -gnl “ auf Seite 247](#)
- [„sa\\_server\\_option-Systemprozedur“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)

## Auswirkungen verschiedener Einstellungen der Multiprogramming-Stufe

Es kann schwierig sein, den optimalen Wert für die Multiprogramming-Stufe zu ermitteln. Beispiel:  
Wenn eine Anwendung gespeicherte Java-Prozeduren verwendet oder die abfrageinterne Parallelität

aktiviert ist, können die zusätzlichen, zur Verarbeitung dieser Anforderungen erstellten Serveraufgaben möglicherweise die aktuelle Multiprogramming-Stufe überschreiten. Die Ausführung dieser Aufgaben muss dann warten, bis eine andere Anforderung abgeschlossen ist. In diesen Fällen kann ein Erhöhen der Multiprogramming-Stufe das Richtige sein. Sie können die Multiprogramming-Stufe eines Netzwerk-Datenbankservers zu jedem beliebigen Zeitpunkt ändern. Es ist jedoch nicht möglich, die Multiprogramming-Stufe für Personal-Datenbankserver zu ändern, nachdem der Server gestartet wurde.

### Die Multiprogramming-Stufe erhöhen

Häufig steigt durch die Erhöhung der Multiprogramming-Stufe der Gesamtdurchsatz des Datenbankservers entsprechend. Eine Erhöhung der Multiprogramming-Stufe ermöglicht, dass gleichzeitig weitere Aufgaben ausgeführt werden können. Es gibt allerdings auch Nachteile bei der Erhöhung der Multiprogramming-Stufe, die bedacht werden sollten. Dazu gehören:

- **Vermehrte Konflikte** Indem Sie die Anzahl gleichzeitig möglicher Aufgaben erhöhen, erhöhen Sie möglicherweise auch die Wahrscheinlichkeit von Konflikten zwischen aktiven Anforderungen. Die Konflikte können Ressourcen wie Schemata und Zeilensperren bzw. interne Datenstrukturen des Datenbankservers und/oder Synchronisationsbasiselemente betreffen. So eine Situation kann den Serverdurchsatz durchaus verringern.
- **Zusätzlicher Server-Overhead** Jede aktive Aufgabe erfordert die Zuordnung und Aufrechterhaltung eines Worker-Threads sowie zusätzliche Protokollstrukturen, um ihre Zeitplanung zu steuern. Zusätzlich erfordert jeder Worker-Thread die Vorabzuweisung von Adressraum für den Ausführungs-Stack. Die Größe des Stacks variiert je nach Plattform. Auf Windows-Betriebssystemen wirkt sich die Zuweisung von Stack-Speicherplatz auf den Adressraum des Prozesses des Datenbankservers aus, aber der Stack-Speicher wird bei Bedarf zugewiesen. Auf Unix-Plattformen (einschließlich Linux) wird der Hintergrundspeicher für den Stack unmittelbar zugewiesen. Daher erhöht eine höhere Multiprogramming-Stufe den Speicherbedarf des Servers und vermindert die Menge des für den Cachemanager verfügbaren Speichers, weil die Menge des verfügbaren Adressraums vermindert wird.
- **Überlastung** Der Datenbankserver kann einen Zustand der Überlastung erreichen, bei dem er signifikante Ressourcenmengen nur zur Verwaltung des Ausführungs-Overheads verwendet, anstatt nützliche Arbeit für eine bestimmte Anforderung auszuführen. Dieser Zustand wird üblicherweise "Thrashing" genannt. Thrashing kann z.B. auftreten, wenn zu viele aktive Aufgaben um Speicherplatz im Datenbankserver-Cache wetteifern, aber der Cache nicht groß genug ist, die Arbeitsmenge von Datenbankseiten aufzunehmen, die von der Menge der aktiven Aufgaben verwendet wird. Diese Situation kann zu Seitenentzug ("page stealing") führen, auf eine ähnliche Weise, wie er bei Betriebssystemen auftreten kann.
- **Auswirkung auf die Abfrageverarbeitung** Der Datenbankserver wählt eine maximale Anzahl von speicherintensiven Anforderungen aus, die gleichzeitig abgearbeitet werden können. Auch wenn Sie die Multiprogramming-Stufe des Datenbankservers erhöhen, müssen Anforderungen möglicherweise warten, bis Speicher verfügbar wird. Siehe „[Cache und der Speichernutzungswächter](#)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].
- **Speicher für Datenstrukturen** Der Datenbankserver verwendet Ressourcen, um Anweisungen syntaktisch zu analysieren und zu optimieren. Bei sehr komplexen Anweisungen oder kleinen Cachegrößen kann der Speicher, der für Serverdatenstrukturen benötigt wird, die verfügbare Menge überschreiten. Ein Speichernutzungswächter beschränkt die Menge an Speicher, die für die

Serverdatenstrukturen der einzelnen Aufgaben verwendet wird. Jede Aufgabe hat folgenden angenäherten Grenzwert:

$$(3/4 \text{ maximum-cache-size}) / (\text{number-of-active-requests})$$

Wenn dieser Grenzwert überschritten wird, schlägt die Anweisung mit einem Fehler fehl.

### Die Multiprogramming-Stufe heruntersetzen

Ein Heruntersetzen der Multiprogramming-Stufe des Datenbankservers durch eine Verringerung der gleichzeitig ausführenden Aufgaben senkt üblicherweise den Durchsatz des Datenbankservers. Ein Heruntersetzen der Multiprogramming-Stufe kann jedoch die Antwortzeit einzelner Anforderungen verbessern, weil es weniger Anforderungen gibt, die um Ressourcen wetten, und weil eine geringere Wahrscheinlichkeit für Sperrenkonflikte besteht.

Wenn die Multiprogramming-Stufe zu niedrig angesetzt ist, kann ein Thread-Deadlock auftreten. Wenn die Multiprogramming-Stufe zur Arbeitslast passt, ist das Auftreten eines Thread-Deadlocks symptomatisch für ein Anwendungsdesignproblem, das zu substanziellen Konflikten führt und dadurch die Skalierbarkeit beeinträchtigt. Ein Beispiel ist eine Tabelle, die jede Anwendung ändern muss, wenn der Datenbank neue Daten hinzugefügt werden. Diese Technik wird häufig als Teil eines Schemas verwendet, um Primärschlüssel zu generieren. Die Konsequenz ist allerdings, dass alle Einfügetransaktionen der Anwendung tatsächlich serialisiert werden. Wenn die Rate der Einfügetransaktionen höher wird, als der Server aufgrund der Serialisierung der gemeinsam genutzten Tabelle verarbeiten kann, tritt üblicherweise ein Thread-Deadlock auf.

Die Datenbankserver-Option -gnl legt die niedrigste Multiprogramming-Stufe fest.

### Siehe auch

- „Deadlocks“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Datenbankserveroption -gn“ auf Seite 244
- „Datenbankserveroption -gna“ auf Seite 245
- „Datenbankserveroption -gnh“ auf Seite 246
- „Datenbankserveroption -gnl“ auf Seite 247
- „Datenbankserveroption -gns“ auf Seite 248
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Dienstprogramm für Performancestatistik (dbstats) (Unix)“ auf Seite 953
- „Optionen des Windows-Systemmonitors“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Verbindungs-, Datenbank- und Datenbankserveigenschaften“ auf Seite 710

### Manuelle Anpassung der Multiprogramming-Stufe

Sie können die Multiprogramming-Stufe eines Netzwerkserver manuell einstellen. Wenn jedoch die automatische Optimierung der Multiprogramming-Stufe aktiviert ist, stellt der Server die Multiprogramming-Stufe nach der manuellen Einstellung möglicherweise neu ein. Wenn Sie die Multiprogramming-Stufe herabsetzen, wird die neue Einstellung möglicherweise nicht sofort wirksam, da der Server warten muss, bis aktive Aufgaben abgeschlossen sind, bevor die neue Multiprogramming-Stufe in Kraft treten kann. Wenn Sie versuchen, die Multiprogramming-Stufe auf einen Wert außerhalb der Unter- bzw. Obergrenze zu setzen, die durch die Einstellungen MinMultiProgrammingLevel und MaxMultiProgrammingLevel festgelegt sind, wird ein Fehler zurückgegeben.

Sie können die automatische Optimierung der Multiprogramming-Stufe deaktivieren, wenn Sie den Datenbankserver starten oder wenn der Datenbankserver läuft:

- **Automatische Multiprogramming-Optimierung beim Serverstart deaktivieren** Wenn Sie den Netzwerk-Datenbankserver starten, geben Sie `-gna 0` an, um die automatische Optimierung der Multiprogramming-Stufe zu deaktivieren:

```
dbsrv16 -gna 0 ...
```

Sie können die Standard-Multiprogramming-Stufe mithilfe der Option `-gn` ändern und die Mindest- und Höchstwerte mit den Optionen `-gnl` bzw. `-gnh` festlegen.

- **Automatische Multiprogramming-Optimierung eines laufenden Servers deaktivieren** Wenn der Netzwerk-Datenbankserver bereits läuft, führen Sie die folgende SQL-Anweisung aus, um die automatische Optimierung der Multiprogramming-Stufe zu deaktivieren:

```
CALL sa_server_option ( 'AutoMultiProgrammingLevel', 'NO' );
```

Sie können die Mindest- und Höchstwerte mit den Eigenschaften `MinMultiProgrammingLevel` bzw. `MaxMultiProgrammingLevel` definieren. Zum Beispiel:

```
CALL sa_server_option ( 'MinMultiProgrammingLevel', 10 );  
CALL sa_server_option ( 'MaxMultiProgrammingLevel', 100 );
```

Sie können die aktuelle Multiprogramming-Stufe unter Verwendung der `CurrentMultiProgrammingLevel`-Eigenschaft wie folgt festlegen:

```
CALL sa_server_option ( 'CurrentMultiProgrammingLevel', 25 );
```

### Siehe auch

- „Datenbankserveroption `-gna`“ auf Seite 245
- „Datenbankserveroption `-gn`“ auf Seite 244
- „Datenbankserveroption `-gnh`“ auf Seite 246
- „Datenbankserveroption `-gnl`“ auf Seite 247
- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserver als Dienst oder Daemon ausführen

Wenn Sie sich bei einem Computer mit einer Benutzer-ID und einem Kennwort anmelden, wird eine **Sitzung** aufgenommen. Wenn Sie einen Datenbankserver oder eine andere Anwendung starten, läuft sie in dieser Sitzung. Wenn Sie sich abmelden, werden alle in dieser Sitzung geöffneten Anwendungen heruntergefahren.

Wenn der Datenbankserver jederzeit verfügbar sein muss, können Sie SQL Anywhere für Windows und für Unix so ausführen, dass der Datenbankserver weiterhin läuft, wenn Sie sich vom Computer abmelden.

- **Windows Dienst** Sie können den Windows-Datenbankserver als Dienst ausführen. Diese Konfiguration ist möglicherweise für Server in Hochverfügbarkeitssystemen geeignet.

- **Unix-Daemon** Sie können den Unix-Datenbankserver als Daemon betreiben, indem Sie die Option `-ud` verwenden. Damit kann der Datenbankserver im Hintergrund ausgeführt werden, und er läuft auch weiter, wenn Sie sich abmelden.
- **Linux-Dienst** Sie können den Linux-Datenbankserver als Dienst ausführen. Die Konfiguration hat einige bedeutende Vorteile bei Servern, die ständig verfügbar sein müssen.

### Programme, die als Dienste ausgeführt werden können

Sie können folgende Programme als Dienste ausführen:

- Netzwerk-Datenbankserver (*dsrv16*)
- Personal Datenbankserver (*dbeng16*)
- SQL Remote-Nachrichtenagent (*dbremote*)
- MobiLink-Server (*mlsrv16*)
- MobiLink-Synchronisationsclient (*dbmlsync*)
- MobiLink Relay Server (*rshost*)
- MobiLink Relay Server Outbound Enabler (*rsoe*)
- MobiLink Listener-Dienstprogramm (*dblsn*) (nur Windows)
- MobiLink-Agent (*mlagent*) (nur Windows)
- SQL Anywhere Broadcast Repeater-Dienstprogramm (*dbns16*)
- SQL Anywhere Volume-Schattenkopiedienst (*dbvss16*) (nur Windows)

Nicht alle diese Anwendungen werden in allen Editionen von SQL Anywhere mitgeliefert.

### Siehe auch

- „Windows-Dienste“ auf Seite 181
- „Datenbankserver als Daemon unter Unix“ auf Seite 192
- „Dienstprogramm für Dienste (dbsvc) für Linux“ auf Seite 968
- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974
- „Windows-Dienste erstellen (Sybase Central)“ auf Seite 182

## Windows-Dienste

Sie können den Datenbankserver sowohl als Dienst, als auch als normales Microsoft Windows-Programm ausführen. Allerdings bestehen Einschränkungen für das Ausführen des Datenbankservers als Standardprogramm, vor allem in Umgebungen mit mehreren Anwendungen.

### Einschränkungen für den Betrieb als Standardprogramm

Wenn Sie ein Programm starten, läuft es unter der Windows-Sitzung, in der Sie sich angemeldet haben. Wenn Sie sich abmelden, wird auch das Programm heruntergefahren. Diese Konfiguration schränkt die Nutzung des Computers ein, wenn es darum geht, ein Programm fast ständig auszuführen, wie es bei Datenbankservern in der Regel der Fall ist. Damit der Datenbankserver ununterbrochen läuft, müssen Sie ständig auf dem Computer angemeldet sein, auf dem der Server ausgeführt wird. Diese Konfiguration kann auch ein Sicherheitsrisiko darstellen, da der Benutzer auf dem Windows-Computer ständig angemeldet bleiben muss.

### Vorteile beim Betrieb als Dienst

Wenn eine Anwendung als Windows-Dienst eingerichtet wird, kann sie auch betrieben werden, nachdem sich der Benutzer abgemeldet hat.

Beim Start eines Dienstes meldet er sich mit einem speziellen Konto, dem so genannten LocalSystem-Konto, an (oder mit einem anderen von Ihnen festgelegten Konto). Da der Dienst nicht an die Benutzer-ID desjenigen gebunden ist, der ihn gestartet hat, wird er nicht gestoppt, wenn sich der Benutzer wieder abmeldet. Ein Dienst kann auch so konfiguriert werden, dass er automatisch startet, wenn der Windows-Computer hochfährt und bevor sich ein Benutzer anmeldet.

### Dienste verwalten

Sybase Central bietet eine einfachere und umfassendere Methode für die Verwaltung von SQL Anywhere-Diensten als der Dienste-Manager von Windows. Sie können mit dem Dienstprogramm dbsvc auch Dienste erstellen und ändern.

### Siehe auch

- [„Dienstprogramm für Dienste \(dbsvc\) für Windows“ auf Seite 974](#)

## Windows-Dienste erstellen (Sybase Central)

Sie können einen Windows-Dienst mit Sybase Central erstellen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Auf jedem Datenbankserver kann mehr als eine Datenbank ausgeführt werden. Wenn Sie mehr als eine Datenbank gleichzeitig ausführen möchten, sollten Sie neue Datenbanken zu Ihrem vorhandenen Windows-Dienst hinzufügen, statt neue Dienste zu erstellen.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Klicken Sie auf **Datei » Neu » Dienst**.
5. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen eines neuen Dienstes**.
  - Dienstnamen müssen in den ersten acht Zeichen eindeutig sein.
  - Wenn Sie einen Dienst in Sybase Central erstellen, geben Sie die Optionen für die Programmdatei, ohne den Namen der Programmdatei selbst anzugeben, im Fenster ein. Wenn z.B. ein

Netzwerkserver mit der Beispieldatenbank, einem Cache von 20 MB und dem Namen myserver gestartet werden soll, geben Sie im Feld **Parameter** des **Assistenten zur Erstellung von Diensten** in Sybase Central folgende Daten ein:

```
-c 20M
-n myserver "%SQLANY16%\demo.db"
```

Die Zeilenschaltungen können Sie optional benutzen.

- Wählen Sie das Konto, unter dem der Dienst ausgeführt werden soll: Das LocalSystem-Konto oder eine andere Benutzer-ID.

Weitere Informationen zu dieser Wahlmöglichkeit finden Sie unter [„Dienstkontooptionen“ auf Seite 187](#).

- Wenn der Dienst vom Windows-Desktop aus zugänglich sein soll, klicken Sie auf **Interaktion mit dem Desktop zulassen**. Wenn diese Option deaktiviert ist, wird in der Taskleiste kein Symbol angezeigt und auf dem Desktop erscheinen keine Fenster.
- Wenn Sie einen Dienst automatisch starten lassen wollen, wird er beim Start von Windows immer automatisch hochgefahren. Wenn Sie ihn manuell starten wollen, müssen Sie den Dienst jedes Mal aus Sybase Central starten. Es kann sinnvoll sein, zunächst auf **Deaktiviert** zu klicken, wenn Sie einen Dienst für zukünftige Zwecke einrichten möchten.

## Ergebnisse

Ein neuer Windows-Dienst wird erstellt.

## Siehe auch

- [„Dienstprogramm für Dienste \(dbsvc\) für Windows“ auf Seite 974](#)
- [„Windows-Dienste konfigurieren“ auf Seite 185](#)
- [„Verwendung des MobiLink-Servers außerhalb der aktuellen Sitzung“ \[MobiLink - Serveradministration\]](#)

## Windows-Dienste erstellen (Dienstprogramm dbsvc)

Sie können einen Windows-Dienst mit dem Dienstprogramm dbsvc erstellen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Auf jedem Datenbankserver kann mehr als eine Datenbank ausgeführt werden. Wenn Sie mehr als eine Datenbank gleichzeitig ausführen möchten, sollten Sie neue Datenbanken zu Ihrem vorhandenen Windows-Dienst hinzufügen, statt neue Dienste zu erstellen.

### Aufgabe

- Führen Sie das Dienstprogramm für Dienste (dbsvc) mit der Option -w aus.

### Ergebnisse

Ein neuer Windows-Dienst wird erstellt.

### Beispiel

Der folgende Befehl erstellt einen Windows-Dienst namens myserv, bei dem der Datenbankserver als Benutzer "LocalSystem" läuft.

```
dbsvc -as -w myserv "C:\Program Files\SQL Anywhere 16\Bin32\dbsrv16.exe"  
-n william -c 8m "c:\temp\sample.db"
```

### Siehe auch

- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974
- „Windows-Dienste konfigurieren“ auf Seite 185
- „Verwendung des MobiLink-Servers außerhalb der aktuellen Sitzung“ [*MobiLink - Serveradministration*]

## Windows-Dienste löschen (Sybase Central)

Sie können einen Windows-Dienst mit Sybase Central löschen, wobei der Dienstname aus der Liste der Dienste entfernt wird. Beim Löschen eines Windows-Diensts wird keine Software von der Festplatte entfernt.

### Voraussetzungen

Der Dienst muss gestoppt sein.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst, den Sie entfernen möchten, und klicken Sie dann auf **Löschen**.

### Ergebnisse

Der Windows-Dienst wird gelöscht.

### Siehe auch

- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974

## Windows-Dienste löschen (Dienstprogramm dbsvc)

Sie können einen Windows-Dienst mit dem Dienstprogramm dbsvc löschen, wobei der Dienstname aus der Liste der Dienste entfernt wird. Beim Löschen eines Windows-Diensts wird keine Software von der Festplatte entfernt.

### Voraussetzungen

Der Dienst muss gestoppt sein.

### Aufgabe

- Führen Sie das Dienstprogramm für Dienste (dbsvc) mit der Option -d aus.

### Ergebnisse

Die Windows-Dienst wird gelöscht.

### Beispiel

Führen Sie den folgenden Befehl aus, um den Dienst myserv zu löschen, ohne dass Sie zum Bestätigen aufgefordert werden.

```
dbsvc -y -d myserv
```

### Siehe auch

- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974

## Windows-Dienste konfigurieren

Ein Windows-Dienst führt Datenbankserver oder andere Anwendungen mit bestimmten Optionen und Eigenschaften aus, einschließlich der Eigenschaften, die das Konto angeben, unter dem der Dienst läuft, sowie der Bedingungen, unter denen er gestartet wird.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Änderungen an einer Dienstkonfiguration treten beim nächsten Starten des Diensts in Kraft.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.

3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst, den Sie konfigurieren möchten, und klicken Sie auf **Eigenschaften**.
5. Ändern Sie die Eigenschaften auf den Registerkarten des Fensters **Eigenschaften des Dienstes** nach Bedarf.
6. Klicken Sie auf **OK**, wenn Sie fertig sind.

### Ergebnisse

Die Eigenschaften für den Dienst werden geändert. Die Eigenschaft **Start** wird beim nächsten Starten von Windows übernommen.

### Startoptionen für

Die folgenden Optionen steuern das Startverhalten der SQL Anywhere-Dienste. Sie können diese Optionen auf der Registerkarte **Allgemein** des Fensters **Diensteigenschaften** einstellen.

- **Automatisch** Der Dienst startet, sobald das Windows-Betriebssystem hochgefahren ist. Diese Einstellung ist für Datenbankserver und andere Anwendungen geeignet, die immer laufen sollen.
- **Manuell** Der Dienst startet nur, wenn ihn ein Benutzer mit Administratorberechtigung startet. Informationen zu den Administratorberechtigungen entnehmen Sie Ihrer Windows-Dokumentation.
- **Disabled** Der Dienst startet nicht.

### Windows-Dienstoptionen

Die Optionen für einen Dienst sind identisch mit denen für die entsprechende Programmdatei.

#### Vorsicht

Die Registerkarte **Konfiguration** des Fensters **Diensteigenschaften** stellt ein Textfeld **Parameter** bereit, um Optionen für einen Dienst anzugeben. Geben Sie in dieses Feld nicht den Namen des Programms ein.

### Beispiele

Die folgende Eingabe im Feld **Parameter** startet den Netzwerkserverdienst my\_server mit zwei Datenbanken und einem Cache von 20 MB:

```
-c 20M  
-n my_server  
c:\db_1.db  
c:\db_2.db
```

Mit dem folgenden Befehl wird ein neuer SQL Remote-Nachrichtenagent gestartet und die Verbindung mit der Beispieldatenbank als Benutzer-ID DBA hergestellt:

```
-c "UID=DBA;PWD=sql;DBN=demo"
```

## Dienstkontooptionen

Sie können auswählen, unter welchem Konto der Dienst laufen soll. Standardmäßig laufen die meisten Dienste unter dem lokalen Systemkonto (LocalSystem). Sie können aber den Dienst so einrichten, dass er unter einem anderen Konto startet, indem Sie die Registerkarte **Konto** des Fensters **Diensteigenschaften** öffnen und die gewünschten Kontoinformationen eingeben.

Wenn der Dienst unter einem anderen Konto als LocalSystem laufen soll, muss dieses Konto das Privileg **Als Dienst anmelden** haben. Dieses Privileg kann in der Windows-Benutzerverwaltung unter "Erweiterte Berechtigungen" erteilt werden. Das Dienstprogramm für Dienste (dbsvc) kann ebenfalls verwendet werden, um dieses Privileg zu erteilen.

### Wenn ein Symbol in der Taskleiste angezeigt wird

- Wenn ein Dienst unter "LocalSystem" läuft und **Interaktion mit Desktop zulassen** des Fensters **Diensteigenschaften** ausgewählt wurde, erscheint ein Symbol auf dem Desktop jedes Benutzers, der sich auf dem Windows-Computer anmeldet, auf dem der Dienst läuft. Jeder Benutzer kann das Anwendungsfenster öffnen und das Programm stoppen, das als Dienst läuft.
- Wenn ein Dienst unter "LocalSystem" läuft und **Interaktion mit Desktop zulassen** im Fenster **Diensteigenschaften** nicht aktiviert wurde, erscheint kein Symbol auf dem Desktop der Benutzer. Nur Benutzer mit der Berechtigung, den Status eines Dienstes zu ändern, können den Dienst stoppen.
- Wenn ein Dienst unter einem anderen Konto läuft, erscheint kein Symbol auf dem Desktop. Nur Benutzer mit der Berechtigung, den Status eines Dienstes zu ändern, können den Dienst stoppen.

## Programmdateien für Dienste ändern

Wenn Sie die einem Dienst zugeordnete Programmdatei ändern möchten, klicken Sie auf die Registerkarte **Konfiguration** im Fenster **Eigenschaften des Dienstes**.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst, den Sie konfigurieren möchten, und klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Konfiguration**.
6. Geben Sie im Textfeld **Dateiname** den neuen Pfad und den Dateinamen ein.

Wenn Sie eine Programmdatei in ein neues Verzeichnis verschieben möchten, müssen Sie diesen Eintrag ändern.

### Ergebnisse

Die Programmdatei wird aktualisiert.

## Datenbanken zu Windows-Diensten hinzufügen

Sie können eine Datenbank zu einem Windows-Dienst hinzufügen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Auf jedem Datenbankserver kann mehr als eine Datenbank ausgeführt werden. Wenn Sie mehr als eine Datenbank gleichzeitig ausführen möchten, sollten Sie Datenbanken zu Ihrem vorhandenen Windows-Dienst hinzufügen, statt neue Dienste zu erstellen.

Datenbanken können auf laufenden Servern durch Clientanwendungen wie Interactive SQL gestartet werden.

Wenn eine Datenbank aus einer Anwendung gestartet wird, erfolgt keine Zuordnung zu einem Dienst. Wenn der Dienst gestoppt und neu gestartet wird, startet die zusätzliche Datenbank nicht auch automatisch.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst und klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Konfiguration**.
6. Fügen Sie Pfad und Dateinamen der neuen Datenbank am Ende der Optionenliste im Feld **Parameter** hinzu.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

### Ergebnisse

Die Datenbank wird beim nächsten Starten des Windows-Diensts gestartet.

**Siehe auch**

- „START DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „db\_start\_database-Funktion“ [[SQL Anywhere Server - Programmierung](#)]

## Einstellen der Aktualisierungsfrequenz

Standardmäßig aktualisiert Sybase Central die angezeigten Informationen alle 10 Sekunden. Sie können die Aktualisierungsfrequenz konfigurieren.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Beim Aktualisieren wird der Status (gestartet oder gestoppt) der einzelnen Windows-Dienste überprüft und die Spalte **Status** wird auf den jeweiligen Status aktualisiert. Zusätzlich aktualisiert Sybase Central dynamische Objekte, z.B. Verbindungen und Sperren, sowie die dynamischen Eigenschaften von Ereignissen und Wartungsplänen.

**Aufgabe**

1. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Voreinstellungen**.
2. Klicken Sie auf die Registerkarte **Automatische Aktualisierung**.
3. Klicken Sie auf **Automatische Aktualisierung aktivieren**.
4. Geben Sie ein Intervall in **Aktualisierung alle X Sekunden** ein.
5. Klicken Sie auf **Übernehmen**.
6. Klicken Sie auf **OK**.

**Ergebnisse**

Die Aktualisierungsfrequenz wird geändert.

## Windows-Dienste starten oder stoppen (Sybase Central)

Wenn Sie einen Dienst starten, läuft er, bis Sie ihn wieder stoppen. Wenn Sie Sybase Central schließen oder sich aus dem System abmelden, wird der Dienst nicht gestoppt.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst und klicken Sie dann auf **Start** bzw. **Stopp**.

### Ergebnisse

Der Windows-Dienst wird gestartet bzw. gestoppt. Durch das Stoppen eines Datenbankserver-Dienstes werden alle Verbindungen zur Datenbank getrennt und der Datenbankserver wird gestoppt. Bei anderen Anwendungen wird das Programm heruntergefahren.

## Der Dienste-Manager von Windows

Sie können Sybase Central für die Dienstverwaltung in SQL Anywhere benutzen. Obwohl Sie den **Dienste-Manager** von Windows in der **Systemsteuerung** für einige Aufgaben benutzen können, ist es nicht möglich, einen SQL Anywhere-Dienst über den **Dienste-Manager** von Windows zu installieren oder zu konfigurieren.

Wenn Sie den **Dienste-Manager** von Windows (aus der **Systemsteuerung**) aufrufen, wird eine Liste von Diensten angezeigt. Die Namen der SQL Anywhere-Dienste werden aus dem Präfix "SQL Anywhere" und dem Dienstenamen gebildet, den Sie beim Einrichten des Dienstes vergeben haben. Alle installierten Dienste erscheinen zusammen in der Liste.

## Dienstgruppen verwalten

In Sybase Central können Sie überprüfen, zu welcher Gruppe ein Dienst gehört, und dies ändern.

### Voraussetzungen

Sie müssen darauf achten, dass Ihre Dienste zur richtigen Gruppe gehören, bevor Sie sie so konfigurieren können, dass sie in der richtigen Reihenfolge gestartet werden.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst und klicken Sie auf **Eigenschaften**.

5. Klicken Sie auf die Registerkarte **Abhängigkeiten**. Im oberen Textfeld wird der Name der Gruppe angezeigt, zu der der Dienst gehört.

Standardmäßig gehört jeder Dienst zu einer Gruppe, wie dies in der folgenden Tabelle gezeigt wird.

Dienst	Standardgruppe
Netzwerkserver	SQLANYServer
Personal Server	SQLANYEngine
MobiLink-Synchronisationsclient	SQLANYMLSync
SQL Remote-Nachrichtenagent	SQLANYRemote
MobiLink-Server	SQLANYMobiLink
SQL Anywhere Broadcast Repeater-Dienstprogramm	SQLANYNS
MobiLink Listener	SQLANYLSN
SQL Anywhere Volume-Schattenkopiedienst	SQLANYVSS
MobiLink Relay Server	SQLANYRSHOST
MobiLink Relay Server Outbound Enabler	SQLANYRSOE
MobiLink-Agent	SQLANYMLAGENT

6. Klicken Sie auf **Ändern**, um eine Liste der verfügbaren Gruppen auf Ihrem System anzuzeigen.
7. Wählen Sie eine der Gruppen oder geben Sie den Namen einer neuen Gruppe ein.
8. Klicken Sie auf **OK**, um den Dienst dieser Gruppe zuzuordnen.

### Ergebnisse

Die Gruppendienste werden überprüft und geändert.

## Abhängigkeiten von Diensten verwalten

Sie können einen Dienst oder eine Gruppe mit Sybase Central zu einer Liste von Abhängigkeiten hinzufügen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

In manchen Fällen ist es nützlich, mehr als eine Programmdatei als Dienst auszuführen, wobei diese Programmdateien möglicherweise voneinander abhängen. Beispiel: Sie können einen Server und einen SQL Remote-Nachrichtenagenten verwenden, die die Replikation unterstützen sollen. Dienste müssen in der richtigen Reihenfolge gestartet werden. Wenn ein SQL Remote-Nachrichtenagent-Dienst startet, bevor der Server gestartet wurde, schlägt der Start fehl, da der Dienst den Server nicht finden kann. Sie können diese Probleme verhindern, indem Sie Dienstgruppen verwenden, die Sie über Sybase Central verwalten. Mit Sybase Central können Sie Abhängigkeiten für einen Dienst festlegen. Zum Beispiel:

- Sie können sicherstellen, dass mindestens ein Mitglied aus jeder Dienstgruppe in einer Liste gestartet wurde, bevor der aktuelle Dienst startet.
- Sie können sicherstellen, dass eine bestimmte Anzahl von Diensten vor dem aktuellen Dienst gestartet wurde. Beispiel: Sie wollen sicherstellen, dass ein bestimmter Netzwerkserver vor einem SQL Remote-Nachrichtenagent startet, der auf diesem Server ausgeführt werden soll.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **SQL Anywhere 16**.
3. Im rechten Fensterausschnitt klicken Sie auf die Registerkarte **Dienste**.
4. Rechtsklicken Sie auf den Dienst und klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Abhängigkeiten**.
6. Klicken Sie auf **Dienste hinzufügen** oder **Dienstgruppen hinzufügen**, um einen Dienst oder eine Gruppe der Liste der Abhängigkeiten hinzuzufügen.
7. Wählen Sie einen der Dienste oder Gruppen aus der Liste.
8. Klicken Sie auf **OK**, um den Dienst oder die Gruppe der Liste der Abhängigkeiten hinzuzufügen.

### Ergebnisse

Der Dienst bzw. die Gruppe wird zu einer Liste von Abhängigkeiten hinzugefügt.

## Datenbankserver als Daemon unter Unix

Um den Datenbankserver unter Unix im Hintergrund und damit unabhängig von der laufenden Sitzung zu betreiben, können Sie ihn als **Daemon** ausführen.

**Hinweis**

Verwenden Sie nicht die Option "&", um den Datenbankserver im Hintergrund auszuführen. Wenn Sie den Unix-Befehl "&" (kaufmännisches "Und") verwenden, um den Datenbankserver im Hintergrund auszuführen, funktioniert dies nicht, weil der Server entweder sofort herunterfährt oder aufhört zu reagieren. Sie müssen den Datenbankserver als Daemon ausführen.

Außerdem gilt: Wenn Sie versuchen, einen Server im Hintergrund aus einem Programm mit der Sequenz `fork() - exec()` zu starten, wird dies nicht funktionieren. Wenn Sie es tun müssen, fügen Sie die Option `-ud` der Liste der Datenbankserveroptionen hinzu.

Sie können den Unix-Datenbankserver als Daemon auf eine der folgenden Arten betreiben:

1. Benutzen Sie die Option `-ud`, wenn Sie den Datenbankserver starten. Zum Beispiel:

```
dbsrv16 -ud demo
```

2. Benutzen Sie das Tool "dbspawn", um den Datenbankserver zu starten. Zum Beispiel:

```
dbspawn dbsrv16 demo
```

Ein Vorteil von "dbspawn" besteht darin, dass der dbspawn-Prozess nicht heruntergefahren wird, bis er bestätigt hat, dass der Daemon gestartet wurde und bereit ist, Anforderungen entgegen zu nehmen. Wenn aus irgendeinem Grund der Daemon nicht startet, ist der Exit-Code für "dbspawn" ein von Null verschiedener Wert.

Wenn Sie den Daemon direkt mit der Option `-ud` starten, erstellt der Datenbankserver den Daemonprozess und kehrt sofort zurück (d.h., er wird beendet und der nächste Befehl kann ausgeführt werden), bevor der Daemon sich initialisiert oder versucht, eine der im Befehl angegebenen Datenbanken zu öffnen.

Wenn Sie sicherstellen möchten, dass ein Daemon eine oder mehrere Anwendungen ausführt, die den Datenbankserver verwenden können, können Sie mithilfe von dbspawn gewährleisten, dass der Daemon läuft, bevor Sie die Anwendungen starten. Nachstehend finden Sie ein Beispiel dafür, wie Sie einen Test mit einem csh-Skript ausführen.

```
#!/bin/csh
# start the server as a daemon and ensure that it is
# running before you start any applications
dbspawn dbsrv16 demo
if ( $status != 0 ) then
    echo Failed to start demo server
    exit
endif
# ok, now you can start the applications
...
```

Dieses Beispiel benutzt ein sh-Skript, um zu testen, ob der Daemon läuft, bevor die Anwendungen gestartet werden.

```
#!/bin/sh
# start the server as a daemon and ensure that it is
# running before you start any applications
dbspawn dbsrv16 demo
if [ $? != 0 ]; then
```

```
        echo Failed to start demo server
        exit
    fi
    # ok, now you can start the applications
    ...
```

3. Starten Sie einen Daemon aus einem C-Programm. Die Option `-ud` muss verwendet werden. Zum Beispiel:

```
...
if( fork() == 0 ) {
    /* child process = start server daemon */
    execl( "/opt/sqlanywhere16/bin/dbsrv16",
        "dbsrv16", "-ud", "demo" );
    exit(1);
}
/* parent process */
...
```

### Siehe auch

- „Datenbankserveroption `-ud`“ auf Seite 298
- „Dienstprogramm für den Serverstart im Hintergrund (`dbspawn`)“ auf Seite 983

## Authentifizierte SQL Anywhere-Anwendungen

Die OEM Edition von SQL Anywhere wird für Sybase OEM-Partner bereitgestellt. Bei der OEM Edition von SQL Anywhere kann eine authentifizierte Anwendung jeden beliebigen Vorgang in der Datenbank ausführen, abhängig von den der Benutzer-ID erteilten Privilegien.

Nicht-authentifizierte Verbindungen haben Lesezugriff und können Einfügungen, Aktualisierungen und Löschungen in temporären Tabellen durchführen. Die Verwendung von nicht-authentifizierten Verbindungen ermöglicht die Erstellung von komplexen Berichten unter Verwendung von gespeicherten Prozeduren und den Zugriff mittels Tools zur Erstellung von Berichten, wie z.B. Crystal Reports.

Das Authentifizierungsverfahren ist unabhängig von Anwendungsprogrammiersprachen und Tools und wird bei jeder Verbindung angewendet. Daher können Sie sowohl authentifizierte Verbindungen als auch eingeschränkte nicht-authentifizierte Verbindungen in Ihrer Anwendung verwenden.

Die Authentifizierung ist kein Sicherheitsmechanismus. Ein Benutzer, der einen nicht authentifizierten Datenbankserver in der Datenbank ausführt, kann jeden beliebigen Vorgang ausführen, abhängig vom üblichen SQL-Privilegschema.

## Entwicklung authentifizierter Anwendungen

Das Entwickeln einer authentifizierten Anwendung ist ein einfacher Prozess: Eine spezielle Authentifizierungssignatur wird in die Datenbank eingefügt und eine zweite Signatur wird in Ihre Anwendung aufgenommen. Wenn die Anwendung eine Verbindung mit der Datenbank herstellt, werden die Signaturen verglichen, um die Anwendung zu authentifizieren. Die folgenden Schritte sind erforderlich, um eine authentifizierte SQL Anywhere-Anwendung zu entwickeln:

1. „Authentifizierungssignaturen beziehen“ auf Seite 195
2. „Datenbanken authentifizieren (SQL)“ auf Seite 195
3. „Anwendung authentifizieren“ auf Seite 197

Alle in SQL Anywhere enthaltenen Datenbanktools wie Sybase Central, Interactive SQL und die Dienstprogramme, wie z.B. dbbackup, sind selbst-authentifizierend. Sie können Vorgänge uneingeschränkt in jeder authentifizierten Datenbank durchführen. Wenn die Datenbank selbst nicht authentifiziert ist, sind die Tools eingeschränkt (nur Lesezugriff).

Sie müssen die OEM Edition des SQL Anywhere-Datenbankservers für eine authentifizierte Anwendung verwenden. Diese Edition unterscheidet sich vom üblichen Datenbankserver nur darin, dass sie Authentifizierungsanweisungen verarbeitet. Die Authentifizierungsanweisungen werden von anderen Editionen des Datenbankservers ignoriert. Wenn Sie nicht den authentifizierten Datenbankserver verwenden, gibt es keine Einschränkungen für unauthentifizierte Anwendungen.

## Authentifizierungssignaturen beziehen

Beziehen Sie Authentifizierungssignaturen für Ihre Datenbank und Ihre Anwendung, um die OEM Edition verwenden zu können.

### Voraussetzungen

Um eine Authentifizierungssignatur zu erhalten, müssen Sie einen OEM-Vertrag mit Sybase iAnywhere haben.

### Aufgabe

1. Gehen Sie zu [http://www.sybase.com/sql\\_anywhere\\_authentication\\_registration](http://www.sybase.com/sql_anywhere_authentication_registration).
2. Füllen Sie das Formular aus, um Ihre Authentifizierungssignaturen zu beziehen. Die folgenden Daten werden in Ihr Authentifizierungsverfahren aufgenommen:
  - **Company** Der Name Ihrer Firma
  - **Application Name** Der Name Ihrer Anwendung

### Ergebnisse

Nachdem Sie das Formular ausgefüllt haben, erhalten Sie innerhalb von 48 Stunden per E-Mail eine Datenbanksignatur und eine Anwendungssignatur. Diese Signaturen sind lange Zeichenfolgen aus Buchstaben und Ziffern.

### Siehe auch

- „Datenbanken authentifizieren (SQL)“ auf Seite 195

## Datenbanken authentifizieren (SQL)

Sie können eine Datenbank mit der SET OPTION-Anweisung authentifizieren.

### Voraussetzungen

Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Aufgabe

1. Setzen Sie die database\_authentication-Option für die Datenbank mithilfe der folgenden SQL-Authentifizierungsanweisung:

```
SET OPTION PUBLIC.database_authentication='company=company-name;  
application=application-name;  
signature=database-signature';
```

#### Hinweis

Dem Syntaxbeispiel wurden Zeilenschaltungen hinzugefügt, um die Lesbarkeit zu verbessern. Die Syntax muss jedoch ohne Zeilenumbrüche und ohne Leerstellen zwischen dem Gleichheitszeichen und Semikola ausgeführt werden.

Die Argumente *company-name* und *application-name* sind die Werte, die Sie beim Erwerb Ihrer Signatur an Sybase übermittelt haben, und *database-signature* ist die Datenbanksignatur, die Sie von Sybase erhalten haben.

2. Starten Sie die Datenbank neu, damit die Option in Kraft tritt.

### Ergebnisse

Die Datenbank wird authentifiziert.

### Nächste Schritte

Sie können die Authentifizierungsanweisung in einem SQL-Skript speichern, um die Eingabe der langen Signatur zu vermeiden. Sie können das SQL-Skript von Interactive SQL aus ausführen, indem Sie auf **Datei » Skript ausführen** klicken.

Wenn Sie die Authentifizierungsanweisung in der Datei *authenticate.sql* im Unterverzeichnis *Scripts* Ihres SQL Anywhere-Installationsverzeichnisses erstellen und die Authentifizierungsanweisung in dieser Datei speichern, wird sie angewendet, wenn Sie eine Datenbank erstellen, neu aufbauen oder ein Upgrade durchführen.

### Siehe auch

- „SET OPTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „database\_authentication-Option“ auf Seite 597
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „Upgrade von authentifizierten Datenbanken“ auf Seite 200

### Überprüfen, ob eine Datenbank authentifiziert wird

Mit der DB\_PROPERTY-Funktion können Sie überprüfen, ob Ihre Datenbank authentifiziert wird.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Wenn der Datenbankserver eine authentifizierte Datenbank lädt, wird im Meldungsfenster des Datenbankservers eine Meldung angezeigt, die Beschreibungen der authentifizierten Firma und Anwendung enthält. Die Meldung hat folgende Form:

```
Diese Datenbank hat eine Lizenz für folgende Nutzung:  
Anwendung: application-name  
Firma: company-name
```

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie die DB\_PROPERTY-Funktion folgendermaßen aus:

```
SELECT DB_PROPERTY ( 'Authenticated' );
```

## Ergebnisse

Es wird eine Meldung zurückgegeben, die angibt, ob die Datenbank authentifziert wird.

## Siehe auch

- „DB\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „database\_authentication-Option“ auf Seite 597

## Anwendung authentifzieren

Eine authentifizierte Anwendung muss die Datenbankoption connection\_authentication unmittelbar nach dem Verbinden setzen. Die Option muss für jede Verbindung unmittelbar nach dem Herstellen der Verbindung gesetzt werden. ODBC- oder JDBC-Anwendungen fragen die Datenbank nach ihren Funktionen ab, und Sie haben möglicherweise keine Kontrolle über diese Aktionen. Daher hat jede Verbindung eine Frist von dreißig Sekunden, bevor die Einschränkungen wirksam werden. Diese Frist ermöglicht es einer Anwendung, sich unabhängig vom verwendeten Entwicklungstool zu authentifzieren.

Sie können der Authenticated-Verbindungseigenschaft entnehmen, ob die aktuelle Verbindung authentifziert wurde:

```
SELECT CONNECTION_PROPERTY ( 'Authenticated' );
```

Die folgende SQL-Anweisung authentifziert die Verbindung. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um die connection\_authentication-Datenbankoption setzen zu können.

```
SET TEMPORARY OPTION connection_authentication='company = company-name;  
application=application-name;  
signature=application-signature';
```

### Hinweis

Dem Syntaxbeispiel wurden Zeilenschaltungen hinzugefügt, um die Lesbarkeit zu verbessern. Die Syntax muss jedoch ohne Zeilenumbrüche und ohne Leerstellen zwischen dem Gleichheitszeichen und Semikola ausgeführt werden.

Die Option darf nur für die Dauer der Verbindung unter Verwendung des Schlüsselworts **TEMPORARY** gesetzt werden. Der *company-name* und der *application-name* müssen mit denjenigen in der Authentifizierungsanweisung für die Datenbank übereinstimmen. Die *application-signature* ist die Signatur, die Sie von Sybase erhalten haben.

Der Datenbankserver überprüft die Anwendungssignatur anhand der Datenbanksignatur. Wenn die Signatur überprüft wird, ist die Verbindung authentifiziert und es gelten nur die Einschränkungen, die durch die SQL-Privilegien festgelegt sind. Wenn die Signatur nicht überprüft wird, ist die Verbindung auf die Aktionen beschränkt, die von nicht authentifizierten Anwendungen zugelassen werden.

### Siehe auch

- „Liste der Verbindungseigenschaften“ auf Seite 711
- „connection\_authentication-Option“ auf Seite 593

## Ausführung der Authentifizierungsanweisung

Die Art, wie Sie die Anweisung **SET TEMPORARY OPTION** ausführen, um die Authentifizierungsoption zu setzen, hängt von der verwendeten Programmierschnittstelle ab. Die hier aufgelisteten Signaturen sind keine gültigen Signaturen. Beispiele werden für das Setzen der Authentifizierungsoption mit den folgenden Schnittstellen bereitgestellt:

- ODBC
- Sybase PowerBuilder
- JDBC
- ADO.NET
- Embedded SQL

### Hinweis

Wenn Ihr Firmenname Anführungszeichen, Apostrophe oder andere Sonderzeichen enthält (z.B. Joe's Garage), müssen Sie bei der Erstellung der Authentifizierungsanweisung besonders vorsichtig sein. Die gesamte Reihe der Authentifizierungsoptionen (**Company=...;Application=...;Signature=...**) ist eine SQL-Zeichenfolge. Die Regeln für Zeichenfolgen in SQL geben vor, dass ein Apostroph bzw. ein Anführungszeichen in der Zeichenfolge verdoppelt werden muss, um akzeptiert zu werden. Zum Beispiel:

```
SET TEMPORARY OPTION connection_authentication='Company = Joe''s Garage;  
Application=Joe''s Program;  
Signature=0fa55157edb8e14d818e...';
```

Dem Syntaxbeispiel wurden Zeilenschaltungen hinzugefügt, um die Lesbarkeit zu verbessern. Die Syntax muss jedoch ohne Zeilenumbrüche und ohne Leerstellen zwischen dem Gleichheitszeichen und Semikola ausgeführt werden.

**ODBC**

Verwenden Sie folgende Anweisung:

```
SQLExecDirect(
    hstmt,
    "SET TEMPORARY OPTION connection_authentication=
      'Company=MyCo;
      Application=MyApp;
      Signature=0fa55159999e14d818e...';",
    SQL_NTS
);
```

Die Zeichenfolge muss in einer Zeile eingegeben werden, oder Sie müssen sie durch eine Verkettung erstellen.

**Sybase PowerBuilder**

Verwenden Sie folgende PowerScript-Anweisung:

```
EXECUTE IMMEDIATE
  "SET TEMPORARY OPTION connection_authentication=
    'Company=MyCo;
    Application=MyApp;
    Signature=0fa551599998e14d818e...';"
USING SQLCA
```

**JDBC**

Verwenden Sie folgende Anweisung:

```
Statement Stmt1 = con.createStatement();
Stmt1.executeUpdate(
  "SET TEMPORARY OPTION connection_authentication=
    'Company=MyCo;
    Application=MyApp;
    Signature=0fa55159999e14d818e...';"
);
```

Die Zeichenfolge muss in einer Zeile eingegeben werden, oder Sie müssen sie durch eine Verkettung erstellen.

**ADO.NET**

Verwenden Sie folgende Anweisung:

```
SACommand cmd=new SACommand(
  "SET TEMPORARY OPTION connection_authentication=
    'Company=MyCo;
    Application=MyApp;
    Signature=0fa551599998e14d818e...';",
  con
);
cmd.ExecuteNonQuery();
```

Die Zeichenfolge muss in einer Zeile eingegeben werden, oder Sie müssen sie durch eine Verkettung erstellen.

**Embedded SQL**

```
Use the following statement:
EXEC SQL SET TEMPORARY OPTION connection_authentication=
```

```
'Company=MyCo;  
Application=MyApp;  
Signature=0fa551599998e14d818e...';
```

Die Zeichenfolge muss in einer Zeile eingegeben werden, oder Sie müssen sie durch eine Verkettung erstellen.

Bei der Herstellung einer Verbindung mit einer authentifizierten Datenbank werden der Verbindungs- und der Authentifizierungsschritt separat durchgeführt. Einige Objekte jedoch, wie z.B. das Microsoft Visual Basic Grid-Objekt, können eine separate, implizite Verbindung versuchen, die nicht automatisch eine Authentifizierung einschließt. In diesen Fällen wird die Verbindung nicht authentifiziert und der Datenbankvorgang kann fehlschlagen. Sie umgehen dieses Problem, indem Sie den Verbindungsparameter `InitString` in die Verbindungszeichenfolge aufnehmen. Das folgende Beispiel zeigt, wie Sie eine Microsoft Visual Basic-Anwendung ändern, um den Verbindungsparameter `InitString` einzubeziehen, damit auf jede Verbindung unmittelbar eine Authentifizierung folgt:

```
mConnectionString =  
"Provider=SAPROV.16;  
UID=DBA;  
PWD=sql;  
Host=test12;  
InitString=SET TEMPORARY OPTION connection_authentication=  
  'Company=MyCo;  
  Application=MyApp;  
  Signature=0fa55157edb8e14d818e...' "  
mdbName.ConnectionString = mConnectionString  
mdbName.Open  
mIsSQL = True
```

## Upgrade von authentifizierten Datenbanken

Sie können ein Upgrade einer authentifizierten Datenbank durchführen, indem Sie die Datei *authenticate.sql* im Verzeichnis *%SQLANY16%/Scripts* erstellen, bevor Sie das Upgrade durchführen oder die Datenbank neu aufbauen. Die Datei wird ausgeführt von den Anweisungen `CREATE DATABASE` und `ALTER DATABASE UPGRADE`, von den Dienstprogrammen `dbupgrad` und `dbunload` sowie vom **Assistenten zum Upgrade einer Datenbank**.

### Voraussetzungen

Um `PUBLIC`-Optionen setzen zu können, benötigen Sie das `SET ANY PUBLIC OPTION`-Systemprivileg.

Es wird empfohlen, Sicherungskopien der Datenbankdateien zu erstellen.

### Kontext und Bemerkungen

Die einzige Möglichkeit, Authentifizierungsinformationen beizubehalten, wenn Sie ein Upgrade durchführen oder die Datenbank neu aufbauen, besteht darin, die Authentifizierungsanweisung in der Datei *authenticate.sql* zu speichern.

## Aufgabe

1. Erstellen Sie eine Datei namens *authenticate.sql* im Verzeichnis *%SQLANY16%/Scripts*.
2. Fügen Sie den folgenden Inhalt in die Datei ein:

```
SET OPTION PUBLIC.database_authentication = 'authentication-statement'  
go
```

Das `go` muss in der Datei vorhanden sein. Andernfalls wird die Anweisung ignoriert.

## Ergebnisse

Das Upgrade der Datenbank wird durchgeführt.

## Nächste Schritte

Führen Sie das Upgrade durch oder bauen Sie die Datenbank neu auf. Welche Schritte Sie befolgen müssen, hängt davon ab, für welche Version der Datenbankdatei Sie das Upgrade bzw. den Neuaufbau durchführen.

## Siehe auch

- „*database\_authentication*-Option“ auf Seite 597.
- „Neuaufbauprozess für Datenbanken der Version 9 und höher“ [*SQL Anywhere 16 - Änderungen und Upgrades*]
- „Upgradevorgang für Datenbanken der Version 10 und später“ [*SQL Anywhere 16 - Änderungen und Upgrades*]
- „Neuaufbauprozess für Datenbanken der Version 10 und höher“ [*SQL Anywhere 16 - Änderungen und Upgrades*]

## Die *oem\_string*-Option über eine Anwendung abfragen

Die *oem\_string*-Datenbankoption speichert benutzerdefinierte Informationen in der Headerseite der Datenbankdatei. Sie können diesen Wert über eine Anwendung abfragen.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Die *oem\_string*-Option wird für authentifizierte Anwendungen gesetzt.

## Aufgabe

1. Öffnen Sie die *System-DBSpace*-Datei der Datenbank.
2. Lesen Sie die erste Seite der Datei in einen Puffer.

3. Durchsuchen Sie den Puffer nach den 2 Byte großen Präfix- und Suffixsequenzen vor und hinter der OEM-Zeichenfolge.

### Ergebnisse

Die Präfix- und Suffixzeichenfolgen sind in *sqldef.h* als DB\_OEM\_STRING\_PREFIX bzw. DB\_OEM\_STRING\_SUFFIX definiert. Alle Bytes zwischen diesen beiden Zeichenfolgen legen die OEM-Zeichenfolge fest, wie sie in der Datenbank definiert ist.

### Siehe auch

- „oem\_string-Option“ auf Seite 643
- oem\_string-Verbindungseigenschaft auf Seite 728

## SQL Anywhere unter Windows Vista und später

Die folgenden Hinweise gelten beim Ausführen von SQL Anywhere-Software unter Windows Vista und späteren Versionen von Windows:

- **Sicherheit** Diese Betriebssysteme umfassen ein integriertes Sicherheitsmodell zur Benutzerkontensteuerung namens User Account Control (UAC). Die Benutzerkontensteuerung ist standardmäßig aktiviert und kann das Verhalten von Programmen beeinflussen, die Dateien schreiben müssen, v.a. wenn der Computer mehrere Benutzer unterstützt. Abhängig davon, wo und wie Dateien und Verzeichnisse erstellt werden, gelten für eine von einem Benutzer erstellte Datei möglicherweise Berechtigungen, die es einem anderen Benutzer nicht gestatten, diese Datei zu lesen oder in sie zu schreiben. Wenn Sie SQL Anywhere in den Standardverzeichnissen installieren, werden die Dateien und Verzeichnisse, für die mehrere Benutzer Lese- bzw. Schreibberechtigung benötigen, entsprechend eingerichtet.
- **SQL Anywhere-Agent für Vorgänge mit erweiterten Berechtigungen** Für bestimmte Aktionen sind erweiterte Privilegien erforderlich, wenn sie unter der Benutzerkontensteuerung (User Account Control, UAC) ausgeführt werden. Die folgenden Programme erfordern möglicherweise erweiterte Berechtigungen in SQL Anywhere:
  - *dbdsn.exe*
  - *dbelevat16.exe*
  - *dblic.exe*
  - *dbsvc.exe*
  - *installULNet.exe*
  - *mlasinst.exe*
  - *SetupVSPackage.exe*
  - *ulcond16.exe*

Die folgenden DLLs erfordern erweiterte Berechtigungen, wenn sie registriert oder gelöscht werden:

- *dbctrs16.dll*
- *dbodbc16.dll*
- *dboledb16.dll*
- *dboledba16.dll*

Wenn die Benutzerkontensteuerung (UAC) aktiviert ist, erhalten Sie möglicherweise eine Erweiterungsaufforderung für den SQL Anywhere-Agenten für Vorgänge mit erweiterten Berechtigungen. Die Aufforderung wird vom Benutzerkontensteuerungssystem ausgegeben, um zu überprüfen, ob Sie weiterhin das gewählte Programm ausführen möchten (wenn Sie als Administrator angemeldet sind) oder ob Sie Administrator-Anmeldeinformationen angeben möchten (wenn Sie nicht als Administrator angemeldet sind).

- **Hinweise zum Deployment** Das Programm *dbelevat16.exe* wird intern von SQL Anywhere-Komponenten verwendet, um Vorgänge auszuführen, die erweiterte Privilegien erfordern. Diese Programmdatei muss in Deployments von SQL-Anywhere enthalten sein.
- **Signierte SQL Anywhere-Programmdateien** SQL Anywhere-Programmdateien werden von iAnywhere Solutions, Inc. signiert.
- **Windows-Dienste** Dienste, die mit Windows Vista, Windows 7 und Windows Server 2008 kompatibel sind, dürfen nicht mit dem Desktop interagieren. Unter diesen Betriebssystemen interagiert kein SQL Anywhere-Dienst mit dem Desktop (selbst wenn die Option **Interaktion mit dem Desktop zulassen** aktiviert wurde). SQL Anywhere-Datenbankserver können von Sybase Central aus oder mit dem SQL Anywhere-Konsolendienstprogramm (dbconsole) überwacht werden.

Sybase Central deaktiviert die Option für die Interaktion von Diensten mit dem Desktop unter diesen Betriebssystemen.

## Syntax des SQL Anywhere-Datenbankservers

Startet einen Datenbankserver.

### Syntax

```
dbsrv16
[ server-options ] [ database-file [ database-options ] ...]
```

### Serveroptionen

Serveroption	Beschreibung
@data	Liest Parameter aus einer Konfigurationsdatei oder Umgebungsvariablen ein. Siehe „@data -Datenbankserveroption“ auf Seite 214.
-?	Zeigt Syntaxinformationen an. Siehe „-? - Datenbankserveroption“ auf Seite 216.
-al userid [ ;userid ... ]	Lässt die Standard-Benutzerauthentifizierung für angegebene Benutzer zu. Siehe „Datenbankserveroption -al“ auf Seite 216.
-b	Ausführung im Massenvorgangsmodus. Siehe „Datenbankserveroption -b“ auf Seite 216.

Serveroption	Beschreibung
<b>-c</b> <i>size</i>	Stellt die Anfangscachegröße ein. Siehe „ <a href="#">Datenbankserveroption -c</a> “ auf Seite 217.
<b>-ca</b> 0	Deaktiviert die dynamische Cachedimensionierung [Windows, Unix, Mac OS X]. Siehe „ <a href="#">Datenbankserveroption -ca</a> “ auf Seite 219.
<b>-cc</b> { +   - }	Sammelt Informationen über Datenbankseiten, die zur Cache-Vorwärmung eingesetzt werden sollen. Siehe „ <a href="#">Datenbankserveroption -cc</a> “ auf Seite 220.
<b>-ch</b> <i>size</i>	Legt die obere Grenze der Cachegröße fest [Windows, Unix, Mac OS X]. Siehe „ <a href="#">Datenbankserveroption -ch</a> “ auf Seite 221.
<b>-chx</b> <i>size</i>	Reserviert Adressraum für eine Verwendung außerhalb des Caches [32-Bit Windows, 32-Bit Unix]. Siehe „ <a href="#">Datenbankserveroption -ch</a> “ auf Seite 221.
<b>-cl</b> <i>size</i>	Legt die untere Grenze der Cachegröße fest [Windows, Unix, Mac OS X]. Siehe „ <a href="#">Datenbankserveroption -cl</a> “ auf Seite 224.
<b>-cp</b> <i>location</i> [ ; <i>location</i> ... ]	Gibt eine Reihe von Verzeichnissen oder JAR-Dateien an, in denen nach Klassen gesucht werden soll. Siehe „ <a href="#">Datenbankserveroption -cp</a> “ auf Seite 225.
<b>-cr</b> { +   - }	Bereitet den Cache mit Datenbankseiten vor. Siehe „ <a href="#">Datenbankserveroption -cr</a> “ auf Seite 226.
<b>-cs</b>	Zeigt die Cachenutzung im Meldungsfenster des Datenbankservers an. Siehe „ <a href="#">Datenbankserveroption -cs</a> “ auf Seite 227.
<b>-cv</b> { +   - }	Steuert die Anzeige von Meldungen zur Cache-Vorwärmung im Meldungsfenster des Datenbankservers. Siehe „ <a href="#">Datenbankserveroption -cv</a> “ auf Seite 227.
<b>-dt</b> <i>temp-file-dir</i>	Gibt das Verzeichnis an, in dem temporäre Dateien gespeichert werden. Siehe „ <a href="#">Datenbankserveroption -dt</a> “ auf Seite 228.
<b>-ec</b> <i>encryption-options</i>	Aktiviert die Paketverschlüsselung [Netzwerkserver]. Siehe „ <a href="#">Datenbankserveroption -ec</a> “ auf Seite 230.
<b>-ep</b>	Fordert zur Eingabe des Chiffrierschlüssels auf. Siehe „ <a href="#">Datenbankserveroption -ep</a> “ auf Seite 233.
<b>-es</b>	Ermöglicht unverschlüsselte Verbindungen über gemeinsam genutzten Speicher. Siehe „ <a href="#">Datenbankserveroption -es</a> “ auf Seite 234.
<b>-f</b>	Erzwingt den Start der Datenbank ohne Transaktionslog. Siehe „ <a href="#">Datenbankserver-Wiederherstellungsoption -f</a> “ auf Seite 234.

Serveroption	Beschreibung
<b>-fc</b> <i>filename</i>	Gibt den Dateinamen der DLL an, die die volle Callback-Funktion für ein Dateisystem enthält. Siehe „ <a href="#">Datenbankserveroption -fc</a> “ auf Seite 235.
<b>-fips</b>	Verlangt die Verwendung von FIPS-zertifizierten Algorithmen für Datenbank- und Kommunikationsverschlüsselung [Windows, Unix und Linux]. Siehe „ <a href="#">Datenbankserveroption -fips</a> “ auf Seite 237.
<b>-ga</b>	Entlädt automatisch die Datenbank nach dem Schließen der letzten Client-Verbindung, die nicht über HTTP verbunden ist. Außerdem wird der Server nach dem Schließen der letzten Datenbank heruntergefahren. Siehe „ <a href="#">Datenbankserveroption -ga</a> “ auf Seite 238.
<b>-gb</b> <i>level</i>	Setzt die Datenbank-Prozessprioritätsklasse auf <i>level</i> [Windows, Unix, <b>Mac OS X</b> ]. Siehe „ <a href="#">Datenbankserveroption -gb</a> “ auf Seite 238.
<b>-gc</b> <i>num</i>	Setzt die maximale Zeit bis zum Checkpoint-Timeout auf <i>num</i> Minuten. Siehe „ <a href="#">Datenbankserveroption -gc</a> “ auf Seite 239.
<b>-gd</b> <i>level</i>	Legt das Privileg zum Starten der Datenbank fest. Siehe „ <a href="#">Datenbankserveroption -gd</a> “ auf Seite 240.
<b>-ge</b> <i>size</i>	Setzt die Stackgröße für Threads, die externe Funktionen ausführen. Siehe „ <a href="#">Datenbankserveroption -ge</a> “ auf Seite 241.
<b>-gf</b>	Deaktiviert das Auslösen von Triggern. Siehe „ <a href="#">Datenbankserveroption -gf</a> “ auf Seite 241.
<b>-gk</b> <i>level</i>	Legt fest, welches Privileg zum Stoppen des Servers erforderlich ist. Siehe „ <a href="#">Datenbankserveroption -gk</a> “ auf Seite 242.
<b>-gl</b> <i>level</i>	Legt fest, welches Privileg zum Laden oder Entladen von Daten erforderlich ist. Siehe „ <a href="#">Datenbankserveroption -gl</a> “ auf Seite 242.
<b>-gm</b> <i>num</i>	Setzt die maximale Anzahl von Verbindungen. Siehe „ <a href="#">Datenbankserveroption -gm</a> “ auf Seite 244.
<b>-gn</b> <i>num</i>	Setzt die Multiprogramming-Stufe des Datenbankservers. Siehe „ <a href="#">Datenbankserveroption -gn</a> “ auf Seite 244.
<b>-gna</b>	Steuert die automatische Optimierung der Multiprogramming-Stufe des Datenbankservers. Siehe „ <a href="#">Datenbankserveroption -gna</a> “ auf Seite 245.
<b>-gnh</b> <i>num</i>	Legt die maximale Anzahl von Aufgaben fest, die der Datenbankserver gleichzeitig ausführen kann. Siehe „ <a href="#">Datenbankserveroption -gnh</a> “ auf Seite 246.

Serveroption	Beschreibung
<b>-gnl</b> <i>num</i>	Legt die minimale Anzahl von Aufgaben fest, die der Datenbankserver gleichzeitig ausführen kann. Siehe „ <a href="#">Datenbankserveroption -gnl</a> “ auf Seite 247.
<b>-gns</b>	Gibt statistische Informationen über die Multiprogramming-Stufe im Meldungslog des Datenbankservers aus. Siehe „ <a href="#">Datenbankserveroption -gns</a> “ auf Seite 248.
<b>-gp</b> <i>size</i>	Setzt die maximale Seitengröße auf <i>size</i> Byte. Siehe „ <a href="#">Datenbankserveroption -gp</a> “ auf Seite 249.
<b>-gr</b> <i>minutes</i>	Legt die maximale Wiederherstellungszeit fest. Siehe „ <a href="#">Datenbankserveroption -gr</a> “ auf Seite 249.
<b>-gss</b> <i>size</i>	Setzt die Größe des Thread-Stacks auf <i>size</i> Byte. Siehe „ <a href="#">Datenbankserveroption -gss</a> “ auf Seite 250.
<b>-gt</b> <i>num</i>	Legt die maximale Anzahl von verwendbaren physischen Prozessoren (bis Lizenzlimit) fest. Diese Option ist nur bei Mehrprozessorsystemen sinnvoll. Siehe „ <a href="#">Datenbankserveroption -gt</a> “ auf Seite 251.
<b>-gta</b> <i>logical-processors-to-use,...</i>	Legt fest, welche logischen Prozessoren der Datenbankserver verwenden kann. Siehe „ <a href="#">Datenbankserveroption -gta</a> “ auf Seite 252.
<b>-gtc</b> <i>logical-processors-to-use</i>	Steuert die maximal möglichen gleichzeitigen Prozessoren, die der Datenbankserver zulässt. Siehe „ <a href="#">Datenbankserveroption -gtc</a> “ auf Seite 253.
<b>-gu</b> <i>level</i>	Legt die Privilegstufe für Dienstprogrammbefehle fest: <i>utility_db</i> , <i>all</i> , <i>none</i> oder <i>DBA</i> . Siehe „ <a href="#">Datenbankserveroption -gu</a> “ auf Seite 255.
<b>-im</b> <i>submode</i>	Führt den Datenbankserver im Speicher aus und reduziert oder eliminiert damit Schreibvorgänge auf der Festplatte. Siehe „ <a href="#">Datenbankserveroption -im</a> “ auf Seite 257.
<b>-k</b>	Steuert die Sammlung von Systemmonitor-Statistiken. Siehe „ <a href="#">Datenbankserveroption -k</a> “ auf Seite 259.
<b>-kl</b> <i>GSS-API-library-file</i>	Gibt den Dateinamen der Kerberos GSS-API-Bibliothek (oder eines Shared Object unter Unix) an und aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver. Siehe „ <a href="#">Datenbankserveroption -kl</a> “ auf Seite 260.
<b>-kp</b> <i>server-principal</i>	Gibt den Kerberos-Serverprinzipal an und aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver. Siehe „ <a href="#">Datenbankserveroption -kp</a> “ auf Seite 261.

Serveroption	Beschreibung
<b>-kr</b> <i>server-realm</i>	Gibt den Bereich des Kerberos-Serverprinzipals an und aktiviert Kerberos-authentifizierte Verbindungen mit dem Datenbankserver. Siehe „ <a href="#">Datenbankserveroption -kr (nicht mehr empfohlen)</a> “ auf Seite 262.
<b>-krb</b>	Aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver. Siehe „ <a href="#">Datenbankserveroption -krb</a> “ auf Seite 263.
<b>-ks</b>	Deaktiviert die Erstellung von gemeinsam genutztem Speicher, der vom Systemmonitor verwendet wird, um Leistungsindikatorwerte vom Datenbankserver zu sammeln [Windows]. Siehe „ <a href="#">Datenbankserveroption -ks</a> “ auf Seite 264.
<b>-ksc</b>	Legt die maximale Anzahl von Verbindungen fest, die der Systemmonitor überwachen kann [Windows]. Siehe „ <a href="#">Datenbankserveroption -ksc</a> “ auf Seite 264.
<b>-ksd</b>	Legt die maximale Anzahl von Datenbanken fest, die der Systemmonitor überwachen kann [Windows]. Siehe „ <a href="#">Datenbankserveroption -ksd</a> “ auf Seite 264.
<b>-m</b>	Kürzt das Transaktionslog nach jedem Checkpoint für alle Datenbanken. Siehe „ <a href="#">Datenbankserveroption -m</a> “ auf Seite 265.
<b>-n</b> <i>name</i>	Verwendet <i>name</i> als Namen des Datenbankservers. <i>Die Option -n ist positionsabhängig.</i> Siehe „ <a href="#">Datenbankserveroption -n</a> “ auf Seite 266.
<b>-o</b> <i>Dateiname</i>	Gibt Meldungen in die festgelegte Datei aus. Siehe „ <a href="#">Datenbankserveroption -o</a> “ auf Seite 268.
<b>-oe</b> <i>Dateiname</i>	Gibt die Logdatei für Startfehler, schwerwiegende Fehler und Assertions an. Siehe „ <a href="#">Datenbankserveroption -oe</a> “ auf Seite 269.
<b>-on</b> <i>Größe</i>	Gibt eine maximale Größe für die Datenbankserver-Nachrichtenlogdatei an, bei deren Erreichen die Datei mit der Erweiterung <i>.old</i> umbenannt und eine neue Datei gestartet wird. Siehe „ <a href="#">Datenbankserveroption -on</a> “ auf Seite 269.
<b>-os</b> <i>Größe</i>	Begrenzt die Größe der Logdatei für Nachrichten. Siehe „ <a href="#">Datenbankserveroption -os</a> “ auf Seite 270.
<b>-ot</b> <i>Dateiname</i>	Kürzt die Meldungslogdatei des Datenbankservers und fügt anschließend Ausgabemeldungen an. Siehe „ <a href="#">Datenbankserveroption -ot</a> “ auf Seite 271.
<b>-p</b> <i>Paketgröße</i>	Setzt die maximale Kommunikationspaketgröße [Netzwerkserver]. Siehe „ <a href="#">Datenbankserveroption -p</a> “ auf Seite 271.

Serveroption	Beschreibung
<b>-pc</b>	Komprimiert alle Kommunikationspakete außer Verbindungen auf demselben Computer. Siehe „Datenbankserveroption -pc“ auf Seite 272.
<b>-pt</b> <i>Größe_in_Byte</i>	Legt die Mindest-Netzwerkpaketgröße zum Komprimieren fest. Siehe „Datenbankserveroption -pt“ auf Seite 273.
<b>-qi</b>	Zeigt das Datenbankserver-Taskleistensymbol bzw. das Meldungsfenster des Datenbankservers nicht an [Windows]. Siehe „Datenbankserveroption -qi“ auf Seite 273.
<b>-qn</b>	Minimiert das Meldungsfenster des Datenbankservers beim Start nicht [Windows und Linux]. Siehe „Datenbankserveroption -qn“ auf Seite 274.
<b>-qp</b>	Unterdrückt Meldungen über die Performance im Meldungsfenster des Datenbankservers. Siehe „Datenbankserveroption -qp“ auf Seite 275.
<b>-qs</b>	Unterdrückt Fehlermeldungen beim Start [Windows]. Siehe „Datenbankserveroption -qs“ auf Seite 275.
<b>-qw</b>	Zeigt nicht das Meldungsfenster des Datenbankservers an. Siehe „Datenbankserveroption -qw“ auf Seite 276.
<b>-r</b>	Öffnet die Datenbank im schreibgeschützten Modus. Siehe „Datenbankserveroption -r“ auf Seite 277.
<b>-s</b> <i>Facility-ID</i>	Legt die Syslog-Facility-ID fest [Unix, Mac OS X]. Siehe „Datenbankserveroption -s“ auf Seite 278.
<b>-sb</b> { 0   1 }	Legt fest, wie der Server auf Broadcasts reagiert. Siehe „Datenbankserveroption -sb“ auf Seite 278.
<b>-sbx</b> { +   - }	Steuert die Sandboxing-Standardeinstellungen für alle auf dem Datenbankserver gestarteten Datenbanken, die keine expliziten Sandboxing-Einstellungen haben. Siehe „Datenbankserveroption -sbx“ auf Seite 279.
<b>-sf</b> <i>Funktionsliste</i>	Sichert Funktionen bei auf diesem Datenbankserver laufenden Datenbanken. Siehe „Datenbankserveroption -sf“ auf Seite 280.
<b>-sk</b> <i>Schlüssel</i>	Gibt einen Schlüssel zum Aktivieren von Funktionen an, die auf dem Datenbankserver deaktiviert sind. Siehe „Datenbankserveroption -sk“ auf Seite 288.
<b>-su</b> <i>Kennwort</i>	Legt das Kennwort für den DBA-Benutzer der Dienstprogrammdatenbank (utility_db) fest oder deaktiviert Verbindungen zur Dienstprogrammdatenbank. Siehe „Datenbankserveroption -su“ auf Seite 289.

Serveroption	Beschreibung
<b>-tdsl</b>	Legt den TDS-Login-Anforderungsmodus fest. Siehe „Datenbankserveroption -tdsl“ auf Seite 290.
<b>-ti</b> <i>Minuten</i>	Setzt die Client-Leerlaufzeit vor dem Herunterfahren. Der Standardwert ist 240 Minuten. Siehe „Datenbankserveroption -ti“ auf Seite 291.
<b>-tl</b> <i>Sekunden</i>	Setzt den Standardwert für das Verfügbarkeits-Timeout für Clients in Sekunden. Der Standardwert ist 120 Sekunden. Siehe „Datenbankserveroption -tl“ auf Seite 292.
<b>-tmf</b>	Erzwingt die Transaktions-Manager-Wiederherstellung bei verteilten Transaktionen [Windows]. Siehe „Datenbankserveroption -tmf“ auf Seite 293.
<b>-tmt</b> <i>Millisekunden</i>	Legt das Wiederaufnahme-Timeout bei verteilten Transaktionen fest [Windows]. Siehe „Datenbankserveroption -tmt“ auf Seite 294.
<b>-tq</b> <i>Zeit</i>	Setzt den Beendigungszeitpunkt [Netzwerkserver]. Siehe „Datenbankserveroption -tq“ auf Seite 294.
<b>-ts</b>	Richtet eine Datenbankserver-Trace-Sitzung ein.
<b>-u</b>	Verwendet gepufferte I/O-Vorgänge [Windows, Unix, Mac OS X]. Siehe „Datenbankserveroption -u“ auf Seite 296.
<b>-ua</b>	Deaktiviert die Verwendung von asynchronen I/O-Vorgängen [Linux]. Siehe „Datenbankserveroption -ua“ auf Seite 297.
<b>-uc</b>	Startet den Datenbankserver im Shell-Modus [Unix und Mac OS X]. Siehe „Datenbankserveroption -uc“ auf Seite 297.
<b>-ud</b>	Wird als Daemon ausgeführt [Unix, Mac OS X]. Siehe „Datenbankserveroption -ud“ auf Seite 298.
<b>-uf</b>	Legt die Aktion fest, die der Datenbankserver ausführt, wenn ein schwerwiegender Fehler oder ein Assertierungsfehler auf einem Datenbankserver auftritt. Siehe „Datenbankserveroption -uf“ auf Seite 298.
<b>-ufd</b>	Legt die Aktion fest, die der Datenbankserver ausführt, wenn ein schwerwiegender Fehler oder ein Assertierungsfehler in einer Datenbank auftritt. Siehe „Datenbankserveroption -ufd“ auf Seite 299.
<b>-ui</b>	Öffnet das Fenster <b>Startoptionen für den Server</b> und zeigt das Meldungsfenster des Datenbankservers an oder startet den Datenbankserver im Shell-Modus, wenn keine nutzbare Anzeige vorhanden ist [Linux]. Siehe „Datenbankserveroption -ui“ auf Seite 300.

Serveroption	Beschreibung
<b>-um</b>	Öffnet das Fenster <b>Startoptionen für den Server</b> und zeigt das Meldungsfenster des Datenbankservers an, wenn <i>DBLauncher.app</i> ausgeführt wird [Mac OS X]. Siehe „ <a href="#">Datenbankserveroption -um</a> “ auf Seite 300.
<b>-ut</b> <i>Minuten</i>	Aktualisiert temporäre Dateien alle <i>min</i> Minuten [Unix, Mac OS X]. Siehe „ <a href="#">Datenbankserveroption -ut</a> “ auf Seite 301.
<b>-ux</b>	Zeigt das Meldungsfenster des Datenbankservers und das Fenster <b>Server-Startoptionen</b> an [Linux]. Siehe „ <a href="#">Datenbankserveroption -ux</a> “ auf Seite 302.
<b>-v</b>	Zeigt die Version des Datenbankservers an und stoppt. Siehe „ <a href="#">Datenbankserveroption -v</a> “ auf Seite 303.
<b>-vss</b> { +   - }	Aktiviert und deaktiviert den Volume Shadow Copy Service (VSS, Schattenkopiedienst) [Windows]. Siehe „ <a href="#">Datenbankserveroption -vss</a> “ auf Seite 303.
<b>-wc</b> { +   - }	Aktiviert Schreib-Prüfsummen bei auf dem Datenbankserver laufenden Datenbanken. Siehe „ <a href="#">Datenbankserveroption -wc</a> “ auf Seite 304.
<b>-x</b> <i>list</i>	Gibt eine kommasetrennte Liste der zu verwendenden Kommunikationsprotokolle an. Siehe „ <a href="#">Datenbankserveroption -x</a> “ auf Seite 305.
<b>-xa</b> <i>Authentifizierungsinformationen</i>	Gibt eine Liste von Datenbanknamen und Authentifizierungszeichenfolgen für einen Arbiterserver an. Siehe „ <a href="#">Datenbankserveroption -xa</a> “ auf Seite 306.
<b>-xd</b>	Verhindert, dass der Datenbankserver der Standarddatenbankserver wird. Siehe „ <a href="#">Datenbankserveroption -xd</a> “ auf Seite 307.
<b>-xf</b> <i>state-file</i>	Gibt den Speicherort der Datei an, die zur Aufrechterhaltung von Statusinformationen über Ihr Datenbank-Spiegelungssystem verwendet wird. Siehe „ <a href="#">Datenbankserveroption -xf</a> “ auf Seite 308.
<b>-xm</b> <i>seconds</i>	Legt die Zeit zum Überprüfen auf neue IP-Adressen in Sekunden fest. Der Mindestwert ist 10, der Standardwert 0. Bei einem tragbaren Gerät beträgt der Standardwert 120. Siehe „ <a href="#">Datenbankserveroption -xm</a> “ auf Seite 309.
<b>-xs</b>	Gibt serverseitige Webdienst-Kommunikationsprotokolle an. Siehe „ <a href="#">Datenbankserveroption -xs</a> “ auf Seite 310.
<b>-z</b>	Liefert Diagnoseinformationen zu Kommunikationsverbindungen [Netzwerkserver]. Siehe „ <a href="#">Datenbankserveroption -z</a> “ auf Seite 312.

Serveroption	Beschreibung
<b>-ze</b>	Zeigt Datenbankserver-Umgebungsvariable im Meldungsfenster des Datenbankservers an. Siehe „ <a href="#">Datenbankserveroption -z</a> “ auf Seite 312.
<b>-zl</b>	Aktiviert die Aufzeichnung der zuletzt vorbereiteten SQL-Anweisung bei jeder Verbindung. Siehe „ <a href="#">Datenbankserveroption -zl</a> “ auf Seite 313.
<b>-zn integer</b>	Gibt die Anzahl der aufzubewahrenden Kopien der Anforderungs-Logdatei an. Siehe „ <a href="#">Datenbankserveroption -zn</a> “ auf Seite 314.
<b>-zo filename</b>	Leitet Informationen der Anforderungsprotokollierung in eine eigene Datei um. Siehe „ <a href="#">Datenbankserveroption -zo</a> “ auf Seite 315.
<b>-zoc</b>	Leitet Webdienst-Clientinformationen in eine Datei um. Siehe „ <a href="#">Datenbankserveroption -zoc</a> “ auf Seite 315.
<b>-zp</b>	Aktiviert die Aufzeichnung des zuletzt vom Abfrageoptimierer verwendeten Plans. Siehe „ <a href="#">Datenbankserveroption -zp</a> “ auf Seite 316.
<b>-zr level</b>	Aktiviert die Protokollierung von SQL-Vorgängen. Der Standardwert ist NONE. Siehe „ <a href="#">Datenbankserveroption -zr</a> “ auf Seite 317.
<b>-zs size</b>	Begrenzt die Größe der für die Anforderungsprotokollierung verwendeten Logdatei. Siehe „ <a href="#">Datenbankserveroption -zs</a> “ auf Seite 319.
<b>-zt</b>	Aktiviert die Protokollierung der Anforderungszeitinformationen. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.

### Datenbankoptionen

Die folgenden Optionen können nur nach einem Datenbank-Dateinamen in der Datenbankserver-Befehlszeile angegeben werden.

Datenbankoption	Beschreibung
<b>-a filename</b>	Übernimmt die angegebene Transaktionslogdatei. Siehe „ <a href="#">Datenbankoption -a</a> “ auf Seite 321.
<b>-ad log-directory</b>	Gibt das Logverzeichnis an, das die in der Datenbank verwendeten Transaktionslogdateien enthält. Siehe „ <a href="#">Datenbankoption -ad</a> “ auf Seite 322.
<b>-al userid [ ;userid ... ]</b>	Lässt die Standard-Benutzerauthentifizierung für angegebene Benutzer der angegebenen Datenbank zu. Siehe „ <a href="#">Datenbankoption -al</a> “ auf Seite 323.
<b>-ar</b>	Übernimmt alle Logdateien in die Datenbank, die sich im selben Verzeichnis wie das Transaktionslog befinden. Siehe „ <a href="#">Datenbankoption -ar</a> “ auf Seite 323.

Datenbankoption	Beschreibung
<b>-as</b>	Führt die Datenbank weiter aus, nachdem Transaktionslogs übernommen wurden (zusammen mit -ad oder -ar verwendet). Siehe „Datenbankoption -as“ auf Seite 324.
<b>-dh</b>	Zeigt die Datenbank nicht an, wenn dblocate auf diesem Server verwendet wird. Siehe „Datenbankoption -dh“ auf Seite 326.
<b>-ds</b>	Gibt den Standort der DBSpaces für die Datenbank an. Siehe „Datenbankoption -ds“ auf Seite 325.
<b>-ek</b> <i>key</i>	Gibt den Chiffrierschlüssel an. Siehe „Datenbankoption -ek“ auf Seite 326.
<b>-m</b>	Kürzt (löscht) das Transaktionslog nach jedem Checkpoint für die angegebene Datenbank. Siehe „Datenbankoption -m“ auf Seite 327.
<b>-n</b> <i>name</i>	Benennt die Datenbank. <i>Die Option -n ist positionsabhängig.</i> Siehe „Datenbankoption -n“ auf Seite 328.
<b>-r</b>	Öffnet die angegebenen Datenbanken im schreibgeschützten Modus. Datenbankänderungen nicht zulassen. Siehe „Datenbankoption -r“ auf Seite 329.
<b>-sbx</b> { +   - }	Steuert das Sandboxing für die Datenbank, durch das Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt werden, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse. Siehe „Datenbankoption -sbx“ auf Seite 330.
<b>-sm</b>	Stellt einen Datenbankservernamen bereit, der benutzt werden kann, um auf die schreibgeschützte Spiegeldatenbank zuzugreifen. Siehe „Datenbankoption -sm (nicht mehr empfohlen)“ auf Seite 331.
<b>-sn</b> <i>alternate-server-name</i>	Gibt einen alternativen Servernamen für eine einzelne auf einem Datenbankserver laufende Datenbank an. Siehe „Datenbankoption -sn“ auf Seite 332.
<b>-wc</b> [ +   - ]	Aktiviert Schreib-Prüfsummen bei auf dem Datenbankserver laufenden Datenbanken. Siehe „Datenbankoption -wc“ auf Seite 334.
<b>-xp</b> <i>mirroring-options</i>	Stellt einem betriebsbereiten Server Informationen bereit, mit denen er sich mit seinem Partner und dem Arbiter verbinden kann, wenn Datenbankspiegelung verwendet wird. Siehe „Datenbankoption -xp“ auf Seite 335.

## Bemerkungen

Der Befehl für den Datenbankserver enthält folgende Elemente:

- **Programmdatei** Mit dem Befehl **dbeng16** wird ein Personal Datenbankserver gestartet.

Mit dem Befehl **dbsrv16** wird ein Netzwerk-Datenbankserver gestartet.

Die Unterstützung für TCP/IP im Netzwerkserver ermöglicht die Durchführung von Aufgaben vom Desktopcomputer aus, einschließlich Datenbankmanagement mit Sybase Central.

Unter Windows-Betriebssystemen mit Ausnahme von Windows Mobile lautet der Name der Programmdatei des Personal Datenbankservers *dbeng16.exe*. Unter Unix-Betriebssystemen lautet der Name *dbeng16*.

Unter Windows-Betriebssystemen einschließlich Windows Mobile lautet der Name der Programmdatei des Netzwerk-Datenbankservers *dbsrv16.exe*. Unter Linux- und Unix-Betriebssystemen lautet der Name *dbsrv16*.

- **Serveroptionen** Diese Optionen steuern das Verhalten des Datenbankservers für alle laufenden Datenbanken.
- **Datenbankdatei** Sie können keinen, einen oder mehrere Datenbanknamen eingeben. Alle diese Datenbanken werden geladen und stehen Anwendungen zur Verfügung.

**Vorsicht**

Die Datenbankdatei und die Transaktionslogdatei müssen sich auf demselben physischen Computer wie der Datenbankserver befinden, oder es muss auf sie über eine SAN- bzw. iSCSI-Konfiguration zugegriffen werden. Wenn sich Datenbankdateien und Transaktionslogdateien in einem entfernten Netzwerkverzeichnis befinden, kann dies zu schlechter Performance, zur Beschädigung von Daten und zur Instabilität des Datenbankservers führen.

Weitere Hinweise finden Sie unter <http://www.sybase.com/detail?id=1034790>.

Die besten Ergebnisse werden erzielt, wenn das Transaktionslog nicht auf derselben Festplatte wie die Datenbankdateien gespeichert wird. Siehe „Das Transaktionslog“ auf Seite 135.

- **Datenbankoptionen** Für jede gestartete Datenbankdatei können Sie Datenbankoptionen eingeben, die bestimmte Verhaltensaspekte einer Datenbank steuern.

Datenbank- und Serveroptionen berücksichtigen im Allgemeinen die Groß- und Kleinschreibung. Sie sollten alle Optionen in Kleinbuchstaben eingeben.

*database-file* gibt den Datenbankdateinamen an. Wenn *database-file* ohne Dateierweiterung angegeben wird, sucht der Datenbankserver nach *database-file* mit der Erweiterung *.db*. Wenn Sie einen relativen Suchpfad verwenden, wird er relativ zum aktuellen Arbeitsverzeichnis gelesen. Sie können einen vollständigen Pfad angeben.

Wenn Sie weder Optionen noch eine Datenbankdatei angeben, wird unter Windows-Betriebssystemen ein Fenster angezeigt, in dem Sie mit "Durchsuchen" zur Datenbankdatei navigieren können.

Wenn Sie einen Datenbankserver aus einer Batchdatei starten möchten, müssen Sie das Dienstprogramm *dbspawn* verwenden. Siehe „Dienstprogramm für den Serverstart im Hintergrund (*dbspawn*)“ auf Seite 983.

Der Personal Datenbankserver hat maximal zehn gleichzeitige Verbindungen, verwendet maximal vier Prozessorkerne einer CPU zur Anforderungsverarbeitung und unterstützt keine Netzwerk-Client/Server-Verbindungen. Standardmäßig verwendet der Personal Datenbankserver nur das Shared Memory-Protokoll. Sie müssen die Option -x verwenden, wenn Sie TCP/IP mit dem Personal Datenbankserver nutzen möchten. Siehe „[Datenbankserveroption -x](#)“ auf Seite 305.

Zusätzlich gibt es noch andere kleinere Unterschiede, z.B. die Privilegstufe, die standardmäßig zum Starten von neuen Datenbanken erforderlich ist, oder die zum Ausführen der CHECKPOINT-Anweisung erforderlichen Privilegien. Weitere Informationen über die Unterschiede zwischen dem Personal Datenbankserver und dem Netzwerk-Datenbankserver finden Sie unter „[SQL Anywhere-Datenbankserver](#)“ auf Seite 150.

Standardmäßig wird die Datenbankserver-Seitengröße in der Befehlszeile auf die größte Seitengröße der Datenbank gesetzt. Wenn ein Datenbankserver gestartet wurde, können Sie keine Datenbank starten, die eine größere Seitengröße hat als der Datenbankserver. Siehe „[Hinweise zur maximalen Seitengröße](#)“ auf Seite 160.

### Beispiel

Der folgende Befehl startet die SQL Anywhere-Beispieldatenbank auf einem Personal Datenbankserver:

```
dbeng16 "%SQLANYAMP16%\demo.db"
```

Der folgende Befehl startet die SQL Anywhere-Beispieldatenbank auf einem Netzwerk-Datenbankserver:

```
dbsrv16 "%SQLANYAMP16%\demo.db"
```

Mit dem folgenden Beispiel (in einer Zeile eingegeben) wird ein Datenbankserver mit dem Namen **myserver** mit einer Cachegröße von 3 MByte gestartet und die Beispieldatenbank geladen:

```
dbsrv16 -c 3m -n myservers "%SQLANYAMP16%\demo.db"
```

### Siehe auch

- [Nachfolgend finden Sie Beispiele zum Starten eines Datenbankservers auf Seite 153](#)

## Datenbankserveroptionen

Diese Parameter gelten für den Datenbankserver insgesamt, und nicht nur für eine bestimmte Datenbank.

### @data -Datenbankserveroption

Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein.

#### Syntax

```
dbsrv16 @data ...
```

#### Gilt für

Alle Betriebssysteme und Datenbankserver, ausgenommen Windows Mobile. Wird unterstützt für alle Datenbank-Dienstprogramme, mit Ausnahme des Dienstprogramms für die Sprachauswahl (dblang), des

Dienstprogramms zur Zertifikatserstellung (createcert), des Dienstprogramms zum Anzeigen von Zertifikaten (viewcert), des Dienstprogramms für die Installation des Microsoft ActiveSync-Providers (mlasinst) und des Dienstprogramms zum Verschleiern von Dateien (dbfhide).

- Dienstprogramm für die Sprachauswahl (dblang)
- Dienstprogramm für die Zertifikatserstellung (createcert)
- Dienstprogramm zum Anzeigen von Zertifikaten (viewcert)
- Dienstprogramm zur Installation des Microsoft ActiveSync-Providers (mlasinst)
- Dienstprogramm zum Verschleiern von Dateien (dbfhide)

### Bemerkungen

Verwenden Sie diese Option, um Befehlszeilenoptionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei zu lesen. Wenn beide mit demselben Namen vorhanden sind, wird die Umgebungsvariable verwendet.

Die Konfigurationsdatei kann Zeilenumbrüche und eine beliebige Menge von Befehlszeilenoptionen enthalten.

Wenn Sie die Informationen in einer Konfigurationsdatei schützen möchten (weil sie beispielsweise Kennwörter enthält), können Sie das Dienstprogramm zum Verschleiern von Dateien (dbfhide) zum Verschleiern des Inhalts von Konfigurationsdateien verwenden.

Der @data-Parameter kann überall im Befehl angegeben werden und Parameter aus der Datei werden an der betreffenden Stelle eingefügt. Mehrere Dateien können angegeben werden, und der Dateibezeichner kann mit Befehlszeilenoptionen verwendet werden.

### Siehe auch

- [„Konfigurationsdateien“ auf Seite 882](#)
- [„Dienstprogramm zum Verschleiern von Dateien \(dbfhide\)“ auf Seite 922](#)

### Beispiel

Die folgende Konfigurationsdatei enthält zum Beispiel eine Gruppe von Optionen für einen Server namens **myserver**, der mit einer Cachegröße von 4 MB startet und die Beispieldatenbank lädt:

```
-c 4096
-n myserver
"c:\mydatabase.db"
```

Wenn diese Konfigurationsdatei als `c:\config.txt` gespeichert wird, kann sie folgendermaßen in einem Befehl verwendet werden:

```
dbsrv16 @c:\config.txt
```

Die folgende Konfigurationsdatei enthält Kommentare:

```
#This is the server name:
-n MyServer
#These are the protocols:
-x tcpip
#This is the database file
my.db
```

Die folgende Anweisung setzt eine Umgebungsvariable, die Parameter für einen Datenbankserver enthält, der mit einer Cachegröße von 4 MB startet und die Beispieldatenbank lädt.

```
SET envvar=-c 4096 "c:\mydatabase.db";
```

Der folgende Befehl startet den Datenbankserver mit der Umgebungsvariablen **envvar**.

```
dbsrv16 @envvar
```

## -? - Datenbankserveroption

Zeigt Syntaxinformationen an

### Syntax

```
dbsrv16 -?
```

### Gilt für

Alle Betriebssysteme und Datenbankserver, ausgenommen Windows Mobile.

### Bemerkungen

Wenn Sie diese Option angeben, wird eine kurze Beschreibung aller Serveroptionen angezeigt.

## Datenbankserveroption -al

Lässt die Standard-Benutzerauthentifizierung für angegebene Benutzer zu.

### Syntax

```
dbsrv16 -al userid[ ;userid ... ] ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Lässt zu, dass die in der durch Semikola getrennten Liste von Benutzer-IDs angegebenen Benutzer die Standard-Authentifizierung verwenden. Es können höchstens 5 Benutzer-IDs angegeben werden.

Diese Option ist nützlich, wenn die login\_mode-Option keine Standard-Authentifizierung umfasst und der Benutzer keine Möglichkeit hat, sich mit anderen Methoden zu authentifizieren. Benutzer mit vollen DBA-Privilegien können immer die Standard-Authentifizierung verwenden.

### Siehe auch

- „login\_mode-Option“ auf Seite 623

## Datenbankserveroption -b

Verwendet den Massenvorgangsmodus

**Syntax**

**dbsrv16 -b ...**

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Diese Option ist sinnvoll, wenn Sie die SQL INPUT-Anweisung von Interactive SQL verwenden, um große Datenmengen in eine Datenbank zu laden.

Die Option -b darf nicht verwendet werden, wenn Sie große Datenmengen mit LOAD TABLE laden.

Wenn Sie diese Option verwenden, lässt der Datenbankserver nur eine Verbindung pro Anwendung zu. Ein Rollback-Log wird geführt, nicht aber ein Transaktionslog. Der Sperrmechanismus für mehrere Benutzer wird deaktiviert.

Wenn Sie den Datenbankserver zum ersten Mal nach dem Laden von Daten mit der Option -b starten, sollten Sie eine neue Transaktionslogdatei verwenden.

Der Massenvorgangsmodus deaktiviert nicht das Auslösen von Triggern.

**Siehe auch**

- „INPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Die Datenwiederherstellung bei Massenvorgängen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Performance-Aspekte von Massenvorgängen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankserveroption -c

Legt den Umfang des Speichers fest, der zu Beginn für die Speicherung der Datenbankseiten und anderer Datenbankserver-Informationen im Cache reserviert wird.

**Syntax**

**dbsrv16 -c { size[ **k** | **m** | **g** | **p** ] } ...**

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Der Speicherplatz, der für den Cache des Datenbankservers verwendet wird, ist einer der Schlüsselfaktoren für die Steuerung der Performance. Die Anfangsgröße des Cachespeichers können Sie mit der Serveroption -c festlegen. Je mehr Cachespeicher dem Datenbankserver gegeben werden kann, desto besser ist seine Performance.

*size* ist die Speichergröße in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit kB, MB bzw. GB anzugeben.

Die Einheit **p** ist ein Prozentsatz des gesamten physischen Systemspeichers oder der maximalen unterstützten Cachegröße, je nachdem, welcher Wert niedriger ist. Die maximale unterstützte Cachegröße hängt vom Betriebssystem ab. Zum Beispiel:

- 2,5 GB für die 32-Bit-Versionen von Windows Advanced Server, Enterprise Server, Datacenter Server und Vista.
- 3,5 GB für den 32-Bit-Datenbankserver, der unter Windows x64 Edition läuft.
- 1,5 GB auf allen anderen 32-Bit-Windows-Systemen
- Unter Windows Mobile wird die Cachegröße durch den verfügbaren physischen Speicher eingeschränkt.
- Auf 64-Bit-Datenbankservern kann die Cachegröße als unbegrenzt betrachtet werden

Wenn Sie **p** verwenden, ist das Argument ein Prozentsatz. Sie können % als Alternative zu **p** verwenden. Allerdings verwenden Windows-Betriebssysteme das Prozentzeichen als ein Umgebungsvariable-Escapezeichen, also müssen Sie in diesem Fall das Prozentzeichen mit Escapezeichen versehen. Führen Sie beispielsweise den folgenden Befehl aus, um die anfängliche Cachegröße auf 50 Prozent des physischen Systemspeichers festzulegen:

```
dbsrv16 -c 50%% ...
```

Wenn die Option -c nicht angegeben wird, berechnet der Datenbankserver die anfängliche Cachezuweisung folgendermaßen:

- **Windows Mobile** Die Formel lautet folgendermaßen:

```
max( 600 KB, min( dbsize, 0.25*TotalPhysicalMemory ) );
```

*dbsize* ist die Gesamtgröße der gestarteten Datenbankdatei(en) und *TotalPhysicalMemory* der gesamte physische Speicher auf dem Computer.

- **Windows** Die Formel lautet folgendermaßen:

```
max( 2 MB, min( dbsize, 0.25*TotalPhysicalMemory ) );
```

*dbsize* ist die Gesamtgröße der gestarteten Datenbankdatei(en) und *TotalPhysicalMemory* der gesamte physische Speicher auf dem Computer.

- **Unix** Mindestes 8 MB.

```
max( 8 MB, min( 0.1*( physical-memory + available-swap ) , database-size*1.1 )
```

Informationen zur anfänglichen Cachegröße unter Unix finden Sie unter „[Dynamische Cachedimensionierung unter Unix](#)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].

### Hinweis

Wenn Sie versuchen, Ihre anfängliche oder minimale Cachegröße auf einen Wert, der kleiner ist als ein Achtel der maximalen Cachegröße zu setzen, werden die anfängliche bzw. die minimale Cachegröße automatisch relativ zur maximalen Cachegröße erhöht.

Wenn Sie dynamische Cachedimensionierung deaktivieren (Option -ca), wird die verwendete Cachegröße möglicherweise durch die Menge an verfügbarem Speicher begrenzt. Siehe „[Tipp: Performance durch den Einsatz des Cachespeichers steigern](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

Im Meldungsfenster des Datenbankservers wird die Größe des Caches beim Start angezeigt und Sie können die folgende Anweisung benutzen, um die aktuelle Größe des Caches abzurufen:

```
SELECT PROPERTY( 'CurrentCacheSize' );
```

### Siehe auch

- [Cachegröße auf Seite 167](#)
- „Dynamische Cachedimensionierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -ca“ auf Seite 219
- „Datenbankserveroption -cc“ auf Seite 220
- „Datenbankserveroption -ch“ auf Seite 221
- „Datenbankserveroption -chx“ auf Seite 222
- „Datenbankserveroption -cl“ auf Seite 224
- „Datenbankserveroption -cr“ auf Seite 226
- „Datenbankserveroption -cs“ auf Seite 227
- „Datenbankserveroption -cv“ auf Seite 227
- „[Tipp: Performance durch den Einsatz des Cachespeichers steigern](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

### Beispiel

Im folgenden Beispiel wird ein Datenbankserver mit dem Namen **myserver** und einer Cachegröße von 3 MB gestartet und die Beispieldatenbank geladen:

```
dbsrv16 -c 3m -n myserver "%SQLANYAMP16%\demo.db"
```

## Datenbankserveroption -ca

Erzwingt eine statische Cachegröße.

### Syntax

```
dbsrv16 -ca 0 ...
```

### Gilt für

Windows, Unix, Mac OS X

### Bemerkungen

Sie können die automatische Cachegrößenoptimierung deaktivieren, indem Sie in der Befehlszeile "-ca 0" eingeben. Wenn Sie die Option -ca 0 nicht verwenden, erhöht der Datenbankserver automatisch die Cachegröße. Wenn Sie diese Option angeben, wird die Cachegröße dennoch angepasst, wenn beim Datenbankserver ansonsten ein Fehler mit der Meldung, dass der dynamische Speicher ausgelastet ist, auftreten würde.

Diese Serveroption darf nur in der Form "-ca 0" verwendet werden.

### Siehe auch

- Cachegröße auf Seite 167
- „Dynamische Cachingdimensionierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -c “ auf Seite 217
- „Datenbankserveroption -cc “ auf Seite 220
- „Datenbankserveroption -ch “ auf Seite 221
- „Datenbankserveroption -chx “ auf Seite 222
- „Datenbankserveroption -cl “ auf Seite 224
- „Datenbankserveroption -cr “ auf Seite 226
- „Datenbankserveroption -cs “ auf Seite 227
- „Datenbankserveroption -cv “ auf Seite 227

### Beispiel

Das folgende Beispiel startet einen Datenbankserver mit dem Namen myserver mit einem statischen Cache von 40 % des gesamten physischen Speichers und lädt die Beispieldatenbank, wobei der Datenbankserver Cachegröße nicht automatisch anpasst:

```
dbsrv16 -c 40P -ca 0 -n myserver "%SQLANYAMP16%\demo.db"
```

## Datenbankserveroption -cc

Sammelt Informationen über Datenbankseiten, die zur Cache-Vorwärmung eingesetzt werden sollen, wenn die Datenbank erneut gestartet wird

### Syntax

```
dbsrv16 -cc{ + | - } ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Standardmäßig ist die Seitensammlung aktiviert. Wenn die Sammlung aktiviert ist, verfolgt der Datenbankserver jede einzelne angeforderte Datenbankseite. Die Sammlung wird gestoppt, wenn die Höchstzahl der Seiten gesammelt wurde, die Datenbank heruntergefahren wird oder die Sammlungsrate unter den Mindestwert fällt. Sie können weder die Höchstzahl der gesammelten Seiten konfigurieren noch den Wert für die Sammlungsrate angeben (dieser Wert basiert auf Cachegröße und Datenbankgröße). Wenn die Sammlung abgeschlossen ist, werden die Informationen über die angeforderten Seiten in der Datenbank aufgezeichnet, sodass die betreffenden Seiten verwendet werden können, um den Cache beim nächsten Datenbankstart mit der Option -cr zur Cache-Vorwärmung verwenden zu können. Die Sammlung referenzierter Seiten ist standardmäßig aktiviert.

**Siehe auch**

- „Datenbankserveroption -c “ auf Seite 217
- „Datenbankserveroption -ca “ auf Seite 219
- „Datenbankserveroption -ch “ auf Seite 221
- „Datenbankserveroption -chx “ auf Seite 222
- „Datenbankserveroption -cl “ auf Seite 224
- „Datenbankserveroption -cr “ auf Seite 226
- „Datenbankserveroption -cs “ auf Seite 227
- „Datenbankserveroption -cv “ auf Seite 227
- „Cachevorwärmung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -ch

Setzt eine maximale Cachegröße als Grenzwert für die automatische Cachevergrößerung.

**Syntax**

```
dbsrv16 -ch { size[ k | m | g | p ] } ...
```

**Gilt für**

Windows, Unix, Mac OS X

**Bemerkungen**

Diese Option beschränkt die Größe des Datenbankserver-Caches während der automatischen Cachevergrößerung. Standardmäßig entspricht die Obergrenze ungefähr dem niedrigeren Wert aus der maximalen Cachegröße und 90 % des gesamten physischen Speichers auf dem Computer.

*size* ist die Speichergröße in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit kB, MB bzw. GB anzugeben.

Die Einheit **p** ist ein Prozentsatz des physischen Systemspeichers oder der maximalen unterstützten Cachegröße, je nachdem, welcher Wert niedriger ist. Die maximale unterstützte Cachegröße hängt vom Betriebssystem ab. Zum Beispiel:

- 2,5 GB für Windows Advanced Server, Enterprise Server und Datacenter Server (32-Bit-Version)
- 3,5 GB für den 32-Bit-Datenbankserver, der unter Windows x64 Edition läuft.
- 1,5 GB auf allen anderen 32-Bit-Windows-Systemen
- Auf 64-Bit-Datenbankservern kann die Cachegröße als unbegrenzt betrachtet werden
- Unter Windows Mobile wird die Cachegröße durch den verfügbaren physischen Speicher eingeschränkt.

Wenn Sie **p** verwenden, ist das Argument ein Prozentsatz. Sie können "%" als Alternative zu **p** verwenden, jedoch nicht unter Windows-Betriebssystemen, es sei denn, Sie fügen entsprechende Escape-Zeichen hinzu. Führen Sie den folgenden Befehl aus, um die anfängliche Cachegröße auf 50 Prozent des physischen Systemspeichers festzulegen:

```
dbsrv16 -ch 50%% ...
```

Wenn Sie mit -ch eine Cachegröße von weniger als 64 MB festlegen, passt der Datenbankserver die maximale Cachegröße auf 64 MB an. Das Angeben einer maximalen Cachegröße von weniger als 64 MB wird nicht empfohlen, ist jedoch mithilfe der Option -chx möglich.

### Siehe auch

- [Cachegröße auf Seite 167](#)
- [„Dynamische Cachedimensionierung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„Datenbankserveroption -c “ auf Seite 217](#)
- [„Datenbankserveroption -ca “ auf Seite 219](#)
- [„Datenbankserveroption -cc “ auf Seite 220](#)
- [„Datenbankserveroption -chx “ auf Seite 222](#)
- [„Datenbankserveroption -cl “ auf Seite 224](#)
- [„Datenbankserveroption -cr “ auf Seite 226](#)
- [„Datenbankserveroption -cs “ auf Seite 227](#)
- [„Datenbankserveroption -cv “ auf Seite 227](#)

### Beispiel

Im folgenden Beispiel wird ein Datenbankserver mit dem Namen silver und einer maximalen Cachegröße von 64 MB gestartet und die Beispieldatenbank geladen:

```
dbsrv16 -ch 64m -n silver "%SQLANYSAMPl6%\demo.db"
```

## Datenbankserveroption -chx

Legt eine maximale Cachegröße als Grenzwert für die automatische Cachevergrößerung fest.

### Syntax

```
dbsrv16 -chx { size[ k | m | g | p ] } ...
```

### Standardwert

Mindestens 512 MByte Adressraum ist reserviert für eine Verwendung außerhalb des Caches.

### Gilt für

Windows und Unix

## Bemerkungen

### Vorsicht

Beim Einstellen einer großen Cachegröße auf 32-Bit-Servern sollten Sie die Option -chx nur verwenden, wenn Sie durch Tests sichergestellt haben, dass sich die zusätzliche Nutzung von Adressraum nicht auf andere Komponenten auswirkt, die Serveradressraum nutzen, z.B. folgende:

- DLLs, die der Server laden muss
- ODBC-Treiber für den Zugriff auf entfernte Tabellen
- Netzwerkpaket-Puffer
- Externe gespeicherte Prozeduren
- Nicht-Cache-Speicherzuordnungen

Wenn Sie einen großen Cache benötigen, sollten Sie die 64-Bit-Version des Datenbankservers unter einem 64-Bit-Betriebssystem verwenden.

Der 32-Bit-Datenbankserver passt normalerweise die Cachegröße so an, dass mindestens 512 MB Adressraum für die Nutzung außerhalb des Cache reserviert sind. Wenn Sie eine maximale Cachegröße angeben möchten, die weniger Adressraum für eine Nutzung außerhalb des Caches reserviert, verwenden Sie die Option -chx. Die Verwendung eines größeren Caches kann möglicherweise zur Instabilität des Datenbankservers führen. Diese Option muss mit Umsicht eingesetzt werden.

Die maximale unterstützte Cachegröße hängt vom Betriebssystem ab. Zum Beispiel:

- 2,5 GB für die 32-Bit-Versionen von Windows Advanced Server, Enterprise Server, Datacenter Server und Vista.
- 3,5 GB für den 32-Bit-Datenbankserver, der unter Windows x64 Edition läuft.
- 1,5 GB auf allen anderen 32-Bit-Windows-Systemen
- Unter Windows Mobile wird die Cachegröße durch den verfügbaren physischen Speicher eingeschränkt.
- Auf 64-Bit-Datenbankservern kann die Cachegröße als unbegrenzt betrachtet werden

*size* ist die Speichergröße in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit kB, MB bzw. GB anzugeben.

Die Einheit **p** ist ein Prozentsatz des physischen Systemspeichers oder der maximalen Cachegröße, je nachdem, welcher Wert niedriger ist. Sie können % als Alternative zu **p** verwenden, aber unter Windows wird das Prozentzeichen als Escapezeichen für Umgebungsvariable verwendet. Daher müssen Sie das Prozentzeichen mit Escapezeichen versehen.

Die Option -chx kann verwendet werden, um eine maximale Cachegröße von weniger als 64 MB anzugeben, aber die Verwendung einer solchen maximalen Cachegröße wird nicht empfohlen.

### Siehe auch

- [Cachegröße auf Seite 167](#)
- [„Datenbankserveroption -c “ auf Seite 217](#)
- [„Datenbankserveroption -ca “ auf Seite 219](#)
- [„Datenbankserveroption -cc “ auf Seite 220](#)
- [„Datenbankserveroption -ch “ auf Seite 221](#)
- [„Datenbankserveroption -cl “ auf Seite 224](#)
- [„Datenbankserveroption -cr “ auf Seite 226](#)
- [„Datenbankserveroption -cs “ auf Seite 227](#)
- [„Datenbankserveroption -cv “ auf Seite 227](#)
- [„Tipp: Performance durch den Einsatz des Cachespeichers steigern“ \[\*SQL Anywhere Server - SQL-Benutzerhandbuch\*\]](#)

## Datenbankserveroption -cl

Legt eine minimale Cachegröße als unteren Grenzwert für die dynamische Cachegrößenveränderung fest.

### Syntax

```
dbsrv16 -cl { size[ k | m | g | p ] } ...
```

### Standardwert

2 MByte unter Windows

8 MByte unter Unix

### Gilt für

Windows, Unix, Mac OS X

### Bemerkungen

Mit dieser Option wird ein unterer Grenzwert für den Cache festgelegt. Wenn -c angegeben und -cl nicht angegeben ist, wird die Mindestgröße für den Cache auf die anfängliche Cachegröße eingestellt (die Einstellung -c). Wenn weder -c noch -cl eingestellt sind, wird die Mindestgröße für den Cache auf einen niedrigen, konstanten Wert eingestellt, sodass der Cache bei Bedarf verringert werden kann. Auf Windows-Plattformen beträgt dieser Wert 2 MB.

*size* ist die Speichergröße in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit in kB, MB bzw. GB anzugeben.

Die Einheit **p** ist ein Prozentsatz des physischen Systemspeichers oder der maximalen unterstützten Cachegröße, je nachdem, welcher Wert niedriger ist. Die maximale unterstützte Cachegröße hängt vom Betriebssystem ab. Zum Beispiel:

- 2,5 GB für Windows Advanced Server, Enterprise Server und Datacenter Server (32-Bit-Version)
- 3,5 GB für den 32-Bit-Datenbankserver, der unter Windows x64 Edition läuft.
- 1,5 GB auf allen anderen 32-Bit-Systemen.

- Unter Windows Mobile wird die Cachegröße durch den verfügbaren physischen Speicher eingeschränkt
- Auf 64-Bit-Datenbankservern kann die Cachegröße als unbegrenzt betrachtet werden

Wenn Sie **p** verwenden, ist das Argument ein Prozentsatz. Sie können % als Alternative zu **p** verwenden, aber unter Windows wird das Prozentzeichen als ein Umgebungsvariable-Escapezeichen verwendet, daher müssen Sie das Prozentzeichen mit Escapezeichen versehen.

Führen Sie beispielsweise den folgenden Befehl aus, um die minimale Cachegröße auf 50 Prozent des physischen Systemspeichers festzulegen:

```
dbsrv16 -cl 50%% ...
```

#### Hinweis

Wenn Sie versuchen, Ihre anfängliche oder minimale Cachegröße auf einen Wert zu setzen, der kleiner ist als ein Achtel der maximalen Cachegröße, werden die anfängliche bzw. die minimale Cachegröße automatisch relativ zur unterstützten Cachegröße erhöht.

#### Siehe auch

- „Dynamische Cachedimensionierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -c “ auf Seite 217
- „Datenbankserveroption -ca “ auf Seite 219
- „Datenbankserveroption -cc “ auf Seite 220
- „Datenbankserveroption -ch “ auf Seite 221
- „Datenbankserveroption -chx “ auf Seite 222
- „Datenbankserveroption -cr “ auf Seite 226
- „Datenbankserveroption -cs “ auf Seite 227
- „Datenbankserveroption -cv “ auf Seite 227

#### Beispiel

Beim folgenden Beispiel wird ein Datenbankserver mit dem Namen "silver" und einer Mindestcachegröße von 5 MByte gestartet und die Datenbankdatei *example.db* geladen:

```
dbsrv16 -cl 5m -n silver "c:\example.db"
```

## Datenbankserveroption -cp

Gibt eine zusätzliche Reihe von Verzeichnissen oder JAR-Dateien an, in denen nach Klassen gesucht werden soll.

#### Syntax

```
dbsrv16 -cp location[ ;location ... ] ...
```

#### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Es wird empfohlen, alle Klassen- und JAR-Dateien, die mit Java in der Datenbank verwendet werden, in der Datenbank zu installieren. Wenn Sie die Klassen und JAR-Dateien in der Datenbank speichern, kann die Datenbank problemlos auf einen anderen Computer oder ein anderes Betriebssystem verschoben werden. Ein weiterer Vorteil der Installation von Klassen und JAR-Dateien in der Datenbank besteht darin, dass der Klassenlader des Datenbankservers die Klassen und Ressourcen aus der Datenbank abrufen kann, sodass jede Verbindung, die Java in der Datenbank verwendet, ihre eigene Instanz dieser Klassen und ihre eigene Kopie statischer Variablen in diesen Klassen besitzt.

Wenn jedoch eine Klasse oder eine JAR-Datei vom Systemklassenlader geladen werden muss, kann sie mit der `java_class_path`-Datenbankoption oder der Datenbankserveroption `-cp` angegeben werden. Beide Optionen fügen Klassen und JAR-Dateien dem Klassenpfad hinzu, den der Datenbankserver zum Start der Java VM aufbaut. Die `java_class_path`-Datenbankoption ist nützlich, wenn auf dem Server mehrere Datenbanken laufen und jede Datenbank eine eigene Gruppe von JAR-Dateien und Verzeichnissen hat, die vom Systemklassenlader geladen werden müssen. Die Datenbankserveroption `-cp` ist nützlich, wenn alle Datenbanken auf dem Server dieselben Klassen oder JAR-Dateien erfordern.

### Siehe auch

- „Java in der Datenbank“ [[SQL Anywhere Server - Programmierung](#)]
- „Eigene Java-Klassen in Datenbanken verwenden“ [[SQL Anywhere Server - Programmierung](#)]
- „`java_class_path`-Option“ auf Seite 620

## Datenbankserveroption `-cr`

Lädt den Cache mit Datenbankseiten erneut (vorwärmen), die gesammelt wurden, als die Datenbank zum letzten Mal ausgeführt wurde

### Syntax

`dbsrv16 -cr{ + | - } ...`

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Sie können den Datenbankserver anweisen, den Cache mit Seiten vorzuwärmen, die referenziert wurden, als die Datenbank zum letzten Mal gestartet wurde (die Sammlung von Seiten wird mit der Option `-cc` aktiviert). Cache-Vorwärmung ist standardmäßig aktiviert. Wenn eine Datenbank gestartet wird, prüft der Server, ob sie eine Sammlung von Seiten enthält, die beim letzten Start der Datenbank angefordert wurden. Wenn eine Datenbank diese Informationen enthält, werden die beim letzten Mal referenzierten Seiten in den Cache geladen.

Den Cache mit Seiten vorzuwärmen, die beim letzten Start der Datenbank referenziert wurden, kann die Performance verbessern, wenn dieselben oder ähnliche Abfragen bei jedem Start einer Datenbank ausgeführt werden.

**Siehe auch**

- „Datenbankserveroption -cc “ auf Seite 220
- „Datenbankserveroption -cl “ auf Seite 224
- „Datenbankserveroption -cs “ auf Seite 227
- „Datenbankserveroption -cv “ auf Seite 227
- „Cachevorwärmung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankserveroption -cs

Zeigt die Statistik zur dynamischen Cachedimensionierung im Meldungsfenster des Datenbankservers an.

**Syntax**

**dbsrv16 -cs ...**

**Gilt für**

Windows, Unix

**Bemerkungen**

Zum Zweck der Fehlerbehandlung zeigt diese Option Statistiken im Meldungsfenster des Datenbankservers, die der Datenbankserver verwendet, um zu ermitteln, wie die Größe des Caches optimiert werden soll.

**Siehe auch**

- CacheSizingStatistics-Servereigenschaft auf Seite 747
- „Datenbankserveroption -c “ auf Seite 217
- „Datenbankserveroption -ca “ auf Seite 219
- „Datenbankserveroption -cc “ auf Seite 220
- „Datenbankserveroption -ch “ auf Seite 221
- „Datenbankserveroption -chx “ auf Seite 222
- „Datenbankserveroption -cl “ auf Seite 224
- „Datenbankserveroption -cr “ auf Seite 226
- „Datenbankserveroption -cv “ auf Seite 227
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Cachevorwärmung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankserveroption -cv

Steuert die Anzeige von Meldungen zur Cache-Vorwärmung im Meldungsfenster des Datenbankservers.

**Syntax**

**dbsrv16 -cv{ + | - } ...**

**Standardwert**

Die Meldungen zur Cache-Vorwärmung werden unterdrückt.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn "-cv+" angegeben wurde, erscheint bei den folgenden Aktivitäten zur Cache-Vorwärmung eine Meldung im Meldungsfenster des Datenbankservers:

- Die Sammlung der angeforderten Seiten wird gestartet oder gestoppt (gesteuert über die Serveroption -cc)
- Das erneute Laden von Seiten wird gestartet oder gestoppt (gesteuert über die Serveroption -cr)

### Siehe auch

- „Datenbankserveroption -c “ auf Seite 217
- „Datenbankserveroption -ca “ auf Seite 219
- „Datenbankserveroption -cc “ auf Seite 220
- „Datenbankserveroption -ch “ auf Seite 221
- „Datenbankserveroption -cl “ auf Seite 224
- „Datenbankserveroption -cr “ auf Seite 226
- „Datenbankserveroption -cs “ auf Seite 227
- „Cachevorwärmung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

### Beispiel

Mit dem folgenden Befehl wird die Datenbank *mydatabase.db* gestartet, das Sammeln von Datenbankseiten sowie das Laden der Seiten wird aktiviert, die Meldungen zu diesen Aktivitäten werden im Meldungsfenster des Datenbankservers angezeigt:

```
dbsrv16 -cc+ -cr+ -cv+ mydatabase.db
```

## Datenbankserveroption -dt

Gibt das Verzeichnis an, in dem temporäre Dateien gespeichert werden

### Syntax

```
dbsrv16 -dt temp-file-dir ...
```

### Gilt für

Alle Server und Betriebssysteme, außer Verbindungen über gemeinsam genutzten Speicher unter Unix

### Bemerkungen

Der Datenbankserver erstellt zwei Arten von temporären Dateien:

- **Dem Datenbankserver zugeordnete temporäre Dateien (auf allen Plattformen erstellt)** Sie können mit der Option -dt ein Verzeichnis für temporäre Dateien des Datenbankservers festlegen. Wenn Sie diese Option beim Start des Datenbankservers nicht angeben, überprüft der Datenbankserver die folgenden Umgebungsvariablen in der angegebenen Reihenfolge, um zu bestimmen, in welchem Verzeichnis die temporäre Datei abgelegt wird.

Windows/Unix
1. SATMP
2. TMP
3. TMPDIR
4. TEMP

Wenn keine der Umgebungsvariablen festgelegt ist, speichert der Datenbankserver seine temporäre Datei unter Windows im aktuellen Verzeichnis und unter Unix im Verzeichnis */tmp*.

Unter Windows Mobile wird der Registrierungsschlüsseleintrag *TempFolder* verwendet, um das Verzeichnis für temporäre Dateien zu bestimmen. Ist er nicht definiert, wird *\Temp* verwendet. Falls das Verzeichnis nicht existiert und nicht erstellt werden kann, wird das aktuelle Verzeichnis verwendet.

- **Der Kommunikation zugeordnete temporäre Dateien (erstellt nur unter Unix für den Client und den Datenbankserver)** Temporäre Dateien für Verbindungen unter Unix werden nicht im durch *-dt* angegebenen Verzeichnis abgelegt. Stattdessen überprüft der Datenbankserver die folgenden Umgebungsvariablen in der angegebenen Reihenfolge, um zu bestimmen, in welchem Verzeichnis die temporäre Datei abgelegt wird:

Unix
1. SATMP
2. TMP
3. TMPDIR
4. TEMP

Wenn keine der Umgebungsvariablen festgelegt ist, speichert der Datenbankserver seine temporäre Datei unter Unix im Verzeichnis */tmp*.

Unter Unix müssen der Client und der Datenbankserver SATMP auf denselben Wert setzen, wenn sie sich über Shared Memory verbinden.

### Siehe auch

- „Registrierungseinstellungen unter Windows Mobile“ auf Seite 491
- „Datenbankdateitypen“ auf Seite 119
- „SATMP-Umgebungsvariable“ auf Seite 475
- „Tipp: Verschiedene Dateien auf verschiedene Geräte platzieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „sa\_disk\_free\_space-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „temp\_space\_limit\_check-Option“ auf Seite 689
- „Sicherstellen von genügend Festplattenspeicher für die temporäre Datei“ auf Seite 1110

### Beispiel

Um festzustellen, wo sich die dem Datenbankserver zugeordneten temporären Dateien befinden, verwenden Sie die DB\_PROPERTY-Systemfunktion mit der TempFileName-Eigenschaft:

```
SELECT DB_PROPERTY ( 'TempFileName' );
```

## Datenbankserveroption -ec

Verwendet Transportschichtssicherheit oder einfache Verschlüsselung zum Verschlüsseln aller Kommunikationsprotokollpakete für die Befehlssequenz (z.B. DBLib und ODBC), die zu und von allen Clients übertragen werden. TDS-Pakete werden nicht verschlüsselt.

### Syntax

```
dbsrv16 -ec encryption-options ...
```

*encryption-options* :

```
{ NONE |  
  SIMPLE |  
  TLS ( [ FIPS={ Y | N }; ]  
    IDENTITY=server-identity-filename;  
    IDENTITY_PASSWORD=password ) }, ...
```

### Zulässige Werte

- **NONE** Hierbei werden nicht verschlüsselte Verbindungen angenommen.
- **SIMPLE** Hierbei werden Verbindungen angenommen, die gemäß der einfachen Verschlüsselung chiffriert wurden. Dieser Verschlüsselungstyp wird auf allen Plattformen sowie von früheren Versionen des Datenbankservers und der Clients unterstützt. Die einfache Verschlüsselung bietet weder Serverauthentifizierung noch RSA-Verschlüsselung oder andere Funktionen der Transportschichtssicherheit.
- **TLS** Hierbei werden Verbindungen angenommen, die gemäß der RSA-Verschlüsselung chiffriert wurden. Der TLS-Parameter akzeptiert die folgenden Argumente:
  - **FIPS** Geben Sie bei FIPS-zertifizierter RSA-Verschlüsselung **FIPS=Y** an. RSA FIPS-zertifizierte Verschlüsselung verwendet eine separate zertifizierte Bibliothek, ist aber auch kompatibel mit Clients der Version 9.0.2 oder höher, die RSA angeben.

Eine Liste der FIPS-zertifizierten Komponenten finden Sie unter <http://www.sybase.com/detail?id=1061806>.

Der Algorithmus muss mit der beim Erstellen Ihrer Zertifikate verwendeten Verschlüsselung übereinstimmen.

- **Serveridentitätsdateiname** Geben Sie den Pfad und den Dateinamen des Serveridentitätszertifikats ein. Wenn Sie FIPS-zertifizierte RSA-Verschlüsselung verwenden, müssen Sie Ihre Zertifikate mit dem RSA-Algorithmus generieren.
- **Kennwort** Hierbei handelt es sich um das Kennwort für den privaten Schlüssel des Servers. Sie geben dieses Kennwort beim Erstellen des Serverzertifikats an.

### Gilt für

NONE und SIMPLE gelten für alle Server und Betriebssysteme.

TLS gilt für alle Server und Betriebssysteme, ausgenommen Windows Mobile.

Weitere Informationen zur Unterstützung für FIPS-zertifizierte Verschlüsselung finden Sie unter <http://www.sybase.com/detail?id=1061806>.

### Bemerkungen

Sie können diese Option verwenden, um sichere Kommunikationspakete zwischen Clientanwendungen und dem Datenbankserver mithilfe von Transportschichtssicherheit zu erhalten.

Der Parameter `-ec` weist den Datenbankserver an, Verbindungen nur zu akzeptieren, die mit einer der angegebenen Chiffriermethoden verschlüsselt wurden. Sie müssen mindestens einen der unterstützten Parameter in einer durch Kommas getrennten Liste angeben. Verbindungen über das TDS-Protokoll, wie etwa Java-Anwendungen, die jConnect verwenden, werden immer zugelassen und nie verschlüsselt, unabhängig von der Verwendung der Option `-ec`. Das Einstellen des TDS-Protokolloption auf NO verbietet solche unverschlüsselten TDS-Verbindungen.

Standardmäßig werden Kommunikationspakete nicht verschlüsselt und stellen so ein Sicherheitsrisiko dar. Wenn die Sicherheit der Netzwerkpakete von Bedeutung ist, verwenden Sie den Parameter `-ec`. Verschlüsselung beeinträchtigt die Performance nur geringfügig.

Wenn der Datenbankserver einfache Verschlüsselung akzeptiert, aber keine unverschlüsselten Verbindungen annimmt, verwendet jede Nicht-TDS-Verbindung, die versucht, keine Verschlüsselung anzuwenden, automatisch einfache Verschlüsselung.

Ein Starten des Datenbankservers mit `-ec SIMPLE` teilt dem Datenbankserver mit, nur Verbindungen zu akzeptieren, die einfache Verschlüsselung verwenden. TLS-Verbindungen (RSA- und RSA FIPS-zertifizierte Verschlüsselung) schlagen fehl und Verbindungen, die keine Verschlüsselung anfordern, verwenden einfache Verschlüsselung.

Wenn der Datenbankserver verschlüsselte Verbindungen über TCP/IP akzeptieren soll, Sie aber auch Shared Memory-Verbindungen mit der Datenbank auf dem lokalen Computer zulassen möchten, können Sie beim Starten des Datenbankservers die Option `-es` mit der Option `-ec` angeben.

Die Datei *dbrsa16.dll* enthält den RSA-Code, der für Ver- und Entschlüsselung verwendet wird. Die Datei *dbfips16.dll* enthält den Code für den FIPS-zertifizierten RSA-Algorithmus. Wenn Sie eine Verbindung zum Datenbankserver herstellen und die passende Datei unauffindbar bzw. ein Fehler aufgetreten ist, wird im Meldungsfenster des Datenbankservers eine Meldung angezeigt. Der Server startet nicht, wenn die angegebenen Verschlüsselungstypen nicht initialisiert werden können.

Wenn die Verschlüsselungseinstellungen von Client und Server nicht übereinstimmen, schlägt die Verbindung fehl, außer in folgenden Fällen:

- Wenn auf dem Datenbankserver "-ec SIMPLE" angegeben ist, aber nicht "-ec NONE", können Verbindungen, die keine Verschlüsselung anfordern, hergestellt werden, wobei automatisch einfache Verschlüsselung verwendet wird.
- Wenn der Datenbankserver RSA-zertifizierte Verschlüsselung angibt und der Client FIPS-zertifizierte Verschlüsselung (bzw. umgekehrt), kommt die Verbindung erfolgreich zustande. In solchen Fällen gibt die Encryption-Verbindungseigenschaft den vom Datenbankserver angegebenen Wert zurück.

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [*SQL Anywhere 16 - Einführung*].

### Siehe auch

- „Transportschichtsicherheit“ auf Seite 1444
- „TDS-Protokolloption (nur serverseitig)“ auf Seite 419
- „Datenbankserver mit Transportschichtsicherheit“ auf Seite 1454
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „Datenbankoption -ek “ auf Seite 326
- „Datenbankserveroption -ep “ auf Seite 233
- „Datenbankserveroption -es “ auf Seite 234
- „Verbindungsparameter DatabaseKey (DBKEY)“ auf Seite 353
- „FIPS-Protokolloption“ auf Seite 404
- „Datenbankserveroption -fips “ auf Seite 237
- „Digitale Zertifikate“ auf Seite 1447

### Beispiel

Das folgende Beispiel gibt an, dass Verbindungen ohne Verschlüsselung bzw. mit einfacher Verschlüsselung zulässig sind.

```
dbsrv16 -ec NONE,SIMPLE -x tcpip c:\mydemo.db
```

Das folgende Beispiel startet einen Datenbankserver, der das RSA-Serverzertifikat *rsaserver.id* verwendet.

```
dbsrv16 -ec TLS(IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test) -x tcpip c:\mydemo.db
```

Das folgende Beispiel startet einen Datenbankserver, der das FIPS-genehmigte RSA-Serverzertifikat *rsaserver.id* verwendet.

```
dbsrv16 -ec TLS(FIPS=Y;IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test) -x  
tcpip c:\mydemo.db
```

## Datenbankserveroption -ep

Fordert den Benutzer beim Starten einer stark verschlüsselten Datenbank zur Eingabe des Chiffrierschlüssels auf

### Syntax

**dbsrv16 -ep ...**

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die Option -ep weist den Datenbankserver an, den Benutzer bei Datenbanken, die in der Befehlszeile gestartet werden und einen Chiffrierschlüssel erfordern, in einem Fenster zur Eingabe des Chiffrierschlüssels aufzufordern. Dieser Serverparameter liefert eine zusätzliche Sicherheitsmaßnahme, die verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird.

Bei Verwendung für den Datenbankserver wird der Benutzer zur Eingabe des Chiffrierschlüssels aufgefordert, wenn alle folgenden Bedingungen erfüllt sind:

- Die Option -ep wurde angegeben.
- Der Server ist ein Windows Personal Server oder der Server wird gerade gestartet.
- Zum Starten der Datenbank ist ein Schlüssel erforderlich.
- Der Datenbankserver ist entweder kein Windows-Dienst oder es handelt sich um einen Windows-Dienst, für den die Option "Interaktive Beziehung mit Desktop erlauben" aktiviert wurde.
- Der Server ist kein Daemon (Unix).

Um Kommunikationspakete zwischen Clientanwendungen und dem Datenbankserver zu sichern, verwenden Sie die Serveroption -ec und Transportschichtssicherheit.

### Siehe auch

- „Transportschichtssicherheit“ auf Seite 1444
- „Datenbankserver mit Transportschichtssicherheit“ auf Seite 1454
- „Datenbankserveroption -ec “ auf Seite 230
- „Datenbankoption -ek “ auf Seite 326
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „Verbindungsparameter DatabaseKey (DBKEY)“ auf Seite 353

### Beispiel

Der Benutzer wird zur Eingabe des Chiffrierschlüssels aufgefordert, wenn die *myencrypted.db*-Datenbank gestartet wird:

```
dbsrv16 -ep -x tcpip myencrypted.db
```

## Datenbankserveroption -es

Ermöglicht unverschlüsselte Verbindungen über gemeinsam genutzten Speicher.

### Syntax

```
dbsrv16 -ec encryption-options -es ...
```

### Gilt für

Alle Server und Betriebssysteme, ausgenommen Windows Mobile.

### Bemerkungen

Diese Option ist nur wirksam, wenn sie mit der Option -ec angegeben wird. Die Option -es weist den Datenbankserver an, nicht verschlüsselte Datenbankverbindungen über gemeinsam genutzten Speicher zuzulassen. Verbindungen über TCP/IP müssen einen Verschlüsselungstyp verwenden, der durch die Option -ec festgelegt wird. Diese Option ist dann sinnvoll, wenn entfernte Clients verschlüsselte Verbindungen verwenden sollen, aus Performancegründen aber auch ein lokaler Zugang zur Datenbank über eine unverschlüsselte Verbindung möglich sein soll.

### Siehe auch

- „Datenbankserveroption -ec“ auf Seite 230
- „Datenbankserver mit Transportschichtssicherheit“ auf Seite 1454

### Beispiel

Im folgenden Beispiel wird festgelegt, dass Verbindungen mit einfacher Verschlüsselung und unverschlüsselte Verbindungen über Shared Memory zugelassen sind.

```
dbsrv16 -ec SIMPLE -es -x tcpip c:\mydemo.db
```

## Datenbankserver-Wiederherstellungsoption -f

Erzwingt einen Start des Datenbankservers, nachdem das Transaktionslog verloren gegangen ist

### Syntax

```
dbsrv16 -f ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

### Vorsicht

Diese Option wird nur bei Wiederherstellungsvorgängen eingesetzt.

Wenn es kein Transaktionslog gibt, führt der Datenbankserver eine Checkpoint-Wiederherstellung durch und fährt herunter. Sie können nun den Datenbankserver ohne die Option -f für den normalen Betrieb erneut starten.

Wenn es ein Transaktionslog im gleichen Verzeichnis wie die Datenbank gibt, führt der Datenbankserver eine Checkpoint-Wiederherstellung und eine Wiederherstellung mit dem Transaktionslog durch und fährt herunter. Sie können nun den Datenbankserver ohne die Option -f für den normalen Betrieb erneut starten.

Wenn Sie beim Starten des Servers eine Cachegröße angeben, kann sich die Wiederherstellungszeit verkürzen.

## Siehe auch

- „Spezielle Betriebsmodi“ auf Seite 170
- „Sicherung und Datenwiederherstellung“ auf Seite 1027

## Beispiel

Der folgende Befehl zwingt den Datenbankserver, eine Wiederherstellung der *mydatabase.db*-Datenbank zu starten und durchzuführen:

```
dbsrv16 mydatabase.db -f
```

## Datenbankserveroption -fc

Gibt den Dateinamen einer DLL (oder eines Shared Object unter Unix) an, die die Callback-Funktion für ein volles Dateisystem (File System Full) enthält

## Syntax

```
dbsrv16 -fc filename ...
```

## Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Diese Option kann dazu verwendet werden, um Benutzer zu benachrichtigen und gegebenenfalls Gegenmaßnahmen zu ergreifen, wenn im Dateisystem Platzmangel droht. Wenn Sie die Option -fc verwenden, versucht der Datenbankserver, die angegebene DLL zu laden und den Eintrittspunkt der Callback-Funktion während des Startens zu finden. Wenn der Datenbankserver weder die DLL noch den Eintrittspunkt finden kann, gibt der Datenbankserver einen Fehler zurück und fährt herunter. Die DLL wird vom Benutzer übergeben und kann Callbacks unter Anderem dazu verwenden, um eine von Ihnen angegebene Anweisungsfolgedatei (oder ein Shell-Skript unter Unix) für Diagnose- bzw.

Fehlerbehebungsmaßnahmen aufzurufen. Alternativ dazu kann die Callback-Funktion selbst so eine Maßnahme durchführen.

Ein Beispiel für eine Callback-Funktion bei voller Festplatte befindet sich unter `%SQLANYSAMPI6%\SQLAnywhere\DiskFull`.

Der Datenbankserver sucht an denselben Speicherorten nach der DLL für die Callback-Funktion, an denen er auch nach anderen DLLs und Dateien sucht.

Wenn der Datenbankserver Speichermangel im Dateisystem ermittelt, ruft er die Callback-Funktion auf (falls eine angegeben wurde), indem er folgende Informationen übergibt:

- Name des DBSpace, in dem der Speichermangel erkannt wurde
- Betriebssystemspezifischer Fehlercode von dem fehlgeschlagenen Vorgang

Der Rückgabecode vom Aufruf an `xp_out_of_disk` zeigt an, ob der Vorgang, der die Bedingung bewirkte, abgebrochen oder erneut versucht werden soll. Wenn ein Wert ungleich NULL zurückgegeben wird, bricht der Vorgang ab, andernfalls wird er erneut versucht. Die Callback-Funktion wird immer wieder aufgerufen, solange sie null zurückgibt und der Dateisystem-Vorgang fehlschlägt.

Auf Microsoft Windows-Plattformen wird, wenn der Datenbankserver mit einem Meldungsfenster des Datenbankservers gestartet (weder `-qi` noch `-qw` angegeben) und keine Callback-DLL zur Verfügung gestellt wurde, ein Fenster angezeigt, wenn die Festplatte zu voll wird. Dieses Fenster enthält den DBSpace-Namens- und Fehlercode. Der Benutzer kann nun entscheiden, ob der Vorgang, der den Speichermangel auf der Festplatte bewirkt, erneut versucht oder abgebrochen werden soll.

Bei allen anderen Betriebssystemen gilt: Wenn `-fc` nicht angegeben ist und Speichermangel auf der Festplatte auftritt, wird ein schwerwiegender Fehler gemeldet.

Sie können Systemereignisse erstellen, um den verfügbaren Speicherplatz von Computern zu protokollieren, die die Datenbankdatei, die Logdatei oder die temporäre Datei enthalten, und um Administratoren bei Speichermangel zu warnen.

### Siehe auch

- „Wie SQL Anywhere die Dateien findet“ auf Seite 483
- „CREATE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Callback-Funktionen“ [*SQL Anywhere Server - Programmierung*]
- „Systemereignisse“ auf Seite 1091
- „max\_temp\_space-Option“ auf Seite 636
- „temp\_space\_limit\_check-Option“ auf Seite 689

### Beispiel

Wenn der Datenbankserver startet, versucht er, die `diskfull.dll`-DLL zu laden.

```
dbsrv16 -fc diskfull.dll -n my_server
```

## Datenbankserveroption -fips

Verlangt, dass nur FIPS-zertifizierte Algorithmen für starke Datenbank- und Kommunikationsverschlüsselung verwendet werden.

### Syntax

**dbsrv16 -fips ...**

### Gilt für

Windows, Unix und Linux.

### Bemerkungen

Das Angeben dieser Option erzwingt, dass für sämtliche Datenbankserververschlüsselung FIPS-zertifizierte Algorithmen verwendet werden. Diese Option gilt für starke Datenbankverschlüsselung, Client/Server-Transportschichtsicherheit und Webdienst-Transportschichtsicherheit. Sie können unverschlüsselte Verbindungen und Datenbanken auch mit aktivierter Option -fips verwenden, einfache Verschlüsselung hingegen ist nicht möglich.

#### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „[Getrennt lizenzierbare Komponenten](#)“ [*SQL Anywhere 16 - Einführung*].

Bei der starken Datenbankverschlüsselung bewirkt die Option -fips, dass neue Datenbanken das FIPS-zertifizierte Äquivalent von AES und AES256 verwenden, wenn diese in der ALGORITHM-Klausel in der CREATE DATABASE-Anweisung angegeben sind.

Wenn der Datenbankserver mit -fips gestartet wird, können Sie Datenbanken mit AES-, AES256-, AES\_FIPS- oder AES256\_FIPS-Verschlüsselung ausführen, jedoch keine Datenbanken mit einfacher Verschlüsselung. Unverschlüsselte Datenbanken können ebenfalls auf dem Server gestartet werden, wenn -fips angegeben wurde.

Die SQL Anywhere-Sicherheitsoption muss auf jedem Computer installiert sein, der verwendet wird, um eine mit AES\_FIPS oder AES256\_FIPS verschlüsselte Datenbank auszuführen.

Bei Transportschichtsicherheit bewirkt die Option -fips, dass der Server den FIPS-zertifizierten RSA-Verschlüsselungsalgorithmus verwendet, auch wenn RSA angegeben ist.

Bei Transportschichtsicherheit für Webdienste bewirkt die Option -fips, dass der Server FIPS-zertifiziertes HTTPS verwendet, auch wenn HTTPS angegeben ist.

Wenn Sie -fips angeben, verwenden die Funktionen ENCRYPT und HASH den FIPS-zertifizierten RSA-Verschlüsselungsalgorithmus und das Kennwort-Hashing verwendet den SHA-256 FIPS-Algorithmus statt des SHA-256-Algorithmus.

### Siehe auch

- „Einfache Verschlüsselung und starke Verschlüsselung“ auf Seite 1425
- „Transportschichtssicherheit“ auf Seite 1444
- „Verschlüsselung für SQL Anywhere-Webdienste“ auf Seite 1458
- „Datenbankserveroption -ec “ auf Seite 230
- „ENCRYPT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „HASH-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption -ga

Entlädt die Datenbank, nachdem der letzte Nicht-HTTP-Client die Verbindung getrennt hat.

### Syntax

**dbsrv16 -ga ...**

### Gilt für

Alle Betriebssysteme.

### Bemerkungen

Wenn diese Option im Netzwerkserver angegeben ist, werden alle Datenbanken entladen, nachdem die letzte Nicht-HTTP-Clientverbindung getrennt wurde. Zusätzlich zum Entladen jeder Datenbank, und nachdem die letzte Nicht-HTTP-Verbindung getrennt wurde, fährt der Datenbankserver herunter, wenn die letzte Datenbank gestoppt ist.

Wenn die einzige Verbindung mit einer Datenbank eine HTTP-Verbindung ist und die Datenbank so konfiguriert ist, dass sie bei der Trennung der HTTP-Verbindung automatisch herunterfährt, wird die Datenbank nicht automatisch entladen. Außerdem gilt: Wenn Sie die Option -ga definiert haben und die Datenbank eine HTTP-Verbindung und eine Befehlssequenz oder eine TDS-Verbindung hat und die letzte Befehlssequenz eine Trennung bewirkt oder die TDS-Verbindung getrennt wird, dann wird die Datenbank automatisch gestoppt und alle HTTP-Verbindungen werden getrennt.

### Siehe auch

- „Neuaufbau von Datenbanken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Verbindungsparameter AutoStop (ASTOP)“ auf Seite 342

## Datenbankserveroption -gb

Legt die Server-Prozessprioritätsklasse fest

### Windows-Syntax

**dbsrv16 -gb { idle | normal | high | maximum } ...**

### Unix-/Mac OS X-Syntax

**dbsrv16 -gb level ...**

**Zulässige Werte**

- **Unix** Unter Unix ist *level* eine Ganzzahl von -20 bis 19. Der Standardwert unter Unix ist derselbe wie der nice-Wert des übergeordneten Prozesses. Niedrigere Werte für *level* stellen eine günstigere Abfolgeplanungspriorität dar. Alle Einschränkungen für die Verwendung von nice-Werten gelten für die Option -gb. Beispiel: Auf den meisten Unix-Plattformen kann nur der root-Benutzer die Prioritätsstufe eines Prozesses herabsetzen (z.B. durch Änderung von 0 auf -1).
- **Windows** Unter Windows werden normalerweise die Einstellungen "normal" und "high" verwendet. Der Wert "idle" wird der Vollständigkeit halber bereitgestellt. Der Wert "maximum" kann den Betrieb Ihres Computers stören.

**Gilt für**

Windows, Unix, Mac OS X.

## Datenbankserveroption -gc

Setzt das maximale Intervall zwischen Checkpoints.

**Syntax**

**dbsrv16 -gc** *minutes* ...

**Standardwert**

60 Minuten

**Zulässige Werte**

- **minutes** Der Standardwert ist die Einstellung der Datenbankoption *checkpoint\_time*, die standardmäßig 60 Minuten beträgt. Wenn ein Wert von "0" eingegeben ist, wird der Standardwert von 60 Minuten verwendet.

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Verwenden Sie diese Option zum Festlegen der maximalen Zeitspanne in Minuten, die der Datenbankserver läuft, ohne für jede Datenbank einen Checkpoint zu setzen.

Checkpoints werden üblicherweise häufiger gesetzt als in der angegebenen Zeitspanne angegeben.

Siehe „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077.

**Siehe auch**

- „*checkpoint\_time*-Option“ auf Seite 588
- „Checkpoint-Logs“ auf Seite 143
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077

## Datenbankserveroption -gd

Legt fest, welche Privilegien zum Starten oder Stoppen einer Datenbank auf einem laufenden Datenbankserver erforderlich sind.

### Syntax

**dbsrv16 -gd { DBA | all | none } ...**

### Zulässige Werte

- **DBA** Nur Benutzer mit SERVER OPERATOR-Systemprivileg können Datenbanken starten oder stoppen.
- **all** Alle Benutzer können neue Datenbanken starten. Nicht empfohlen für Netzwerkserver, auf die von entfernten Clients zugegriffen werden kann.
- **none** Starten und Stoppen der Datenbanken ist nur dann zulässig, wenn der Datenbankserver selbst gestartet oder gestoppt wird.

### Standardwert

Die Standardeinstellung für den Personal Datenbankserver ist **all**.

Die Standardeinstellung für den Netzwerk-Datenbankserver ist **DBA**. Groß- und Kleinschreibung sind gleichermaßen zulässig.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option gibt die Privilegiestufe an, mit der der Benutzer einen Datenbankserver veranlassen kann, eine neue Datenbankdatei zu laden, oder eine Datenbank auf einem laufenden Datenbankserver stoppen kann.

Wenn die Option auf DBA gesetzt ist, muss die Clientanwendung zum Starten und Stoppen von Datenbanken eine vorhandene DBA-Verbindung mit einer anderen Datenbank verwenden, die auf demselben Server läuft. Sie können eine noch nicht laufende Datenbank nicht starten, indem Sie den DatabaseFile-Verbindungsparameter angeben.

Sie können die Einstellung der Option -gd mithilfe der StartDBPermission-Servereigenschaft abrufen:

```
SELECT PROPERTY ( 'StartDBPermission' );
```

Die Privilegien zum Stoppen eines Datenbankservers werden durch die Option -gk angegeben.

### Siehe auch

- „Datenbankserveroption -gk“ auf Seite 242
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „STOP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Beispiel**

Die folgenden Schritte veranschaulichen, wie Sie die Option -gd für den Netzwerk-Datenbankserver verwenden.

1. Starten Sie einen Netzwerk-Datenbankserver:

```
dbsrv16 -su mypwd -gd DBA -n my_server
```

2. Verbinden Sie sich mit Interactive SQL mit der Dienstprogrammdatenbank:

```
dbisql -c "UID=DBA;PWD=mypwd;DBN=utility_db"
```

3. Starten Sie eine Datenbank:

```
START DATABASE 'demo.db';
```

4. Stellen Sie eine Verbindung mit der Datenbank her:

```
CONNECT USING 'DBN=demo;UID=DBA;PWD=sql';
```

## Datenbankserveroption -ge

Legt die Stackgröße für externe Funktionen fest

**Syntax**

```
dbsrv16 -ge integer ...
```

**Standardwert**

32 kB

**Gilt für**

Windows.

**Bemerkungen**

Setzt die Stackgröße in Byte für Threads, die in externen Funktionen laufen.

**Siehe auch**

- [„Threading-Verhalten“ auf Seite 174](#)

## Datenbankserveroption -gf

Deaktiviert das Auslösen von Triggern durch den Server

**Syntax**

```
dbsrv16 -gf ...
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Mit der Serveroption `-gf` wird der Server angewiesen, das Auslösen von Triggern zu deaktivieren, einschließlich Trigger zur Wahrung der referenziellen Integrität (wie kaskadierendes Aktualisieren und Löschen).

### Siehe auch

- „`fire_triggers`-Option“ auf Seite 612
- „Trigger“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -gk

Legt fest, welche Privilegien zum Stoppen des Datenbankservers erforderlich sind.

### Syntax

`dbsrv16 -gk { DBA | all | none } ...`

### Zulässige Werte

- **DBA** Nur Benutzer mit dem `SERVER OPERATOR`-Systemprivileg können den Datenbankserver stoppen. Dies ist die Standardeinstellung des Netzwerkservers.
- **all** Zum Herunterfahren des Datenbankservers sind keine Privilegien erforderlich. Dies ist die Standardeinstellung des Personal Servers.
- **none** Der Datenbankserver kann nicht gestoppt werden.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die Datenbankserveroption `-gd` gilt für das Dienstprogramm `dbstop` sowie für die folgenden Anweisungen:

- `ALTER DATABASE Datenbankname FORCE START`-Anweisung.
- `STOP DATABASE`-Anweisung

### Siehe auch

- „Serverstopp-Dienstprogramm (`dbstop`)“ auf Seite 984

## Datenbankserveroption -gl

Legt fest, welches Privileg zum Laden von Daten mit der `LOAD TABLE`-Anweisung und zum Entladen von Daten mit der Anweisung `UNLOAD` oder `UNLOAD TABLE` erforderlich ist.

### Syntax

`dbsrv16 -gl { DBA | all | none } ...`

### Zulässige Werte

- **DBA** Zum Entladen von Daten müssen Sie das SELECT ANY TABLE-Systemprivileg haben.

Zum Laden von Daten müssen Sie das Systemprivileg LOAD ANY TABLE, ALTER ANY TABLE oder ALTER ANY OBJECT haben.

- **all** Zum Entladen von Daten müssen Sie der Eigentümer der Tabellen sein bzw. das SELECT-Privileg für die Tabellen oder das SELECT ANY TABLE-Systemprivileg haben.

Zum Laden von Daten muss eine der folgenden Bedingungen erfüllt sein:

- Sie sind der Eigentümer der Tabelle
  - Sie haben das LOAD-Privileg für die Tabelle
  - Sie haben das LOAD ANY TABLE-Systemprivileg
  - Sie haben das ALTER ANY TABLE-Systemprivileg
  - Sie haben das ALTER ANY OBJECT-Systemprivileg
- **none** Daten können nicht geladen oder entladen werden.

### Standardwert

Die Standardeinstellung ist **all** für Personal Datenbankserver unter Windows und **DBA** für den Personal Server unter Unix.

Die Standardeinstellungen tragen der Tatsache Rechnung, dass bei Nicht-Unix-Plattformen der Personal Datenbankserver auf dem aktuellen Computer läuft, sodass der Benutzer bereits Zugriff auf das Dateisystem hat.

Die Standardeinstellung für den Netzwerk-Datenbankserver ist **DBA**.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Mit den Anweisungen UNLOAD TABLE oder UNLOAD werden Daten in Dateien auf dem Datenbankserver platziert, während die Anweisung LOAD TABLE Dateien vom Datenbankserver einliest.

Mit der Serveroption -gl können Sie steuern, welche Privilegien erforderlich sind, um mit diesen Anweisungen auf das Dateisystem zuzugreifen.

Groß- und Kleinschreibung werden gleichermaßen akzeptiert.

### Siehe auch

- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UNLOAD-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Datenbankserveroption -gm

Begrenzt die Anzahl von gleichzeitigen Verbindungen mit dem Datenbankserver.

### Syntax

**dbsrv16 -gm** *integer* ...

### Standardwert

Der Standardwert für den Personal Server beträgt 10. Der Standardwert für den Netzwerk-Datenbankserver ist 32766, doch diese Zahl wird durch interne temporäre Verbindungen verringert, die vom Server während des Betriebs genutzt werden.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Definiert die Verbindungsbeschränkung für den Server. Falls diese Zahl größer als die von Lizenz- und Speicherbeschränkungen erlaubte Zahl ist, hat sie keine Auswirkung. Computerressourcen begrenzen üblicherweise die Anzahl der Verbindungen zu einem Netzwerkserver auf einen niedrigeren Wert als den Standardwert.

Der Datenbankserver lässt eine zusätzliche DBA-Verbindung über den Verbindungsgrenzwert hinaus zu, damit ein Benutzer mit DROP CONNECTION-Systemprivileg sich mit dem Datenbankserver verbinden und andere Verbindungen trennen kann.

### Siehe auch

- [MaxConnections-Servereigenschaft auf Seite 753](#)

## Datenbankserveroption -gn

Setzt die Multiprogramming-Stufe des Datenbankservers.

### Syntax

**dbsrv16 -gn** *integer* ...

### Standardwert

20 aktive Aufgaben für den Netzwerk-Datenbankserver

20 aktive Aufgaben für den Personal Datenbankserver

3 für Windows Mobile

### Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Die Serveroption `-gn` legt die erste Datenbankserver-Multiprogramming-Stufe fest.

Standardmäßig passt der Netzwerk-Datenbankserver automatisch die Server-Multiprogramming-Stufe als Reaktion auf Änderungen in der Arbeitslast des Servers an. Sie können die Einstellung für das Multiprogramming manuell außer Kraft setzen, nachdem ein Netzwerk-Datenbankserver gestartet wurde, indem Sie die Systemprozedur `sa_server_option` und den `CurrentMultiprogrammingLevel`-Parameter verwenden.

### Hinweis

Wenn Sie einen großen *integer*-Wert festlegen, kann dies die maximale auf 32-Bit-Plattformen verfügbare Cachinggröße reduzieren.

## Siehe auch

- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL Anywhere-Threading“ auf Seite 171
- „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175
- „Datenbankserveroption `-gna`“ auf Seite 245
- „Datenbankserveroption `-gnh`“ auf Seite 246
- „Datenbankserveroption `-gnl`“ auf Seite 247
- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption `-gna`

Steuert die automatische Optimierung der Multiprogramming-Stufe des Netzwerk-Datenbankservers.

## Syntax

```
dbsrv16 -gna { 0 | 1 }
```

## Standardwert

1 (Aktiviert)

## Gilt für

Alle Betriebssysteme, ausgenommen Windows Mobile.

Nur Netzwerk-Datenbankserver (dbsrv16).

## Bemerkungen

Diese Option aktiviert und deaktiviert die dynamische Optimierung der Multiprogramming-Stufe des Netzwerk-Datenbankservers. Sie können die Multiprogramming-Stufe manuell ändern, während der Netzwerk-Datenbankserver läuft, indem Sie die Systemprozedur `sa_server_option` verwenden.

Standardmäßig ist die automatische Optimierung der Multiprogramming-Stufe des Netzwerk-Datenbankservers aktiviert.

### Siehe auch

- „SQL Anywhere-Threading“ auf Seite 171
- „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175
- AutoMultiProgrammingLevel-Servereigenschaft auf Seite 745
- „max\_query\_tasks-Option“ auf Seite 633
- „Datenbankserveroption -gn “ auf Seite 244
- „Datenbankserveroption -gnh “ auf Seite 246
- „Datenbankserveroption -gnl “ auf Seite 247
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption -gnh

Legt die höchste Multiprogramming-Stufe fest - die maximale Anzahl von Aufgaben, die der Netzwerk-Datenbankserver gleichzeitig ausführen kann.

### Syntax

**dbsrv16 -gnh integer ...**

### Standardwert

Der Wert der Datenbankserveroption -gn, multipliziert mit vier.

### Gilt für

Alle Betriebssysteme ausgenommen Windows Mobile.

Nur Netzwerk-Datenbankserver (dbsrv16).

### Bemerkungen

Diese Option legt die maximale Multiprogramming-Stufe des Netzwerk-Datenbankservers fest. Sie begrenzt die maximale Anzahl der Aufgaben (Benutzer- und Systemanforderungen), die der Netzwerk-Datenbankserver gleichzeitig ausführen kann. Wenn der Netzwerk-Datenbankserver an diesem Limit eine zusätzliche Anforderung erhält, muss die neue Anforderung warten, bis eine ausführende Aufgabe abgeschlossen ist. Die Anzahl der aktiven Aufgaben, die gleichzeitig ausgeführt werden können, hängt von der Anzahl der Netzwerk-Datenbankserver-Threads und der Anzahl der logischen Prozessoren ab, die im System verwendet werden.

Die maximale Anzahl von nicht-geplanten und aktiven Anforderungen wird durch die Netzwerk-Datenbankserveroption -gm begrenzt, die die Anzahl der Verbindungen zum Netzwerk-Datenbankserver limitiert.

Wenn Sie den Wert -gnh zu hoch festlegen, kann dies zu Fehlern führen, weil ein größerer Teil des Adressraumes des Systems für Stack-Speicherplatz verbraucht wird.

Der Kernel des Netzwerk-Datenbankservers verwendet Aufgaben als Zeitplaneinheit. Die Ausführung einer Benutzeranforderung erfordert zumindest eine Aufgabe. Eine Anforderung kann allerdings das Einplanen von weiteren, durch sie bedingte Aufgaben bewirken. Ein Beispiel für dieses Verhalten liegt vor, wenn die Anforderung die Ausführung einer externen Prozedur oder Funktion (Java, Perl, CLR etc.) verlangt, die selbst wiederum Datenbankabfragen im Netzwerk-Datenbankserver durchführt.

Wenn die abfrageinterne Parallelität verwendet wird, ist jede parallel ausgeführte Zugriffskomponente eine Aufgabe. Demzufolge werden diese Aufgaben beim Limit -gnh so gezählt, als wären sie separate Anforderungen. Aufgaben jedoch, die für die abfrageinterne Parallelität erstellt wurden, werden in den Datenbankeigenschaften, die die Anzahl der aktiven und inaktiven Anforderungen protokollieren, nicht wiedergegeben.

#### **Vorsicht**

Ein Stack der durch -gss angegebenen Größe wird jedem Datenbankserver-Worker-Thread zugewiesen.

Die maximale Anzahl von Worker-Threads wird für Netzwerkserver durch die Option -gnh festgelegt.

Bei Personal Servern wird die maximale Anzahl von Worker-Threads durch die Option -gn festgelegt.

Wenn Sie einen hohen Wert -gss und einen hohen Wert für die maximale Anzahl von Worker-Threads festlegen, kann der Datenbankserver möglicherweise nicht gestartet werden oder die Größe des Cache signifikant beschränkt sein. Beispiel: Wenn Sie für den Start des Netzwerk-Datenbankservers -gss 16M und -gnh 100 angegeben haben, werden 1,6 GB des Server-Adressraums für Stacks reserviert.

#### **Siehe auch**

- „SQL Anywhere-Threading“ auf Seite 171
- „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175
- MaxMultiProgrammingLevel-Servereigenschaft auf Seite 753
- „max\_query\_tasks-Option“ auf Seite 633
- „Datenbankserveroption -gn “ auf Seite 244
- „Datenbankserveroption -gna “ auf Seite 245
- „Datenbankserveroption -gnl “ auf Seite 247
- „Datenbankserveroption -gss “ auf Seite 250
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## **Datenbankserveroption -gnl**

Legt die minimale Netzwerkserver-Multiprogramming-Stufe fest.

#### **Syntax**

**dbsrv16 -gnl integer ...**

#### **Standardwert**

Das Minimum des Werts der Serveroption -gtc und die Anzahl der logischen CPUs auf dem Computer.

#### **Gilt für**

Alle Betriebssysteme ausgenommen Windows Mobile.

Nur Netzwerk-Datenbankserver (dbsrv16).

#### **Bemerkungen**

Ein Festlegen des Werts -gnl stellt sicher, dass die aktuelle Multiprogramming-Stufe nicht niedriger als dieser Wert gesetzt werden kann. Bei intensiven Arbeitslasten, denen Perioden von Leerlaufzeit folgen,

lohnt es sich möglicherweise, den Wert `-gnl` zu erhöhen, um die Netzwerk-Datenbankserver-Performance zu verbessern, wenn die intensive Phase wieder auftritt.

### Siehe auch

- „Datenbankserveroption `-gtc`“ auf Seite 253
- „SQL Anywhere-Threading“ auf Seite 171
- „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175
- `MinMultiProgrammingLevel`-Servereigenschaft auf Seite 754
- „`max_query_tasks`-Option“ auf Seite 633
- „Datenbankserveroption `-gn`“ auf Seite 244
- „Datenbankserveroption `-gna`“ auf Seite 245
- „Datenbankserveroption `-gnh`“ auf Seite 246
- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption `-gns`

Zeigt die Statistik für automatische Anpassungen der Multiprogramming-Stufe im Meldungslog des Datenbankservers an.

### Syntax

`dbsrv16 -gns ...`

### Standardwert

Statistiken werden nicht angezeigt.

### Gilt für

Alle Betriebssysteme ausgenommen Windows Mobile.

Nur Netzwerk-Datenbankserver.

### Bemerkungen

Statistiken zur Multiprogramming-Stufe werden im Meldungslog des Datenbankservers nur aufgezeichnet, wenn die Option `-gns` gesetzt ist.

Sie können die Einstellung für die Berichterstellung in Verbindung mit Statistiken zur Multiprogramming-Stufe ändern, sobald der Datenbankserver damit begonnen hat, die Systemprozedur `sa_server_option` zu verwenden.

Um zu ermitteln, ob Statistiken zur Multiprogramming-Stufe derzeit gemeldet werden, führen Sie die folgende Abfrage aus:

```
SELECT PROPERTY ( 'AutoMultiProgrammingLevelStatistics' );
```

**Siehe auch**

- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175
- AutoMultiProgrammingLevelStatistics-Servereigenschaft auf Seite 745
- „Datenbankserveroption -gn “ auf Seite 244
- „Datenbankserveroption -gna “ auf Seite 245
- „Datenbankserveroption -gnh “ auf Seite 246
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Protokollieren von Datenbankserver-Aktionen“ auf Seite 163

## Datenbankserveroption -gp

Legt die maximal zulässige Seitengröße der Datenbank fest

**Syntax**

**dbsrv16 -gp { 2048 | 4096 | 8192 | 16384 | 32768 } ...**

**Standardwert**

4096 (wenn ein Datenbankserver gestartet wird, ohne dass eine Datenbank geladen ist)

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Datenbankdateien mit einer größeren Seitengröße als die Seitengröße des Servers können nicht geladen werden. Diese Option setzt die Seitengröße des Servers in Byte fest.

Standardmäßig wird die Serverseitengröße in der Befehlszeile auf die größte Seitengröße der Datenbank gesetzt.

Wenn Sie diese Option nicht verwenden und einen Server ohne Datenbanken starten, ist der Standardwert auf allen Plattformen 4096.

**Siehe auch**

- „Hinweise zur maximalen Seitengröße“ auf Seite 160
- „Tipp: Angemessene Seitengröße verwenden“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankserveroption -gr

Legt die maximale Dauer in Minuten für die Wiederherstellung nach einem Systemausfall fest

**Syntax**

**dbsrv16 -gr minutes ...**

### Standardwert

Die Einstellung der Datenbankoption `recovery_time`, die standardmäßig 2 Minuten beträgt.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn ein Datenbankserver mit mehreren Datenbanken läuft, wird die in der ersten gestarteten Datenbank festgelegte Wiederherstellungszeit verwendet, falls sie nicht durch diese Option überschrieben wird.

Der von der Option `-gr` angegebene Wert teilt dem Datenbankserver mit, wie oft ein Checkpoint ausgeführt werden soll. Beispiel: Wenn Sie die Option `-gr` auf 5 setzen, versucht der Datenbankserver, Checkpoints so häufig auszuführen, dass die Wiederherstellung nicht länger als fünf Minuten dauert. Wenn allerdings eine Wiederherstellung erforderlich ist, wird sie bis zum Abschluss durchgeführt, auch wenn sie länger als die in der Option `-gr` angegebene Zeitspanne dauert.

Die Wiederherstellungszeit enthält sowohl die geschätzte Wiederherstellungszeit als auch die geschätzte Checkpoint-Zeit für die Datenbank.

### Siehe auch

- „`recovery_time`-Option“ auf Seite 661
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077

## Datenbankserveroption `-gss`

Legt die Stackgröße pro Worker-Thread auf dem Datenbankserver fest.

### Syntax

```
dbsrv16 -gss { integer[ k | m ] } ...
```

### Gilt für

Alle Betriebssysteme und Server. Für Windows wird diese Option ab Windows XP unterstützt.

### Bemerkungen

Mit der Option `-gss` können Sie in Umgebungen mit begrenztem Speicher eine geringere Speichernutzung durch den Datenbankserver einstellen.

*size* ist der zu nutzende Speicherplatz in Byte. Verwenden Sie **k** oder **m**, um die Einheit in kB bzw. MB anzugeben.

**Vorsicht**

Ein Stack der durch -gss angegebenen Größe wird jedem Datenbankserver-Worker-Thread zugewiesen. Die maximale Anzahl von Worker-Threads wird für Netzwerkserver durch die Option -gnh festgelegt.

Bei Personal Servern wird die maximale Anzahl von Worker-Threads durch die Option -gn festgelegt.

Wenn Sie einen hohen Wert -gss und einen hohen Wert für die maximale Anzahl von Worker-Threads festlegen, kann der Datenbankserver möglicherweise nicht gestartet werden oder die Größe des Cache signifikant beschränkt sein. Beispiel: Wenn Sie für den Start des Netzwerk-Datenbankservers -gss 16M und -gnh 100 angegeben haben, werden 1,6 GB des Server-Adressraums für Stacks reserviert.

Die minimalen, maximalen, und Standard-Stackgrößen pro Worker-Thread lauten folgendermaßen:

Plattform	Minimum	Standardwert	Maximum
Unix (32-Bit)	512 kB	512 kB	4 MB
Unix (64-Bit)	1 MB	1 MB	8 MB
Windows (32-Bit)	64 kB	1 MB	16 MB
Windows (64-Bit)	64 kB	4 MB	256 MB
Windows Mobile	64 kB	96 kB	512 kB

**Siehe auch**

- „SQL Anywhere-Threading“ auf Seite 171
- „Datenbankserveroption -gss“ auf Seite 250

**Datenbankserveroption -gt**

Legt die maximale Anzahl von verwendbaren physischen Prozessoren (bis Lizenzlimit) fest. Diese Option ist nur bei Mehrprozessorsystemen sinnvoll.

**Syntax**

**dbsrv16 -gt** *num-processors* ...

**Zulässige Werte**

- **Anzahl\_Prozessoren** Diese Ganzzahl kann einen Wert annehmen zwischen "1" und dem Minimum von:
  - der Anzahl von physischen Prozessoren auf dem Computer
  - der maximalen Anzahl von CPUs, für die der Server lizenziert ist, falls CPU-Lizensierung verwendet wird

Wenn der angegebene -gt-Wert außerhalb dieses Bereichs liegt, wird die Unter- bzw. Obergrenze wirksam. Beim Personal Datenbankserver (dbeng16) verwendet der Server für -gt einen Wert von 1.

### Gilt für

Windows (außer Windows Mobile), Linux und Solaris.

### Bemerkungen

Bei Perseat-Lizenzierung nutzt der Netzwerk-Datenbankserver alle auf dem Computer verfügbaren CPUs. Bei CPU-basierter Lizenzierung nutzt der Netzwerk-Datenbankserver nur die lizenzierte Anzahl von Prozessoren. Die Anzahl der CPUs, die ein Netzwerk-Datenbankserver nutzen kann, wird möglicherweise auch durch Ihre SQL Anywhere-Edition eingeschränkt.

Der Personal Datenbankserver ist immer auf einen einzelnen Prozessor begrenzt.

Wenn Sie einen Wert für die Option `-gt` angeben, passt der Datenbankserver seine Affinitätsmaske an (sofern auf der jeweiligen Hardware-Plattform unterstützt), um den Datenbankserver auf die Ausführung dieser Anzahl physischer Prozessoren zu beschränken. Wenn der Datenbankserver für  $n$  Prozessoren lizenziert ist, wird der Server standardmäßig auf allen logischen Prozessoren (Hyperthreads und Prozessorkerne) von  $n$  physischen Prozessoren ausgeführt. Dieses Verhalten kann mit der Option `-gtc` weiter eingeschränkt werden.

Die Option `-gt` kann nicht mit der Option `-gta` verwendet werden.

### Siehe auch

- „Editionen und Lizenzierung“ [[SQL Anywhere 16 - Einführung](#)]
- „Datenbankserveroption `-gnh`“ auf Seite 246
- „Datenbankserveroption `-gtc`“ auf Seite 253
- „Datenbankserveroption `-gta`“ auf Seite 252
- ProcessorAffinity-Option: „`sa_server_option-Systemprozedur`“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SQL Anywhere-Threading“ auf Seite 171

## Datenbankserveroption `-gta`

Legt fest, welche logischen Prozessoren der Datenbankserver verwenden kann.

### Syntax

**`dbsrv16 -gta`** *logical-processors-to-use*,...

### Zulässige Werte

- **Einsetzbare\_logische\_Prozessoren** Akzeptiert eine durch Kommas getrennte Liste von Prozessorzahlen bzw. Bereichen. Wenn der niedrigere Endpunkt eines Bereichs nicht angegeben ist, wird angenommen, dass er null ist. Wenn der obere Endpunkt des Bereichs nicht angegeben ist, wird angenommen, dass er der höchsten vom Betriebssystem erkannten CPU entspricht. Um alle Prozessoren anzugeben, müssen Sie `-` oder **0-** eingeben.

### Gilt für

Windows und Linux. Sie müssen die `MANAGE_SERVER`-Rolle haben, um diese Datenbankserveroption verwenden zu können.

## Bemerkungen

Mit der Option -gta können Sie angeben, welche logischen Prozessoren der Datenbankserver nutzt.

Der Datenbankserver nutzt in den folgenden Fällen möglicherweise nicht alle angegebenen logischen Prozessoren:

- Wenn mindestens einer der angegebenen logischen Prozessoren nicht vorhanden oder offline ist.
- Wenn die Lizenz dies nicht zulässt.

Wenn die Gruppe der durch die Option -gta angegebenen logischen Prozessoren die Grenzen der Lizenz überschreitet, nutzt der Datenbankserver die durch die Option -gta angegebenen logischen Prozessoren mit den niedrigsten Nummern, wobei aber die Grenzen der Lizenz nicht überschritten werden. Der Datenbankserver wählt logische Prozessoren nicht in der durch die Option -gta angegebenen Reihenfolge. Der Server versucht nicht, die Parallelität innerhalb der Grenzen der Lizenz und der angegebenen Option -gta zu maximieren.

Wenn die Gruppe der durch die Option -gta angegebenen logischen Prozessoren zu keinem Online-Prozessor passt, verhält sich der Datenbankserver so, als wäre die Option -gta nicht angegeben worden, und nutzt maximal die lizenzierte Anzahl logischer Prozessoren, beginnend mit Prozessor 0.

Die Option -gta kann nicht mit der Option -gt oder -gtc verwendet werden.

Während der Datenbankserver läuft, können Sie die genutzten logischen Prozessoren mithilfe der ProcessorAffinity-Option der sa\_server\_option-Systemprozedur ändern.

## Siehe auch

- „Editionen und Lizenzierung“ [[SQL Anywhere 16 - Einführung](#)]
- „Datenbankserveroption -gt“ auf Seite 251
- „Datenbankserveroption -gtc“ auf Seite 253
- ProcessorAffinity-Option: „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Beispiel

Im folgenden Beispiel muss der Datenbankserver einige oder alle der logischen Prozessoren 3, 5, 6, 7 bzw. 9 verwenden:

```
dbsrv16 -gta 3,5-7,9
```

## Datenbankserveroption -gtc

Steuert die maximal möglichen gleichzeitigen Prozessoren, die der Datenbankserver zulässt

### Syntax

```
dbsrv16 -gtc logical-processors-to-use ...
```

### Gilt für

Linux-, Solaris- und Windows-Betriebssysteme, die auf Intel-kompatiblen x86- und x64-Plattformen laufen, ausgenommen Windows Mobile.

### Bemerkungen

Wenn Sie den Datenbankserver starten, wird die vom Datenbankserver erkannte Anzahl der physischen und logischen Prozessoren im Meldungsfenster des Datenbankservers angezeigt.

Physische Prozessoren werden manchmal als **Pakete** oder **Dies** (Rohchips) bezeichnet und sind die CPUs des Computers. Weitere logische Prozessoren bestehen, wenn die physischen Prozessoren Hyperthreads unterstützen oder selbst als **Mehrprozessoren** konfiguriert sind (üblicherweise Mehr-Kern-Prozessoren genannt). Das Betriebssystem erstellt den Zeitplan für Threads auf logischen Prozessoren.

Mit der Option `-gtc` können Sie die Anzahl der logischen Prozessoren festlegen, die vom Datenbankserver verwendet werden können. Ihr Zweck ist es, die Anzahl der Datenbankserver-Threads zu begrenzen, die beim Start des Datenbankservers erstellt werden. Dies begrenzt die Anzahl der aktiven Datenbankserver-Aufgaben, die gleichzeitig ausgeführt werden können. Standardmäßig ist die Anzahl der erstellten Threads 1 + die Anzahl der logischen Prozessoren auf allen lizenzierten physischen Prozessoren.

Standardmäßig lässt der Datenbankserver die gleichzeitige Nutzung aller logischen Prozessoren (Prozessorkerne oder Hyperthreads) auf jedem lizenzierten physischen Prozessor zu.

Beispiel: Wenn Sie eine Lizenz für eine CPU für ein System mit zwei CPUs verwenden, in dem jede CPU vier Prozessorkerne mit zwei Threads pro Prozessorkern enthält, lässt der Netzwerk-Datenbankserver acht parallele Threads auf einer CPU und null Threads auf der anderen zu. Wenn die Option `-gtc` angegeben wird und die Anzahl der zu verwendenden logischen Prozessoren ist geringer als die Anzahl der verfügbaren lizenzierten physischen Prozessoren, weist der Datenbankserver logische Prozessoren basierend auf einer Round Robin-Zuordnung zu. Wenn Sie 1 bei der Option `-gtc` angeben, wird die abfrageinterne Parallelität (parallele Verarbeitung von einzelnen Abfragen) implizit deaktiviert. Die abfrageinterne Parallelität kann auch mit der `max_query_tasks`-Option explizit begrenzt oder deaktiviert werden.

Die Option `-gtc` kann nicht mit der Option `-gta` verwendet werden.

Der Personal Datenbankserver ist auf vier Prozessorkerne in einer CPU beschränkt.

### Siehe auch

- „[max\\_query\\_tasks-Option](#)“ auf Seite 633
- „[Datenbankserveroption -gnh](#)“ auf Seite 246
- „[Datenbankserveroption -gt](#)“ auf Seite 251
- „[Datenbankserveroption -gta](#)“ auf Seite 252
- ProcessorAffinity-Option: „[sa\\_server\\_option-Systemprozedur](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „[SQL Anywhere-Threading](#)“ auf Seite 171

### Beispiel

Betrachten wir die folgenden Beispiele bei einem Windows-basierten SMP-Computer. Es wird jeweils ein 4-Prozessorensystem mit zwei Kernen auf jedem physischen Prozessor (also insgesamt acht logischen Prozessoren) angenommen. Die physischen Prozessoren werden mit Buchstaben und die logischen Prozessoren (in diesem Fall Kerne) mit Zahlen gekennzeichnet. Dieses 4-Prozessorensystem hat daher die Verarbeitungseinheiten A0, A1, B0, B1, C0, C1, D0 und D1.

Szenario	Einstellungen des Netzwerk-Datenbankservers
Eine einzelne CPU-Lizenz oder -gt 1 angegeben	<ul style="list-style-type: none"> <li>• -gt 1</li> <li>• -gtc 2</li> <li>• -gnh 20</li> </ul> <p>Threads können auf A0 und A1 ausgeführt werden.</p>
Keine Lizenz einschränkungen auf der CPU mit angegebenem -gtc 5	<ul style="list-style-type: none"> <li>• -gt 4</li> <li>• -gtc 5</li> <li>• -gnh 20</li> </ul> <p>Threads können auf A0, A1, B0, C0 und D0 ausgeführt werden.</p>
Ein Datenbankserver mit 3-CPU-Lizenz und angegebenem -gtc 5	<ul style="list-style-type: none"> <li>• -gt 3</li> <li>• -gtc 5</li> <li>• -gnh 20</li> </ul> <p>Threads können auf A0, A1, B0, B1 und C0 ausgeführt werden.</p>
Keine Lizenz einschränkungen auf der CPU mit angegebenem -gtc 1	<ul style="list-style-type: none"> <li>• -gt 4</li> <li>• -gtc 1</li> <li>• -gnh 20</li> </ul> <p>Threads können nur auf A0 ausgeführt werden.</p>

## Datenbankserveroption -gu

Legt fest, welches Privileg zum Ausführen von Anweisungen zur Datenbankdateiverwaltung erforderlich ist, z.B. zum Erstellen oder Löschen von Datenbanken.

### Syntax

```
dbsrv16 -gu { all | none | DBA | utility_db } ...
```

### Zulässige Werte

Befehlszeilenoption "-gu"	Auswirkung	Gilt für
<b>all</b>	<i>Diese Option wird nicht mehr empfohlen. Jeder Benutzer kann Anweisungen zur Dateiverwaltung ausführen.</i>	Jede Datenbank, einschließlich der Dienstprogrammdateiabank

Befehlszeilenoption "-gu"	Auswirkung	Gilt für
<b>none</b>	Das Ausführen von Anweisungen zur Dateiverwaltung ist nicht zulässig.	Jede Datenbank, einschließlich der Dienstprogrammdatenbank
<b>DBA</b>	Nur Benutzer mit SERVER OPERATOR-Systemprivileg können Anweisungen zur Dateiverwaltung ausführen.	Jede Datenbank, einschließlich der Dienstprogrammdatenbank
<b>utility_db</b>	Nur die Benutzer, die eine Verbindung mit der Dienstprogrammdatenbank herstellen können, dürfen Anweisungen zur Dateiverwaltung ausführen.	Nur die Dienstprogrammdatenbank

**Standardwert**

DBA

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Beschränkt die Benutzer, die die folgenden Anweisungen zur Datenbankdateiverwaltung ausführen können:

- ALTER DATABASE Datenbankdatei ALTER TRANSACTION LOG
- CREATE DATABASE-Anweisung
- CREATE DECRYPTED DATABASE-Anweisung
- CREATE DECRYPTED FILE-Anweisung
- CREATE ENCRYPTED DATABASE-Anweisung
- CREATE ENCRYPTED FILE-Anweisung
- DROP DATABASE-Anweisung
- RESTORE DATABASE-Anweisung.

Wenn utility\_db angegeben wird, können diese Anweisungen nur über die Dienstprogrammdatenbank ausgeführt werden. Wenn DBA angegeben wird, können diese Anweisungen nur von einem Benutzer mit SERVER OPERATOR-Systemprivileg ausgeführt werden. Wenn "none" angegeben wird, kann kein Benutzer diese Anweisungen ausführen.

**Siehe auch**

- „Die Dienstprogrammdatenbank“ auf Seite 145
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Beispiele**

Wenn Sie die Verwendung von Anweisungen zur Dateiverwaltung verhindern möchten, starten Sie den Datenbankserver mit der Privilegstufe "none" der Option -gu. Mit dem folgenden Befehl wird ein Datenbankserver gestartet und ihm der Name "TestSrv" gegeben. Damit wird die Datenbank *mytestdb.db* geladen, jedoch hat niemand die Berechtigung, den Server zum Erstellen bzw. Löschen einer Datenbank zu benutzen oder irgendeine sonstige Anweisung zur Dateiverwaltung auszuführen, und zwar unabhängig von den ursprünglichen Berechtigungen zum Erstellen oder von der Berechtigung, die Dienstprogrammdatenbank zu laden und eine Verbindung mit ihr herzustellen.

```
dbsrv16 -n TestSrv -gu none c:\mytestdb.db
```

Damit nur Benutzer, die das Kennwort der Dienstprogrammdatenbank kennen, das Ausführen von Anweisungen zur Dateiverwaltung gestattet wird, starten Sie den Server mit dem folgenden Befehl: Siehe „Datenbankserveroption -su“ auf Seite 289.

```
dbsrv16 -n TestSrv -su secret -gu utility_db
```

Der folgende Befehl startet Interactive SQL als Clientanwendung, verbindet sich mit dem Server "TestSrv", lädt die Dienstprogrammdatenbank und stellt eine Verbindung für den Benutzer her.

```
dbisql -c "UID=DBA;PWD=secret;DBN=utility_db;Host=host1;Server=TestSrv"
```

Nachdem der oben angeführte Befehl erfolgreich ausgeführt wurde, stellt der Benutzer eine Verbindung mit der Dienstprogrammdatenbank her und kann nun Anweisungen zur Dateiverwaltung ausführen.

## Datenbankserveroption -im

Führt den Datenbankserver im Speicher aus und reduziert oder eliminiert damit Schreibvorgänge auf der Festplatte.

**Syntax**

```
dbsrv16 -im { c | nw } ...
```

**Zulässige Werte**

- **Nur Checkpoint (-im c)** Im Nur-Checkpoint-Modus verwendet der Datenbankserver kein Transaktionslog und Sie können die letzte festgeschriebene Transaktion nicht wiederherstellen. Da jedoch das Checkpoint-Log aktiviert ist, kann die Datenbank bis zum letzten Checkpoint wiederhergestellt werden. Wenn Sie eine Datenbank ohne Transaktionslog betreiben, setzt der Datenbankserver beim Festschreiben dennoch einen Checkpoint, worunter die Performance leidet. Wenn Sie hingegen den Datenbankserver im Nur-Checkpoint-Modus betreiben, setzt der Datenbankserver nicht nach jedem Festschreiben einen Checkpoint.

Dieser Modus ist bei Anwendungen sinnvoll, die eine höhere Performance benötigen, und bei denen ein Verlust von festgeschriebenen Transaktionen nach dem letzten Checkpoint akzeptiert werden kann.

Die folgenden Einschränkungen gelten, wenn der Datenbankserver im Nur-Checkpoint-Modus läuft:

1. Es gibt kein Transaktionslog.
  2. Es gibt keine temporäre Datei.
  3. Checkpoints sind sowohl bei Bedarf als auch im Rhythmus der normalen Checkpoint-Frequenz des Datenbankservers zulässig.
  4. Dirty Pages werden nur bei einem Checkpoint auf die Festplatte ausgelagert.
- **Nie Schreiben (-im nw)** Im Nie-Schreiben-Modus werden festgeschriebene Transaktionen nicht in die Datenbankdatei auf dem Plattenspeicher geschrieben. Alle Änderungen gehen verloren, wenn die Datenbank herunterfährt oder abstürzt, die Datenbankdateien bleiben daher immer in ihrem ursprünglichen Zustand. Anforderungen zur Erweiterung bestehender oder Schaffung neuer DBSpaces sind zulässig, aber die Änderungen spiegeln sich in den Datenbankdateien nicht wider. Sie können neue DBSpaces erstellen und verwenden, sie werden aber nicht auf die Festplatte geschrieben. Eine Sicherung im Nie-Schreiben-Modus ist nicht sinnvoll, weil Änderungen im System-DBSpace nicht in die Datei geschrieben werden.

Die folgenden Einschränkungen gelten, wenn der Datenbankserver im Nie-Schreiben-Modus läuft:

1. Es gibt kein Transaktionslog.
2. Es gibt kein Checkpoint-Log.
3. Es gibt keine temporäre Datei.
4. Dirty Pages der Datenbank werden nie auf Festplatte ausgeschrieben.
5. Die ursprünglichen Datenbankdateien werden nie geändert.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

#### Hinweis

Für den In-Memory-Modus benötigen Sie eine separate Lizenz. Siehe „[Getrennt lizenzierte Komponenten](#)“ [[SQL Anywhere 16 - Einführung](#)].

### Bemerkungen

Diese Funktion ist besonders sinnvoll auf Systemen mit großem Arbeitsspeicher, der alle Datenbankdateien im Cache verfügbar halten kann.

Da im Never-Write-Modus (-im nw) Änderungen nie in die ursprünglichen Datenbankdateien geschrieben werden, müssen Sie das Dienstprogramm dbunload oder die UNLOAD TABLE-Anweisung verwenden,

wenn Sie eine beständige Kopie des aktuellen Datenbankinhalts benötigen. Sie können auch SQL-Abfragen verwenden, um die Änderungen abzufragen, müssen diese Änderungen dann aber manuell in die Datenbankdatei schreiben.

Ob der In-Memory-Modus Performancevorteile bringt, hängt von der Verarbeitungslast der Anwendung und dem Datendurchsatz des I/O-Subsystems ab. Die größten Performancegewinne werden bei Anwendungen erzielt, die große Datenmengen einfügen oder aktualisieren, sowie in Anwendungen, die häufig Festschreibungsvorgänge durchführen und einen Checkpoint setzen.

Oft ist die Performance bei speicherresidenten Modi mindestens so gut wie bei der Verwendung von transaktionalen globalen temporären Tabellen. Die geringsten Performanceverbesserungen werden bei Anwendungen festzustellen sein, die hauptsächlich die Datenbank abfragen. Im Allgemeinen können bei der Verwendung des In-Memory-Modus die größten Performancevorteile erzielt werden, wenn der Cache von vornherein auf eine Größe erweitert wird, der den gesamten, zu erwartenden Inhalt der Datenbankdateien aufnehmen kann. Damit wird viel Overhead vermieden, der durch die inkrementierte Erhöhung des Caches während der laufenden Anwendung entsteht.

#### **Vorsicht**

Da die Seiten im Nie-Schreiben-Modus nie aus dem Cache ausgelagert werden, kann der verfügbare Cache aufgebraucht werden, wenn die Menge der Daten in der Datenbank zu groß wird. Wenn dies eintritt, gibt der Datenbankserver eine Fehlermeldung aus und stoppt die Verarbeitung von Anforderungen. Aus diesem Grund sollte der Nie-Schreiben-Modus mit Bedacht verwendet und dafür Sorge getragen werden, dass der Cache so groß bemessen wird, dass die komplette Arbeitskopie der von der Anwendung benutzten Seiten darin Platz hat. Da Checkpoints im Modus "Nur-Checkpoint" weiterhin gesetzt werden, besteht im Vergleich zum Nie-Schreiben-Modus ein geringeres Risiko, dass der Server nicht mehr genügend verfügbaren Cache hat.

Für die Anweisung `LOAD TABLE` und einige `ALTER TABLE`-Anweisung wird das Checkpoint-Log verwendet, um die Auswirkungen einer Systemstörung teilweise aufzuheben oder eine Wiederherstellung nach einem Fehler vorzunehmen. Im Nie-Schreiben-Modus wird kein Checkpoint-Log erstellt und Sie können die Wirkungen bestimmter Anweisungen bei Fehlern nicht teilweise zurücksetzen. Falsche oder unvollständige Daten könnten daher in Tabellen verbleiben. Siehe „Checkpoint-Logs“ auf Seite 143.

#### **Siehe auch**

- „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)]
- „Datenbankserveroption -c“ auf Seite 217
- „Tipp: In-Memory-Modus verwenden“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## **Datenbankserveroption -k**

Steuert die Sammlung von Systemmonitor-Statistiken

#### **Syntax**

`dsrv16 -k ...`

#### **Standardwert**

Systemmonitor-Statistiken werden gesammelt.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn Sie -k beim Start des Datenbankservers angeben, sammelt der Datenbankserver keine Systemmonitor-Statistiken. Die Option -k wirkt sich nicht auf die Sammlung von Spaltenstatistiken aus, die vom Abfrageoptimierer verwendet werden.

Diese Option sollte nur verwendet werden, wenn der Datenbankserver auf einem Mehrprozessorcomputer läuft, bei dem sich durch Tests nachweisen lässt, dass sie die Performance verbessert. Bei den meisten Arbeitslasten ist der Nutzen vernachlässigbar, daher wird die Verwendung dieser Option nicht empfohlen. Wenn Sie die Leistungsindikatoren deaktivieren, stehen diese Informationen nicht für die Analyse von Performance-Problemen zur Verfügung.

Sie können die Einstellung für das Sammeln von Systemmonitor-Statistiken auch mit der Systemprozedur `sa_server_option` ändern.

### Siehe auch

- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- CollectStatistics-Serveigenschaft auf Seite 747
- „Datenbankserveroption -ks“ auf Seite 264
- „Datenbankserveroption -ksc“ auf Seite 264
- „Datenbankserveroption -ksd“ auf Seite 264
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Funktionen des Sybase Central-Systemmonitors zum Überwachen von Statistiken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -kl

Gibt den Dateinamen der Kerberos GSS-API-Bibliothek (oder eines Shared Object unter Unix) an und aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver.

### Syntax

```
dbsrv16 -kl GSS-API-library-file ...
```

### Gilt für

Alle Betriebssysteme, ausgenommen Windows Mobile.

### Bemerkungen

Diese Option gibt den Standort und den Namen der Kerberos GSS-API an. Diese Option ist nur erforderlich, wenn der Kerberos-Client einen anderen als den Standard-Dateinamen für die Kerberos GSS-API-Bibliothek verwendet, oder wenn mehrere GSS-API-Bibliotheken auf dem Computer installiert sind, der den Datenbankserver ausführt. Ein Kerberos-Client muss bereits installiert und konfiguriert sein, und SSPI kann vom Datenbankserver nicht verwendet werden.

Das Angeben dieser Option aktiviert die Kerberos-Authentifizierung für den Datenbankserver.

**Siehe auch**

- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Datenbankserveroption -krb “ auf Seite 263
- „Verbindungsparameter Kerberos (KRB)“ auf Seite 367
- „Kerberos-Authentifizierung“ auf Seite 63
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Beispiel**

Der folgende Befehl startet einen Datenbankserver, der das Shared Object *libgssapi\_krb5.so* für die Kerberos-Authentifizierung verwendet.

```
dbsrv16 -kl libgssapi_krb5.so -n my_server_princ /opt/myapp/kerberos.db
```

## Datenbankserveroption -kp

Gibt den Realm des Kerberos-Prinzips an und aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver.

**Syntax**

```
dbsrv16 -kp server-principal ...
```

**Gilt für**

Alle Betriebssysteme, ausgenommen Windows Mobile.

**Bemerkungen**

Diese Option gibt den Kerberos-Serverprinzipal an, der vom Datenbankserver verwendet wird, und aktiviert die Kerberos-Authentifizierung. Standardmäßig ist der Prinzipal, der vom Datenbankserver für die Kerberos-Authentifizierung verwendet wird, *Servername@Standardbereich*, wobei *Standardbereich* der für den Kerberos-Client konfigurierte Standardbereich ist. Geben Sie diese Option an, um einen anderen Serverprinzipal zu verwenden. Das Branchenstandardformat für Kerberos-Serverprinzipale ist *Servername/Hostname@Bereich*.

Wenn über OpenClient oder jConnect Kerberos-authentifizierte Verbindungen zum Datenbankserver hergestellt werden, muss der Serverprinzipal auch von der Anwendung angegeben werden. Weitere Informationen finden Sie in der jConnect-Dokumentation unter SERVICE\_PRINCIPAL\_NAME.

Die Option -kr kann nicht angegeben werden, wenn die Option -kp angegeben ist.

**Siehe auch**

- „Datenbankserveroption -kl “ auf Seite 260
- „Datenbankserveroption -krb “ auf Seite 263
- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Verbindungsparameter Kerberos (KRB)“ auf Seite 367
- „Kerberos-Authentifizierung“ auf Seite 63
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

### Beispiel

Der folgende Befehl startet einen Datenbankserver, der Kerberos-Logins akzeptiert, und verwendet für die Authentifizierung den Serverprinzipal `myserver/mycomputer.example.com@EXAMPLE.COM`.

```
dbsrv16 -kp myserver/mycomputer.example.com@EXAMPLE.COM -n myserver C:\kerberos.db
```

### Datenbankserveroption -kr (nicht mehr empfohlen)

Gibt den Realm des Kerberos-Prinzips an und aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver.

#### Hinweis

Die Verwendung der Option `-kr` wird nicht mehr empfohlen. Es wird empfohlen, dass Sie die Option `-kp` verwenden, um den Kerberos-Serverprinzipal anzugeben. Wenn Sie die Option `-kp` angeben, muss der Serverprinzipal in die Kerberos Keytab-Datei auf dem Computer extrahiert worden sein, auf dem der Datenbankserver läuft. Siehe „Datenbankserveroption -kp“ auf Seite 261.

### Syntax

```
dbsrv16 -kr server-realm ...
```

### Gilt für

Alle Betriebssysteme, ausgenommen Windows Mobile.

### Bemerkungen

Diese Option legt den Realm des Kerberos-Prinzips fest. Normalerweise ist der Prinzipal, der vom Datenbankserver für die Kerberos-Authentifizierung verwendet wird, *Servername@Standardbereich*, wobei *Standardbereich* der für den Kerberos-Client konfigurierte Standardbereich ist. Verwenden Sie diese Option, wenn der Serverprinzipal einen anderen als den Standardbereich verwenden soll. In diesem Fall wird der Serverprinzipal *Servername@Serverbereich* verwendet.

Das Angeben dieser Option aktiviert die Kerberos-Authentifizierung für den Datenbankserver.

Die Option `-kr` kann nicht angegeben werden, wenn die Option `-kp` angegeben ist.

### Siehe auch

- „Datenbankserveroption -kl“ auf Seite 260
- „Datenbankserveroption -krb“ auf Seite 263
- „Verbindungsparameter Kerberos (KRB)“ auf Seite 367
- „Kerberos-Authentifizierung“ auf Seite 63
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

### Beispiel

Der folgende Befehl startet einen Datenbankserver, der Kerberos-Logins akzeptiert, und verwendet den Prinzipal `my_server_princ@MYREALM` für die Authentifizierung.

```
dbsrv16 -kr MYREALM -n my_server_princ C:\kerberos.db
```

## Datenbankserveroption -krb

Aktiviert von Kerberos authentifizierte Verbindungen zum Datenbankserver

### Syntax

**dbsrv16 -krb ...**

### Gilt für

Alle Betriebssysteme, ausgenommen Windows Mobile.

### Bemerkungen

Diese Option aktiviert die Kerberos-Authentifizierung für den Datenbankserver. Sie müssen eine oder mehrere der Optionen -krb, -kl und -kr angeben, damit der Datenbankserver in der Lage ist, Clients mithilfe von Kerberos zu authentifizieren..

Bevor Sie die Kerberos-Authentifizierung verwenden können, muss ein Kerberos-Client bereits auf dem Client- und dem Datenbankserver-Computer installiert und konfiguriert sein. Zusätzlich muss der Prinzipal *Servername@Bereich* bereits im Kerberos-KDC vorhanden sein und die keytab-Datei für den Prinzipal *Servername@Bereich* muss bereits sicher in die keytab-Datei auf dem Datenbankserver-Computer extrahiert worden sein. Der Datenbankserver startet nicht, wenn die Option -krb angegeben wird, aber dieses Setup nicht durchgeführt wurde.

#### Hinweis

Der Datenbankservername darf keine der folgenden Zeichen enthalten: "/", "\" oder "@", und Datenbankservernamen mit Mehrbyte-Zeichen können nicht mit Kerberos verwendet werden.

Die Datenbankoption login\_mode muss gesetzt sein, um Kerberos-Logins zuzulassen, und Kerberos-Client-Prinzipale müssen den Datenbankbenutzer-IDs unter Verwendung der Anweisung GRANT KERBEROS LOGIN zugeordnet sein.

### Siehe auch

- „Datenbankserveroption -kl“ auf Seite 260
- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Verbindungsparameter Kerberos (KRB)“ auf Seite 367
- „Kerberos-Authentifizierung“ auf Seite 63
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „login\_mode-Option“ auf Seite 623

### Beispiel

Bei einem Kerberos-Prinzipal für den Datenbankserver namens my\_server\_princ@MYREALM startet der folgende Befehl einen Datenbankserver namens my\_server\_princ.

```
dbsrv16 -krb -n my_server_princ C:\kerberos.db
```

## Datenbankserveroption -ks

Deaktiviert die Erstellung von Shared Memory, das vom Systemmonitor verwendet wird, um Leistungsindikatoren vom Datenbankserver zu sammeln.

### Syntax

**dbsrv16 -ks 0 ...**

### Gilt für

Windows

### Bemerkungen

Wenn Sie diese Option festlegen, zeigt der Systemmonitor keine Datenbankserver-, Datenbank- oder Verbindungsstatistiken für den aktuellen Datenbankserver.

### Siehe auch

- „Funktionen des Sybase Central-Systemmonitors zum Überwachen von Statistiken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -k “ auf Seite 259
- „Datenbankserveroption -ksc “ auf Seite 264
- „Datenbankserveroption -ksd “ auf Seite 264

## Datenbankserveroption -ksc

Legt die maximale Anzahl von Verbindungen fest, die der Systemmonitor überwachen kann.

### Syntax

**dbsrv16 -ksc integer ...**

### Standardwert

10

### Gilt für

Windows

### Siehe auch

- „Funktionen des Sybase Central-Systemmonitors zum Überwachen von Statistiken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -k “ auf Seite 259
- „Datenbankserveroption -ks “ auf Seite 264
- „Datenbankserveroption -ksd “ auf Seite 264

## Datenbankserveroption -ksd

Legt die maximale Anzahl von Datenbanken fest, die der Systemmonitor überwachen kann.

**Syntax**

**dbsrv16 -ksd** *integer* ...

**Standardwert**

2

**Gilt für**

Windows

**Siehe auch**

- „Funktionen des Sybase Central-Systemmonitors zum Überwachen von Statistiken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -k “ auf Seite 259
- „Datenbankserveroption -ks “ auf Seite 264
- „Datenbankserveroption -ksc “ auf Seite 264

## Datenbankserveroption -m

Kürzt das Transaktionslog, wenn ein Checkpoint gesetzt wurde.

**Syntax**

**dbsrv16 -m** ...

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Diese Option kürzt das Transaktionslog, wenn ein Checkpoint ausgeführt wurde, entweder beim Herunterfahren, oder als Ergebnis eines vom Server geplanten Checkpoints.

**Vorsicht**

Wenn diese Option gewählt ist, gibt es keinen Schutz gegen Datenträgerausfall auf dem Gerät, das die Datenbankdatei enthält.

Mit dieser Option kann das Wachstum von Transaktionslogs automatisch begrenzt werden. Die Checkpoint-Häufigkeit wird weiterhin durch die Optionen `checkpoint_time` und `recovery_time` gesteuert (die Sie auch in der Befehlszeile setzen können).

Die Option `-m` ist sinnvoll für die Beschränkung der Größe des Transaktionslogs in Situationen, wenn Transaktionen mit hohem Volumen und kurzen Antwortzeiten verarbeitet werden und der Inhalt des Transaktionslogs für die Wiederherstellung oder Replikation nicht herangezogen wird. Die Option `-m` bietet eine Alternative für den Betrieb ganz ohne Transaktionslogs. In diesem Fall wäre nach jedem COMMIT ein Checkpoint erforderlich und die Performance würde entsprechend darunter leiden. Wenn die Option `-m` angegeben wurde, gibt es keinen Schutz bei einem Datenträgerausfall auf dem Gerät, auf dem sich die Datenbankdatei befindet. Andere Alternativen für die Verwaltung des Transaktionslogs (z.B.

mit der BACKUP-Anweisung und Ereignissen) sollten in Betracht gezogen werden, bevor Sie die Option -m verwenden.

Um Datenbankdatei-Fragmentierung zu vermeiden, wird empfohlen, das Transaktionslog beim Verwenden dieser Option auf ein anderes Gerät oder eine andere Partition als die Datenbank selbst zu legen.

Wenn diese Option verwendet wird, können keine Vorgänge verarbeitet werden, während ein Checkpoint ausgeführt wird.

**Vorsicht**

Verwenden Sie die Option -m nicht bei Datenbanken, die repliziert oder synchronisiert werden. SQL Remote und MobiLink stützen sich auf die Informationen aus dem Transaktionslog.

**Siehe auch**

- „Datenbankoption -m “ auf Seite 327
- „Das Transaktionslog“ auf Seite 135
- „Checkpoint-Logs“ auf Seite 143
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998
- „checkpoint\_time-Option“ auf Seite 588
- „recovery\_time-Option“ auf Seite 661

## Datenbankserveroption -n

Legt den Namen des Datenbankservers fest

**Syntax**

**dbsrv16 -n** *server-name database-filename ...*

**Standardwert**

Der Name der ersten Datenbankdatei (ohne Suchpfad und Erweiterung), die auf dem Datenbankserver gestartet wird.

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Wenn ein Datenbankserver startet, versucht er, auf diesem Computer zum Standarddatenbankserver zu werden. Der erste Datenbankserver der startet, wenn kein Standardserver vorhanden ist, wird zum Standarddatenbankserver. Shared Memory-Verbindungen auf diesem Computer, die nicht ausdrücklich einen Datenbankservernamen angeben, erfolgen mit dem Standardserver.

**Hinweis**

Es wird empfohlen, die Option -xd für Datenbankserver anzugeben, die von bereitgestellten Anwendungen verwendet werden, und dafür zu sorgen, dass alle Clients mit dem ServerName-Verbindungsparameter (Server) explizit den Namen des Datenbankservers angeben, mit dem sie sich verbinden sollen. Damit wird sichergestellt, dass die Datenbank mit dem richtigen Datenbankserver verbunden wird, wenn auf einem Computer mehrere Datenbankserver laufen.

Beim Servernamen wird keine Zeichensatzkonvertierung durchgeführt. Wenn der Client- und der Serverzeichensatz verschieden sind, kann die Verwendung von erweiterten Zeichen im Servernamen dazu führen, dass der Server nicht gefunden wird. Wenn Ihre Clients und Server auf unterschiedlichen Betriebssystemen oder in verschiedenen Sprachumgebungen laufen, sollten Sie 7-Bit-ASCII-Zeichen im Servernamen verwenden. Siehe „[Verbindungszeichenfolgen und Zeichensätze](#)“ auf Seite 503.

Datenbankservernamen müssen gültige Bezeichner sein. Lange Datenbankservernamen werden je nach Protokoll auf unterschiedliche Längen gekürzt. Datenbankservernamen dürfen Folgendes nicht:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola, Schrägstriche (/) oder Backslashes (\) enthalten.
- Sie dürfen nicht länger sein als 250 Byte.
- Sie dürfen keine Leerstellen enthalten, wenn sie unter Unix laufen.

**Hinweis**

Unter Windows und Unix können sich Clients der Version 9.0.2 und früher nicht mit Datenbankservern der Version 10.0.0 und höher verbinden, die längere Namen als die folgenden Längen haben:

- 40 Byte bei Shared Memory unter Windows
- 31 Byte bei Shared Memory unter Unix
- 40 Byte bei TCP/IP

Der Servername legt den Namen fest, der im Verbindungsparameter "ServerName" (Server) von Verbindungszeichenfolgen bei Clientanwendungen oder Profilen verwendet werden soll. Vorausgesetzt, es ist nicht -xd angegeben, wird bei Shared Memory ein Standarddatenbankserver verwendet, wenn kein Servername angegeben ist und wenn auf dem Computer mindestens ein Datenbankserver läuft.

Es wird nicht empfohlen, mehrere Datenbankserver mit demselben Namen zu betreiben.

**Hinweis**

Es gibt zwei Optionen -n. Die Option -n ist positionsabhängig. Wenn sie vor Datenbank-Dateinamen steht, ist sie eine Serveroption und benennt den Server. Wenn sie nach einem Datenbankdateinamen steht, ist sie eine Datenbankoption und benennt die Datenbank.

Der folgende Befehl benennt beispielsweise den Datenbankserver SERV und die Datenbank DATA:

```
dbsrv16 -n SERV sales.db -n DATA
```

Siehe „[Datenbankoption -n](#)“ auf Seite 328.

### Siehe auch

- „Bezeichner“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindungsparameter ServerName (Server)“ auf Seite 383
- „Datenbankservernamen und Datenbanknamen“ auf Seite 161
- „Datenbankserveroption -xd “ auf Seite 307

### Beispiel

Wenn der Datenbankserver mit der Datei `%SQLANYXSAMP16%\demo.db` gestartet und die Option `-n` nicht angegeben wird, ist der Name des Servers `demo`.

## Datenbankserveroption -o

Gibt alle Datenbankservermeldungen in das Datenbankserver-Meldungslog aus.

### Syntax

**dbsrv16 -o** *filename* ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Gibt alle Datenbankservermeldungen, einschließlich Informationsmeldungen, Fehlermeldungen, Warnmeldungen und Ausgaben der MESSAGE-Anweisung in die angegebene Datei und in das Meldungsfenster des Datenbankservers aus. Wenn Sie die Option `-qi` mit `-o` angeben, werden die Meldungen nur ins Datenbankserver-Meldungslog ausgegeben.

Es wird empfohlen, dass Sie den Dateinamen nicht mit `.log` abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

Führen Sie die folgende Anweisung aus, um den Namen der Datenbankserver-Meldungslogdatei zu ermitteln:

```
SELECT PROPERTY ( 'ConsoleLogFile' );
```

### Siehe auch

- ConsoleLogFile-Servereigenschaft auf Seite 748
- „Protokollieren von Datenbankserver-Aktionen“ auf Seite 163
- „Datenbankserveroption -oe “ auf Seite 269
- „Datenbankserveroption -on “ auf Seite 269
- „Datenbankserveroption -os “ auf Seite 270
- „Datenbankserveroption -ot “ auf Seite 271
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -qi “ auf Seite 273

## Datenbankserveroption -oe

Gibt einen Dateinamen zur Protokollierung von Startfehlern, schwerwiegenden Fehlern und Assertierungen an

### Syntax

**dbsrv16 -oe** *filename* ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Jede Zeile in der Ausgabelog-Datei hat ein Präfix mit Datum- und Zeitangabe. Zu den Startfehlern gehören folgende Fehler:

- Datenbankdatei konnte nicht geöffnet/gelesen werden: *Datenbankdatei*.
- Ein Datenbankserver mit diesem Namen wurde bereits gestartet.

Schwerwiegende Fehler und Assertierungen werden im Anwendungsereignisprotokoll von Windows (ausgenommen Windows Mobile) bzw. im Unix-Systemprotokoll protokolliert, unabhängig davon, ob -oe angegeben wurde.

Es wird empfohlen, dass Sie den Dateinamen nicht mit *.log* abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

### Siehe auch

- „Datenbankserveroption -o “ auf Seite 268
- „Datenbankserveroption -on “ auf Seite 269
- „Datenbankserveroption -os “ auf Seite 270
- „Datenbankserveroption -ot “ auf Seite 271
- „Datenbankserveroption -qi “ auf Seite 273

## Datenbankserveroption -on

Gibt eine maximale Größe für die Datenbankserver-Meldungslogdatei an, bei deren Erreichen die Datei mit der Erweiterung *.old* umbenannt und eine neue Datei gestartet wird.

### Syntax

**dbsrv16 -on** { *size* [ **k** | **m** | **g** ] } ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die *Größe* ist die maximale Dateigröße für das Meldungslog des Datenbankservers, in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit in kB, MB bzw. GB anzugeben. Die minimale Größenbegrenzung beträgt 10 kB. Standardmäßig gibt es keine maximale Größenbegrenzung.

Wenn das Datenbankserver-Meldungslog die angegebene Größe erreicht, benennt der Datenbankserver die Datei mit der Erweiterung *.old* um und legt eine neue mit demselben Namen an.

#### Hinweis

Wenn die *.old*-Datenbankserver-Meldungslogdatei bereits besteht, wird sie überschrieben. Um den Verlust von alten Datenbankserver-Meldungslogdateien zu verhindern, benutzen Sie lieber die Option *-os*.

Diese Option kann nicht mit der Option *-os* verwendet werden.

Es wird empfohlen, dass Sie den Namen der Datenbankserver-Nachrichtenlogdatei nicht mit *.log* abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

### Siehe auch

- [ConsoleLogMaxSize-Servereigenschaft auf Seite 748](#)
- [„Protokollieren von Datenbankserver-Aktionen“ auf Seite 163](#)
- [„Datenbankserveroption -o “ auf Seite 268](#)
- [„Datenbankserveroption -oe “ auf Seite 269](#)
- [„Datenbankserveroption -os “ auf Seite 270](#)
- [„Datenbankserveroption -ot “ auf Seite 271](#)
- [„sa\\_server\\_option-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Datenbankserveroption -os

Gibt eine Maximalgröße für die Datenbankserver-Meldungslogdatei an, bei der das Log umbenannt wird.

### Syntax

```
dbsrv16 -os { size[ k | m | g ] } ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

*Größe* ist die maximale Dateigröße für die Protokollierung von Meldungen des Datenbankservers, in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit in kB, MB bzw. GB anzugeben. Die minimale Größenbegrenzung beträgt 10 kB. Standardmäßig gibt es keine maximale Größenbegrenzung.

Bevor der Datenbankserver Ausgabemeldungen in der Datenbankserver-Meldungslogdatei protokolliert, prüft er die aktuelle Dateigröße. Wenn die Dateigröße aufgrund der Logmeldung den angegebenen Wert übersteigt, benennt der Datenbankserver die Datenbankserver-Meldungslogdatei in *jjmmttxx.slg* um, wobei *jjmmtt* das Datum (Jahr, Monat und Tag) darstellt, an dem die Datei erstellt wurde, und *xx* eine Zahl ist, die bei 00 beginnt und fortlaufend erhöht wird.

Mit dieser Option können Sie alte Datenbankserver-Meldungslogdateien identifizieren, die gelöscht werden können, um Festplattenspeicher freizugeben.

Diese Option kann nicht mit der Option `-on` verwendet werden.

Es wird empfohlen, dass Sie den Namen der Datenbankserver-Nachrichtenlogdatei nicht mit `.log` abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

#### Siehe auch

- „Protokollieren von Datenbankserver-Aktionen“ auf Seite 163
- „Datenbankserveroption `-o`“ auf Seite 268
- „Datenbankserveroption `-oe`“ auf Seite 269
- „Datenbankserveroption `-on`“ auf Seite 269
- „Datenbankserveroption `-ot`“ auf Seite 271

## Datenbankserveroption `-ot`

Kürzt die Meldungslogdatei des Datenbankservers und fügt anschließend Ausgabemeldungen an.

#### Syntax

```
dbsrv16 -ot logfile ...
```

#### Gilt für

Alle Betriebssysteme und Datenbankserver.

#### Bemerkungen

Die Funktion ist die gleiche wie bei der Option `-o`, außer dass die Datenbankserver-Meldungslogdatei gekürzt wird, bevor Meldungen darin eingetragen werden. Führen Sie die folgende Anweisung aus, um den Namen der Datenbankserver-Meldungslogdatei zu ermitteln:

```
SELECT PROPERTY ( 'ConsoleLogFile' );
```

Es wird empfohlen, dass Sie den Namen der Datenbankserver-Nachrichtenlogdatei nicht mit `.log` abschließen, weil dies zu Problemen bei Dienstprogrammen führen kann, die Vorgänge unter Verwendung des Transaktionslogs ausführen.

#### Siehe auch

- „Protokollieren von Datenbankserver-Aktionen“ auf Seite 163
- „Datenbankserveroption `-o`“ auf Seite 268
- „Datenbankserveroption `-oe`“ auf Seite 269
- „Datenbankserveroption `-on`“ auf Seite 269
- „Datenbankserveroption `-os`“ auf Seite 270

## Datenbankserveroption `-p`

Legt die Maximalgröße von Kommunikationspaketen fest

### Syntax

**dbsrv16 -p** *integer* ...

### Standardwert

7300 Byte (alle Betriebssysteme außer Windows Mobile)

1460 Byte (Windows Mobile)

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Der Mindestwert ist 500 Byte, der Maximalwert 65535.

Sie können die Größe des Kommunikationspuffers durch Einstellen des Verbindungsparameters CommBufferSize (CBSIZE) ändern.

### Siehe auch

- „Datenbankserveroption -pc“ auf Seite 272
- „Datenbankserveroption -pt“ auf Seite 273
- „Verbindungsparameter CommBufferSize (CBSIZE)“ auf Seite 343
- „Tipp: Paketgröße ändern, um die Performance zu steigern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -pc

Komprimiert alle Verbindungen, außer denen auf dem lokalen Computer

### Syntax

**dbsrv16 -pc** ...

### Gilt für

Alle Betriebssysteme und Netzwerkserver, außer Webserver

### Bemerkungen

Die zwischen einem Client und einem Datenbankserver gesendeten Pakete können mit der Option -pc komprimiert werden. Unter bestimmten Voraussetzungen kann das Komprimieren einer Verbindung die Performance verbessern. Umfangreiche Datenübertragungen mit stark komprimierbaren Daten erzielen im Allgemeinen die besten Komprimierungswerte. Dieser Parameter kann für einen bestimmten Client aufgehoben werden, indem Sie COMPRESS=NO in den Verbindungsparametern des Clients eingeben.

Standardmäßig werden Verbindungen nicht komprimiert. Wenn Sie den Parameter -pc angeben, werden alle Verbindungen komprimiert, außer Verbindungen auf demselben Computer, Webdienstverbindungen und TDS-Verbindungen. TDS-Verbindungen (einschließlich jConnect) unterstützen die Verbindungskomprimierung von nicht.

Verbindungen auf demselben Computer über eine beliebige Kommunikationsverbindung werden nicht komprimiert, auch wenn die Option -pc oder der Verbindungsparameter COMPRESS=YES verwendet wird.

**Siehe auch**

- „Datenbankserveroption -p “ auf Seite 271
- „Datenbankserveroption -pt “ auf Seite 273
- „Komprimierungseinstellungen für die Kommunikation“ auf Seite 112
- „Verbindungsparameter Compress (COMP)“ auf Seite 347
- „Tipp: Komprimierung mit Umsicht verwenden“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -pt

Erhöht oder verringert die Größenbegrenzung für die Komprimierung von Paketen.

**Syntax**

**dbsrv16** -pt *size* ...

**Standardwert**

120 Byte

**Gilt für**

Alle Betriebssysteme und Netzwerkservers

**Bemerkungen**

Als Parameter wird eine Ganzzahl akzeptiert, die für die Mindest-Byte-Anzahl von zu komprimierenden Paketen steht. Werte von unter 80 sind nicht empfehlenswert.

Unter gewissen Umständen kann die Änderung der Komprimierung die Performance einer komprimierten Verbindung verbessern, weil Sie festlegen können, dass nur die Pakete komprimiert werden, bei denen die Komprimierung zu einer Erhöhung der Übertragungsgeschwindigkeit führt. Die Standardeinstellungen sollten für die meisten Fälle geeignet sein.

Wenn Client und Server unterschiedliche Einstellungen für den Komprimierungsschwellenwert aufweisen, gelten die Clienteneinstellungen.

**Siehe auch**

- „Datenbankserveroption -p “ auf Seite 271
- „Datenbankserveroption -pc “ auf Seite 272
- „Komprimierungseinstellungen für die Kommunikation“ auf Seite 112
- „Verbindungsparameter CompressionThreshold (COMPTH)“ auf Seite 348
- „Tipp: Komprimierung mit Umsicht verwenden“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -qi

Steuert, ob das Taskleistensymbol und das Meldungsfenster des Datenbankservers angezeigt werden.

## Syntax

**dbsrv16 -qi ...**

## Gilt für

Windows

## Bemerkungen

Bei dieser Option gibt es nach dem Start keinen Hinweis darauf, dass der Server läuft, abgesehen von eventuellen Fehlermeldungen beim Start. Sie können die Logdateien von "-o" bzw. "-oe" verwenden, um Fehler zu diagnostizieren.

## Siehe auch

- „Datenbankserveroption -qn“ auf Seite 274
- „Datenbankserveroption -qp“ auf Seite 275
- „Datenbankserveroption -qs“ auf Seite 275
- „Datenbankserveroption -qw“ auf Seite 276
- „Datenbankserveroption -o“ auf Seite 268
- „Datenbankserveroption -oe“ auf Seite 269

## Datenbankserveroption -qn

Legt fest, dass das Meldungsfenster des Datenbankservers beim Starten nicht minimiert angezeigt wird.

## Syntax

**dbsrv16 -qn ...**

## Gilt für

Windows

Linux (wenn X Window-Server verwendet wird)

## Bemerkungen

Standardmäßig wird das Meldungsfenster des Datenbankservers automatisch minimiert, sobald der Datenbankserver-Start abgeschlossen ist. Wenn diese Option angegeben ist, wird das Meldungsfenster des Datenbankservers nicht minimiert, nachdem der Datenbankserver gestartet ist.

Das Meldungsfenster des Datenbankservers wird möglicherweise im Hintergrund angezeigt, wenn eine Anwendung den Datenbankserver automatisch startet, wobei die Anwendung nicht aktiv ist und "-qn" angegeben ist.

Unter Linux müssen Sie die Option -ux mit der Option -qn angeben (mithilfe von X Window-Server).

**Siehe auch**

- „Datenbankserveroption -ux “ auf Seite 302
- „Datenbankserveroption -qi “ auf Seite 273
- „Datenbankserveroption -qp “ auf Seite 275
- „Datenbankserveroption -qs “ auf Seite 275
- „Datenbankserveroption -qw “ auf Seite 276

**Beispiel**

Der folgende Befehl startet den Datenbankserver unter Linux oder Solaris, zeigt das Meldungsfenster des Datenbankservers an und minimiert das Meldungsfenster des Datenbankservers nicht, wenn der Datenbankserver gestartet ist:

```
dbsrv16 -ux -qn sample.db
```

## Datenbankserveroption -qp

Legt fest, dass keine Performance-Meldungen im Meldungsfenster des Datenbankservers angezeigt werden.

**Syntax**

```
dbsrv16 -qp ...
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Keine Performance-Meldungen im Meldungsfenster des Datenbankservers anzeigen. Die unterdrückten Meldungen sind:

- Kein eindeutiger Index oder Primärschlüssel für die Tabelle "*Tabellenname*"
- Datenbankdatei "*mydatabase.db*" besteht aus *nnn* Fragmenten

**Siehe auch**

- „Datenbankserveroption -qi “ auf Seite 273
- „Datenbankserveroption -qn “ auf Seite 274
- „Datenbankserveroption -qs “ auf Seite 275
- „Datenbankserveroption -qw “ auf Seite 276

## Datenbankserveroption -qs

Unterdrückt Fehlermeldungen beim Start.

**Syntax**

```
dbsrv16 -qs ...
```

### Gilt für

Windows

### Bemerkungen

Diese Option unterdrückt Fehlermeldungen beim Start. Fehlermeldungen beim Start können etwa beinhalten, dass der Datenbankserver eine Datenbankdatei nicht öffnen oder lesen kann oder dass ein Datenbankserver nicht startet, weil ein anderer Datenbankserver mit dem angegebenen Namen bereits läuft.

Wenn auf Windows-Plattformen der Server nicht automatisch gestartet wird, erscheinen diese Fehler in einem Fenster und müssen gelöscht werden, bevor der Server heruntergefahren wird. Diese Fenster erscheinen nicht, wenn die Option -qs benutzt wird.

Falls beim Laden der Sprachen-DLL ein Fehler auftritt, erscheint kein Fenster, wenn "-qs" in der Befehlszeile und nicht in @data angegeben wurde. Dieser Fehler wird nicht in den Logs der Optionen -o und -oe, sondern im Anwendungsereignisprotokoll von Windows (ausgenommen Windows Mobile) protokolliert.

Syntaxfehler werden unterdrückt, wenn "-qs" in der Befehlszeile und nicht in der @data-Erweiterung angegeben wurde.

### Siehe auch

- „Datenbankserveroption -qi“ auf Seite 273
- „Datenbankserveroption -qn“ auf Seite 274
- „Datenbankserveroption -qp“ auf Seite 275
- „Datenbankserveroption -qw“ auf Seite 276
- „Datenbankserveroption -o“ auf Seite 268
- „Datenbankserveroption -oe“ auf Seite 269

## Datenbankserveroption -qw

Legt fest, dass das Meldungsfenster des Datenbankservers nicht erscheint.

### Syntax

**dbsrv16 -qw ...**

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option unterdrückt das Meldungsfenster des Datenbankservers. Auf Windows-Plattformen ist das Taskleistensymbol des Datenbankservers im Infobereich weiterhin sichtbar. Sie können die Logdateien von "-o" bzw. "-oe" verwenden, um Fehler zu diagnostizieren.

**Siehe auch**

- „Datenbankserveroption -qi “ auf Seite 273
- „Datenbankserveroption -qn “ auf Seite 274
- „Datenbankserveroption -qp “ auf Seite 275
- „Datenbankserveroption -qs “ auf Seite 275

## Datenbankserveroption -r

Erzwingt, dass alle auf dem Datenbankserver gestarteten Datenbanken schreibgeschützt sind. Es sind keine Änderungen der Datenbanken zulässig. Der Datenbankserver ändert weder Datenbankdateien noch Transaktionslogdateien.

**Syntax**

**dbsrv16 -r ...**

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Öffnet alle Datenbankdateien schreibgeschützt, außer der temporären Datei, wenn der Parameter in der Befehlszeile vor dem Datenbanknamen angegeben wird. Wenn die Option -r nach einem Datenbanknamen angegeben wird, behandelt das System nur die betreffende Datenbank als schreibgeschützt. Sie können an temporären Tabellen Änderungen durchführen, aber ROLLBACK ist wirkungslos, weil die Transaktions- und Rollback-Logs deaktiviert sind.

Eine auf einer CD-ROM gelieferte Datenbank ist ein Beispiel für eine Datenbankdatei, die nicht geändert werden kann. Sie können auf diese Art von Datenbank nur im schreibgeschützten Modus zugreifen.

Wenn Sie versuchen, die Datenbank zu ändern, zum Beispiel mit einer INSERT- oder DELETE-Anweisung, wird ein `SQLSTATE_READ_ONLY_DATABASE`-Fehler ausgegeben.

Datenbanken, die eine Wiederherstellung erfordern, können nicht im schreibgeschützten Modus gestartet werden. Dies gilt zum Beispiel für Datenbankdateien, die unter Verwendung einer Online-Sicherung erstellt wurden: Sie können nicht im schreibgeschützten Modus gestartet werden, wenn beim Start der Sicherung offene Transaktionen vorhanden waren, da diese Transaktionen eine Wiederherstellung verlangen, sobald die Sicherungskopie gestartet wird.

Datenbanken mit aktiviertem Auditing können nicht im schreibgeschützten Modus gestartet werden.

Wenn Sie die Gültigkeit einer Sicherungskopie prüfen, muss die Datenbank schreibgeschützt ausgeführt werden, damit sie während der Prüfung nicht verändert werden kann. Siehe [„Datenbanken validieren \(Sybase Central\)“](#) auf Seite 1081.

### Siehe auch

- „Datenbankoption -r“ auf Seite 329
- „auditing-Option“ auf Seite 582
- „Datenbank-Deployment auf schreibgeschützten Datenträgern“ [*SQL Anywhere Server - Programmierung*]
- „Spezielle Betriebsmodi“ auf Seite 170

### Beispiel

Der folgende Befehl startet zwei Datenbanken im schreibgeschützten Modus.

```
dbsrv16 -r database1.db database2.db
```

Der folgende Befehl startet nur die erste von zwei Datenbanken im schreibgeschützten Modus.

```
dbsrv16 database1.db -r database2.db
```

## Datenbankserveroption -s

Legt die Benutzer-ID für Syslog-Nachrichten fest.

### Syntax

```
dbsrv16 -s { none | user | daemon | localn } ...
```

### Gilt für

Unix, Mac OS X

### Bemerkungen

Legt die Systembenutzer-ID fest, die in Nachrichten an die syslog-Funktion benutzt wird. Standardwert ist "user" für Datenbankserver, die im Vordergrund gestartet werden, und "daemon" für diejenigen, die im Hintergrund laufen (z.B. gestartet von "dbspawn", automatisch gestartet durch einen Client, gestartet mit der Datenbankserveroption -ud).

Ein Wert von "none" verhindert, dass Syslog-Nachrichten protokolliert werden. Mit dem Argument "localn" können Sie Meldungen anhand einer Facility-ID in eine Datei umleiten. Sie können für *n* eine Zahl zwischen 0 und 7 (inklusive) angeben. Weitere Informationen finden Sie in der Unix-Manpage "Syslog(3)".

### Siehe auch

- „MESSAGE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption -sb

Legt fest, wie der Datenbankserver auf Broadcasts reagiert.

### Syntax

```
dbsrv16 -sb { 0 | 1 } ...
```

## Gilt für

TCP/IP.

## Bemerkungen

Der Datenbankserver startet einen oder mehrere UDP-Listener, damit er auf drei Arten von Broadcasts antworten kann:

1. Clientverbindungs-Broadcasts, die nach diesem Server suchen.
2. Broadcasts zur Datenbankserver-Enumeration (z.B. solche vom Dienstprogramm dblocate oder vom **Assistenten "Server suchen"**, der zu den Administrationstools im Fenster **Verbinden** gehört).
3. Broadcasts von einem anderen Datenbankserver, der nach Datenbankservern mit demselben Namen sucht.

Bei Embedded SQL-Verbindungen bewirken das Dienstprogramm dblocate und die db\_locate\_servers-Funktion, dass Broadcast-Pakete auf lokalen Netzwerken ausgesendet werden, um alle Datenbankserver zu finden. Der UDP-Listener im Datenbankserver antwortet dann dem Absender mit Informationen dazu, wie eine Verbindung mit dem Datenbankserver hergestellt werden kann.

Die Option -sb steuert das Verhalten der UDP-Listener im Datenbankserver.

Wenn die Option -sb nicht angegeben wird, antwortet der Datenbankserver auf alle drei Arten von Anforderungen.

Wenn Sie -sb 0 angeben, antwortet der Datenbankserver nur auf (3). Dieses Verhalten zwingt Clients dazu, beim Verbinden mit dem Datenbankserver einen Host-Verbindungsparameter oder eine HOST-Protokolloption zu verwenden. Zusätzlich gilt: Wenn der Server einen anderen Port als den Standardport (2638) verwendet, muss der Client auch den Port des Servers angeben. Da der Datenbankserver nicht auf Broadcasts zur Datenbankserver-Enumeration antwortet, wird er nicht in die Ausgabe von dblocate aufgenommen.

Wenn Sie -sb 1 angeben, antwortet der Datenbankserver auf (1) und (3). Da der Datenbankserver nicht auf Broadcasts zur Datenbankserver-Enumeration antwortet, wird er nicht in die Ausgabe von dblocate aufgenommen.

## Siehe auch

- „BroadcastListener-Protokolloption (BLISTENER) (nur serverseitig)“ auf Seite 391
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- „Host-Verbindungsparameter“ auf Seite 363
- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399

## Datenbankserveroption -sbx

Legt die Sandboxing-Standardeinstellungen für alle auf dem Datenbankserver gestarteten Datenbanken fest, die keine expliziten Sandboxing-Einstellungen haben.

**Syntax**

**dbsrv16 -sbx**{ + | - } ...

**Standardwert**

Aus

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Diese Option legt die Sandboxing-Standardeinstellungen für alle auf dem Datenbankserver gestarteten Datenbanken fest, die keine expliziten Sandboxing-Einstellungen haben. Die Datenbankoption -sbx, mit der explizit Sandboxing-Einstellungen für eine Datenbank festgelegt werden, hebt die Datenbankserveroption -sbx auf.

Durch Aktivieren dieser Option werden die Dateivorgänge mit Lese- und Schreibzugriff für alle auf dem Datenbankserver laufenden Datenbanken auf das Verzeichnis beschränkt, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse.

Mithilfe der DiskSandbox-Option in der sa\_server\_option-Systemprozedur können Sie die Sandboxing-Standardeinstellungen für den Datenbankserver ändern, während der Datenbankserver läuft. Die sa\_server\_option-Systemprozedur hat keine Auswirkungen auf Datenbanken, die bereits auf dem Datenbankserver gestartet wurden, oder auf Datenbanken, die explizite Sandboxing-Einstellungen haben.

**Siehe auch**

- „Datenbankoption -sbx “ auf Seite 330
- „disk\_sandbox-Option“ auf Seite 608
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**Datenbankserveroption -sf**

Steuert, ob Benutzer Zugriff auf Funktionen für Datenbanken haben, die auf dem aktuellen Datenbankserver ausgeführt werden. Auf eine gesicherte Funktion können nur Benutzer mit entsprechenden Privilegien zugreifen, während bei einer nicht gesicherten Funktion alle Benutzer Zugriff haben.

**Syntax**

**dbsrv16 -sf** *feature-list* ...

*feature-list* :  
*feature-name* | *feature-set* [ ,*feature-name* | *feature-set* ] ...

Funktionsgruppe	Enthaltene Funktionen (Funktionsgruppen fett)
none	All features are unsecured except manage_features, manage_keys, and disk_sandbox.

<b>Funktionsgruppe</b>	<b>Enthaltene Funktionen (Funktionsgruppen fett)</b>
manage_server	<ul style="list-style-type: none"><li>• processor_affinity</li></ul>
manage_security	<ul style="list-style-type: none"><li>• manage_features</li><li>• manage_keys</li><li>• manage_disk_sandbox</li></ul>
server_security	<ul style="list-style-type: none"><li>• disk_sandbox</li><li>• trace_system_event</li></ul>

Funktionsgruppe	Enthaltene Funktionen (Funktionsgruppen fett)
all	<ul style="list-style-type: none"><li><b>client</b><ul style="list-style-type: none"><li>○ read_client_file</li><li>○ write_client_file</li></ul></li><li><b>remote</b><ul style="list-style-type: none"><li>○ remote_data_access</li><li>○ send_udp</li><li>○ send_email</li><li>○ web_service_client</li></ul></li><li><b>local</b><ul style="list-style-type: none"><li>○ <b>local_call</b><ul style="list-style-type: none"><li>● cmdshell</li><li>● external_procedure</li><li>● java</li></ul></li><li>○ <b>local_db</b><ul style="list-style-type: none"><li>● backup</li><li>● restore</li><li>● database</li><li>● dbspace</li></ul></li><li>○ <b>local_env</b><ul style="list-style-type: none"><li>● getenv</li></ul></li><li>○ <b>local_io</b><ul style="list-style-type: none"><li>● create_trace_file</li><li>● read_file</li><li>● write_file</li><li>● directory</li><li>● sp_list_directory</li><li>● sp_create_directory</li><li>● sp_copy_directory</li><li>● sp_move_directory</li><li>● sp_delete_directory</li><li>● sp_copy_file</li><li>● sp_move_file</li><li>● sp_delete_file</li></ul></li><li>○ <b>local_log</b></li></ul></li></ul>

Funktionsgruppe	Enthaltene Funktionen (Funktionsgruppen fett)
	<ul style="list-style-type: none"> <li>request_log</li> <li>console_log</li> <li>webclient_log</li> </ul>

### Parameter

- **none** Gibt an, dass keine Funktionen gesichert werden.
- **manage\_server** Verhindert für alle Datenbankserver-bezogenen Funktionen den Zugriff durch Benutzer. Diese Gruppe besteht aus den folgenden Funktionen:
  - **processor\_affinity** Verhindert, dass Benutzer die Prozessoraffinität (die Anzahl der genutzten logischen Prozessoren) des Datenbankservers ändern.
- **manage\_security** Hindert Benutzer am Zugriff auf Funktionen, mit denen die Sicherheit des Datenbankservers verwaltet werden kann. Diese Funktionen sind standardmäßig gesichert.
  - **manage\_features** Verhindert, dass Benutzer die Liste der Funktionen ändern, die auf dem Datenbankserver gesichert werden können.
  - **manage\_keys** Verhindert das Erstellen, Ändern, Löschen oder Auflisten von Schlüsseln für gesicherte Funktionen.  
  
Ein Benutzer, der Zugriff auf die manage\_keys-Funktion hat, aber nicht auf die manage\_features-Funktion, kann keine Schlüssel mit mehr gesicherten Funktionen definieren, als dem Benutzer zugeordnet sind.
  - **manage\_disk\_sandbox** Verhindert, dass Benutzer temporär Sandboxing-Einstellungen ändern, indem sie die Systemprozedur sa\_server\_option oder sa\_db\_option ausführen. Die gesicherte Funktion manage\_disk\_sandbox kann nicht für alle Datenbanken oder Benutzer deaktiviert werden. Sie kann nur mithilfe der sp\_use\_secure\_feature\_key-Systemprozedur für einzelne Verbindungen deaktiviert werden. Siehe „Datenbankserveroption -sbx “ auf Seite 279 oder „Datenbankoption -sbx “ auf Seite 330.
- **server\_security** Hindert Benutzer am Zugriff auf Funktionen, mit denen Sicherheitseinstellungen temporär umgangen werden können. Diese Funktionen sind standardmäßig gesichert.
  - **disk\_sandbox** Verhindert, dass Benutzer Dateivorgänge an der Datenbank mit Lese-/Schreibzugriff außerhalb des Verzeichnisses ausführen, in dem sich die Hauptdatenbankdatei befindet. Siehe „Datenbankserveroption -sbx “ auf Seite 279.
  - **trace\_system\_event** Hindert Benutzer am Erstellen von benutzerdefinierten Trace-Ereignissen. Siehe „Ereignisprotokollierung“ auf Seite 1101.
- **all** Hindert Benutzer am Zugriff auf die folgenden Gruppen:
  - **client** Hindert Benutzer am Zugriff auf alle Funktionen, mit denen auf die clientbezogene Ein- und Ausgabe zugegriffen werden kann. Diese Funktion steuert den Zugriff auf die Clientcomputerumgebung. Diese Gruppe besteht aus den folgenden Funktionen:

- **read\_client\_file** Verhindert die Verwendung von Anweisungen, die das Lesen einer Clientdatei bewirken können. Beispiel: Die READ\_CLIENT\_FILE-Funktion und die LOAD TABLE-Anweisung. Siehe „Zugriff auf Daten auf Clientcomputern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].
- **write\_client\_file** Verhindert die Verwendung aller Anweisungen, die das Schreiben in eine Clientdatei bewirken können. Beispiel: Die UNLOAD-Anweisung und die WRITE\_CLIENT\_FILE-Funktion. Siehe „Zugriff auf Daten auf Clientcomputern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].
- **remote** Hindert Benutzer am Zugriff auf alle Funktionen, die einen Fernzugriff oder eine Kommunikation mit entfernten Prozessen ermöglichen. Diese Gruppe besteht aus den folgenden Funktionen:
  - **remote\_data\_access** Verhindert die Verwendung von Ferndatenzugriffsdiensten, z.B. Proxytabellen.
  - **send\_udp** Verhindert, dass UDP-Pakete mit der sa\_send\_udp-Systemprozedur an eine angegebene Adresse gesendet werden können.
  - **send\_email** Verhindert die Verwendung von E-Mail-Systemprozeduren, z.B. xp\_sendmail.
  - **web\_service\_client** Verhindert die Verwendung von Aufrufen an gespeicherte Webdienst-Clientprozeduren (gespeicherte Prozeduren, die HTTP-Anforderungen absetzen).
- **local** Hindert Benutzer am Zugriff auf alle local-bezogenen Funktionen. Diese Funktion steuert den Zugriff auf die Servercomputerumgebung. Diese Gruppe besteht aus den Funktionsuntergruppen **local\_call**, **local\_db**, **local\_io** und **local\_log**.
  - **local\_call** Hindert Benutzer am Zugriff auf alle Funktionen, mit denen Code ausgeführt werden kann, der nicht direkt Teil des Datenbankservers ist und nicht vom Datenbankserver gesteuert wird. Diese Gruppe besteht aus den folgenden Funktionen:
    - **cmdshell** Verhindert die Verwendung der xp\_cmdshell-Prozedur. Siehe „xp\_cmdshell-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
    - **external\_procedure** Verhindert die Verwendung von externen gespeicherten Prozeduren. Diese Einstellung deaktiviert nicht die Verwendung der Systemprozeduren xp\_\* (wie z.B. xp\_cmdshell, xp\_readfile usw.), die in den Datenbankserver integriert sind. Getrennte Funktionskontrolloptionen werden für diese Systemprozeduren bereitgestellt. Siehe „SQL Anywhere-Schnittstelle für externe Aufrufe“ [*SQL Anywhere Server - Programmierung*].
    - **java** Verhindert die Verwendung von Java-bezogenen Funktionen, z.B. Java-Prozeduren. Siehe „Java in der Datenbank“ [*SQL Anywhere Server - Programmierung*].
  - **local\_db** Hindert Benutzer am Zugriff auf alle Funktionen im Zusammenhang mit Datenbankdateien. Diese Gruppe besteht aus den folgenden Funktionen:
    - **backup** Verhindert die Verwendung der BACKUP-Anweisung und damit die Möglichkeit, serverseitige Sicherungen auszuführen. Sie können weiterhin clientseitige

Sicherungen mithilfe des Dienstprogramms dbbackup durchführen. Siehe „[BACKUP-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

- **restore** Verhindert die Verwendung der RESTORE DATABASE-Anweisung. Siehe „[RESTORE DATABASE-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- **database** Verhindert die Verwendung der Anweisungen CREATE DATABASE, ALTER DATABASE, DROP DATABASE, CREATE ENCRYPTED FILE, CREATE DECRYPTED FILE, CREATE ENCRYPTED DATABASE und CREATE DECRYPTED DATABASE.
- **dbspace** Verhindert die Verwendung der Anweisungen CREATE DBSPACE, ALTER DBSPACE und DROP DBSPACE.
- **local\_env** Hindert Benutzer am Zugriff auf alle Funktionen im Zusammenhang mit Umgebungsvariablen. Diese Gruppe besteht aus den folgenden Funktionen:
  - **getenv** Verhindert, dass Benutzer die Werte von Umgebungsvariablen lesen. Siehe „[xp\\_getenv-Systemprozedur](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- **local\_io** Hindert Benutzer am Zugriff auf alle Funktionen, die direkten Zugriff auf Dateien und ihren Inhalt ermöglichen. Diese Gruppe besteht aus den folgenden Funktionen:
  - **create\_trace\_file** Verhindert die Verwendung von Anweisungen, mit denen ein Ereignisprotokollierungsziel erstellt wird. Siehe „[Ereignisprotokollierung](#)“ auf Seite 1101.
  - **read\_file** Verhindert die Verwendung von Anweisungen, die das Lesen einer lokalen Datei bewirken können. Beispiele hierfür sind die xp\_read\_file-Systemprozedur, die LOAD TABLE-Anweisung und die Verwendung von OPENSTRING( FILE... ). Die alternativen Namen load\_table und xp\_read\_file sind veraltet.
  - **write\_file** Verhindert die Verwendung aller Anweisungen, die das Schreiben in eine lokale Datei bewirken können. Beispiel: Die UNLOAD-Anweisung und die xp\_write\_file-Systemprozedur. Die alternativen Namen unload\_table und xp\_write\_file sind veraltet.
  - **delete\_file** Verhindert die Verwendung aller Anweisungen, die das Löschen einer lokalen Datei bewirken können. Das Sichern dieser Funktion bewirkt beispielsweise, dass das Dienstprogramm dbbackup fehlschlägt, wenn die Option -x oder -xo angegeben wird.
  - **directory** Verhindert die Verwendung von Proxytabellen der directory-Klasse. Diese Funktion wird deaktiviert, wenn remote\_data\_access deaktiviert ist.
  - **sp\_list\_directory** Verhindert die Verwendung der sp\_list\_directory-Systemprozedur.
  - **sp\_create\_directory** Verhindert die Verwendung der sp\_create\_directory-Systemprozedur.
  - **sp\_copy\_directory** Verhindert die Verwendung der sp\_copy\_directory-Systemprozedur.

- **sp\_move\_directory** Verhindert die Verwendung der sp\_move\_directory-Systemprozedur.
- **sp\_delete\_directory** Verhindert die Verwendung der sp\_delete\_directory-Systemprozedur.
- **sp\_copy\_file** Verhindert die Verwendung der sp\_copy\_file-Systemprozedur.
- **sp\_move\_file** Verhindert die Verwendung der sp\_move\_file-Systemprozedur.
- **sp\_delete\_file** Verhindert die Verwendung der sp\_delete\_file-Systemprozedur.
- **local\_log** Hindert Benutzer am Zugriff auf alle Protokollierungsfunktionen, die dazu führen, dass Daten direkt in einer Datei auf der Festplatte erstellt oder in diese geschrieben werden. Diese Gruppe besteht aus den folgenden Funktionen:
  - **request\_log** Verhindert, dass der Name der Anforderungs-Logdatei geändert werden kann sowie die Grenzwerte für die Größe der Anforderungs-Logdatei oder die Anzahl der Dateien erhöht werden können. Sie können die Anforderungs-Logdatei und die Grenzwerte für diese Datei im Befehl zum Starten des Datenbankservers angeben. Nach dem Starten des Datenbankservers können die Angaben jedoch nicht mehr geändert werden. Wenn Anforderungslog-Funktionen deaktiviert sind, können Sie trotzdem die Anforderungsprotokollierung aktivieren bzw. deaktivieren sowie die maximale Dateigröße und die Anzahl der Dateien für die Anforderungsprotokollierung verringern. Siehe [„Anforderungsprotokollierung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).
  - **console\_log** Verhindert, dass der Dateiname des Datenbankserver-Meldungslogs mit der ConsoleLogFile-Option der sa\_server\_option-Systemprozedur geändert werden kann. Durch das Sichern dieser Option wird außerdem verhindert, dass die maximale Größe der Logdatei mit der ConsoleLogMaxSize-Option der sa\_server\_option-Systemprozedur erhöht werden kann. Sie können eine Serverlogdatei und ihre Größe angeben, wenn Sie den Datenbankserver starten.
  - **webclient\_log** Verhindert, dass der Dateiname des Webdienst-Clientlogs mit der WebClientLogFile-Option der sa\_server\_option-Systemprozedur geändert werden kann. Sie können eine Webdienst-Clientlogdatei angeben, wenn Sie den Datenbankserver starten. Siehe [„Datenbankserveroption -zoc“ auf Seite 315](#).

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Mit dieser Option kann der Eigentümer des Datenbankservers steuern, ob Benutzer Zugriff auf Funktionen für auf dem Datenbankserver laufende Datenbanken haben. Mit der Option -sk kann der Eigentümer des Datenbankservers einen Systemschlüssel für gesicherte Funktionen erstellen, der verhindert, dass Benutzer auf durch die Option -sf angegebene Funktionen zugreifen.

Wenn Sie eine Datenbank starten, ohne einen Systemschlüssel für gesicherte Funktionen anzugeben, sind die standardmäßig gesicherten Funktionen gesichert und Sie können die Einstellungen für gesicherte

Funktionen weder für den Datenbankserver noch für darauf laufende Datenbanken ändern. Sie können den Systemschlüssel für gesicherte Funktionen nicht später erstellen, sondern müssen den Datenbankserver herunterfahren und beim Neustart einen Systemschlüssel für gesicherte Funktionen angeben.

Die *feature-list* ist eine kommagetrennte Liste von Funktionsnamen oder Funktionsgruppen, die für den Datenbankserver gesichert werden sollen. Durch Sichern einer Funktion ist diese für alle Datenbankbenutzer außer Administratoren nicht mehr verfügbar. Wenn Sie eine Funktionsgruppe angeben, werden alle Funktionen in der Gruppe gesichert. Um eine oder mehrere, aber nicht alle Funktionen in der Funktionsgruppe zu sichern, müssen Sie die einzelnen Funktionsnamen angeben.

#### Hinweis

Bei Unterfunktionen von Funktionsgruppen, die standardmäßig gesichert sind, kann die Sicherung nicht über die Befehlszeile aufgehoben werden. Das bedeutet, dass der folgende Befehl nicht funktioniert:

```
-sf manage_security, -manage_keys
```

Sie können mit *feature-name* angeben, dass die Funktion gesichert werden (somit nicht mehr verfügbar sein) soll, sowie mit *-feature-name* oder *feature-name-*, dass die Funktion nicht gesichert werden (für alle Datenbankbenutzer verfügbar sein) soll. Der folgende Befehl gibt beispielsweise an, dass nur DBSpace-Funktionen für alle Benutzer verfügbar sind:

```
dbsrvl6 -n secure_server -sf all,-dbspace
```

#### Siehe auch

- „Gesicherte Funktionen“ auf Seite 1413
- „Datenbankserveroption -sk “ auf Seite 288
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415
- „sp\_create\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_alter\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_list\_secure\_feature\_keys-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_drop\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_use\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

#### Beispiel

Der folgende Befehl startet einen Datenbankserver namens *secure\_server*, der Zugriff auf das Anforderungslog hat und bei dem alle Ferndatenzugriffsfunktionen gesichert sind. Der durch die Option -sk angegebene Schlüssel kann später mit der *sp\_use\_secure\_feature\_key*-Systemprozedur verwendet werden, um diese Funktionen für alle Benutzer in der aktuellen Verbindung verfügbar zu machen.

```
dbsrvl6 -n secure_server -sf remote,-request_log -sk j978kls12
```

Wenn ein Benutzer, der mit einer auf dem Datenbankserver *secure\_server* laufenden Datenbank verbunden ist, die *sp\_use\_secure\_feature\_key*-Systemprozedur verwendet und dabei den *authorization\_key*-Parameter auf denselben Wert setzt wie durch die Option -sk angegeben, hat diese Verbindung Zugriff auf die Ferndatenzugriffsfunktionen:

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

Mit dem folgenden Befehl werden alle Funktionen gesichert, ausgenommen lokale Datenbankfunktionen:

```
dbsrv16 -n secure_server -sf all,-local_db
```

## Datenbankserveroption -sk

Gibt einen Systemschlüssel für gesicherte Funktionen an, mit dessen Hilfe Zugriff auf Funktionen gewährt werden kann, die für den Datenbankserver gesichert sind.

### Syntax

```
dbsrv16 -sk key ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn Sie Funktionen für einen Datenbankserver mithilfe der Option -sf sichern, können Sie gleichzeitig mit der Option -sk einen Schlüssel angeben, der mit der `sp_use_secure_feature_key`-Systemprozedur verwendet werden kann, um für eine Verbindung Zugriff auf gesicherte Funktionen zu gewähren. Diese Verbindung kann auch die `sa_server_option`-Systemprozedur verwenden, um Funktionen oder Funktionsgruppen zu ändern, die für alle auf dem Datenbankserver laufenden Datenbanken gesichert sind.

Der Schlüssel muss eine nicht leere Zeichenfolge aus mindestens sechs Zeichen sein und darf keine Anführungszeichen, Steuerzeichen (alle Zeichen unter 0x20) oder Backslashes enthalten. Die Anzahl der Schlüssel für gesicherte Funktionen ist auf 1000 pro Datenbank begrenzt.

Wenn der `authorization_key`-Parameter der `sp_use_secure_feature_key`-Systemprozedur auf einen anderen als den durch -sk angegebenen Wert gesetzt ist, wird kein Fehler ausgegeben und die durch -sf angegebenen Funktionen bleiben für die Verbindung gesichert.

Wenn Sie -sk ohne -sf angeben, werden nur die standardmäßig gesicherten Funktionen aktiviert, aber Sie können mithilfe des Systemschlüssels für gesicherte Funktionen die Einstellungen für gesicherte Funktionen ändern, während der Datenbankserver läuft.

### Siehe auch

- „Datenbankserveroption -sf“ auf Seite 280
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sp\_use\_secure\_feature\_key-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415

### Beispiel

Der folgende Befehl startet einen Datenbankserver namens `secure_server`, bei dem die Sicherungsfunktionen gesichert sind. Der durch die Option -sk angegebene Schlüssel kann später verwendet werden, um Zugriff auf diese Funktionen für eine bestimmte Verbindung zu gewähren.

```
dbsrv16 -n secure_server -sf backup -sk j978kls12
```

Wenn Sie den `authorization_key`-Parameter für eine Verbindung mit einer auf dem Datenbankserver `secure_server` laufenden Datenbank auf den durch `-sk` angegebenen Wert setzen, können über diese Verbindung Sicherungen durchgeführt oder die auf dem Datenbankserver `secure_server` gesicherten Funktionen geändert werden:

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

Der Benutzer kann dann alle Funktionen für auf dem Datenbankserver `secure_server` laufende Datenbanken sichern, indem er die folgende Anweisung ausführt:

```
CALL sa_server_option( 'SecureFeatures', 'all' );
```

## Datenbankserveroption -su

Legt das Kennwort für den DBA-Benutzer der Dienstprogrammdateiabank (`utility_db`) fest oder deaktiviert Verbindungen zur Dienstprogrammdateiabank

### Syntax

```
dbsrv16 -su password ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option gibt das Ausgangskennwort für den DBA-Benutzer der Dienstprogrammdateiabank an. Bei Kennwörtern wird die Groß- und Kleinschreibung berücksichtigt. Sie können **none** für das Kennwort angeben, um alle Verbindungen mit der Dienstprogrammdateiabank zu deaktivieren.

- Wenn Sie einen Personal Datenbankserver verwenden und die Option `-su` nicht angeben, können Verbindungen zur Dienstprogrammdateiabank mit der DBA-Benutzer-ID und jedem beliebigen Kennwort hergestellt werden. Es wird angenommen, dass jeder Benutzer, der eine Verbindung mit dem Personal Datenbankserver herstellen kann, direkten Zugriff auf das Dateisystem hat. Daher wird nicht versucht, Benutzer über Kennwörter zu filtern.
- Wenn Sie einen Netzwerk-Datenbankserver verwenden und die Option `-su` nicht angeben, sind Verbindungen zur Dienstprogrammdateiabank nicht zulässig, außer die `util_db.ini`-Datei ist vorhanden und die Benutzer-ID ist DBA mit einem Kennwort, das dem Kennwort in der `util_db.ini`-Datei entspricht. Wenn auf einem Netzwerkserver sowohl `-su` und `util_db.ini` verwendet werden, wird `util_db.ini` ignoriert. Die Datei `util_db.ini` wird nicht mehr empfohlen.

Die Festlegung eines Kennworts für die Dienstprogrammdateiabank eines Netzwerk-Datenbankservers ist in den Fällen nützlich, in denen der Datenbankserver läuft, aber eine Verbindung mit der Datenbank nicht hergestellt werden kann. Beispiel: In einem Spiegelungssystem können Sie eine Verbindung mit der Dienstprogrammdateiabank herstellen, um den Datenbankserver herunterzufahren oder notfalls erzwingen, dass der Spiegelserver zum Primärserver wird. Siehe [„Einen Datenbankserver in einem Spiegelungssystem stoppen“ auf Seite 1490](#) und [„Fehlerbehandlung: Primärserver kann nicht neu gestartet werden“ auf Seite 1500](#).

Sie können die Anweisung `CREATE USER DBA IDENTIFIED BY neues_Kennwort` ausführen, während Sie mit `utility_db` verbunden sind, um das Kennwort für den DBA-Benutzer der Dienstprogrammdatenbank zu ändern. Die `REVOKE CONNECT FROM DBA`-Anweisung kann verwendet werden, um Verbindungen mit der `utility_db`-Datenbank zu deaktivieren. Nicht alle SQL-Anweisungen werden für die Dienstprogrammdatenbank unterstützt.

Um zu vermeiden, dass das Kennwort der Dienstprogrammdatenbank in lesbarer Form in der Befehlszeile erscheint, können Sie mithilfe des Dienstprogramms `dbfhide` eine das Kennwort enthaltende Datei verschleiern und anschließend die verschleierte Datei in der Befehlszeile referenzieren.

### Siehe auch

- „Die Dienstprogrammdatenbank“ auf Seite 145
- Zulässige Anweisungen für die Dienstprogrammdatenbank auf Seite 146
- „Verbindung mit der Dienstprogrammdatenbank herstellen“ auf Seite 147
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm zum Verschleiern von Dateien (`dbfhide`)“ auf Seite 922
- „CREATE USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

### Beispiel

Der folgende Befehl deaktiviert alle Verbindungen zur Dienstprogrammdatenbank:

```
dbsrv16 -su none c:\inventory.db
```

Im folgenden Beispiel wird die Datei namens `util_db_pwd.cfg`, die das Kennwort der Dienstprogrammdatenbank enthält, mithilfe von `"dbfhide"` verschleiert und in `util_db_pwd_hide.cfg` umbenannt:

```
dbfhide util_db_pwd.cfg util_db_pwd_hide.cfg
```

Die Datei `util_db_pwd_hide.cfg` kann nun verwendet werden, um das Kennwort der Dienstprogrammdatenbank anzugeben:

```
dbsrv16 -su @util_db_pwd_hide.cfg -n my_server c:\inventory.db
```

## Datenbankserveroption `-tdsl`

Legt den Login-Modus TDS fest.

### Syntax

```
dbsrv16 -tdsl { all | RSA | RSANonce }...
```

### Standardwert

`all`

### Gilt für

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Diese Option beschränkt den Typ der TDS-Login-Anforderungen, die der Datenbankserver unterstützt.

Modustyp	Beschreibung
alle	Verschlüsselte und unverschlüsselte Kennwörter (einschließlich solcher mit Nonce) sind in TDS-Login-Anforderungen zulässig:
RSA	Nur RSA-verschlüsselte Kennwörter (einschließlich solcher mit Nonce) sind in TDS-Login-Anforderungen zulässig:
RSANonce	Nur RSA-verschlüsselte Kennwörter mit Nonce sind in TDS-Login-Anforderungen zulässig:

Wenn Sie über eine TDS-Anwendung, die RSA ohne Nonce unterstützt, Login-Anforderungen erstellen, generiert der Datenbankserver neue Chiffrierschlüssel für die Login-Anforderungen. Das Generieren neuer Chiffrierschlüssel kann zeitaufwändig sein.

Wenn Sie über eine TDS-Anwendung, die RSA mit Nonce unterstützt, Login-Anforderungen erstellen, verwendet der Datenbankserver vorhandene RSA-Chiffrierschlüssel erneut. Diese Chiffrierschlüssel werden alle 24 Stunden neu generiert. Durch die Wiederverwendung der RSA-Chiffrierschlüssel kann die Performance verbessert werden, während der Datenbankserver gegen Wiedergabeangriffe geschützt wird.

Sowohl jConnect als auch Open Client unterstützen RSA-Login-Anforderungen mit und ohne Nonce.

**Siehe auch**

- [Tabular Data Stream \(TDS\) auf Seite 1569](#)

**Datenbankserveroption -ti**

Trennt inaktive Verbindungen

**Syntax**

**dsrv16 -ti** *minutes* ...

**Standardwert**

240 (4 Stunden)

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Trennt Verbindungen, die seit der angegebenen Anzahl von *Minuten* keine Anforderung gesendet haben. Der Höchstwert ist 32767. Ein Clientsystem hält während einer Datenbanktransaktion Sperren aufrecht, bis die Transaktion abgeschlossen ist oder die Verbindung beendet wird. Die Option -ti dient dazu, inaktive Verbindungen zu trennen, damit deren Sperren aufgehoben werden.

Die Option `-ti` ist sinnvoll, wenn sie in Verbindung mit `"dbsrv16"` eingesetzt wird, weil die meisten Verbindungen über Netzwerkverbindungen (TCP) erfolgen).

Die Option `-ti` ist mit `dbeng16` nur für lokale TCP/IP-Verbindungen sinnvoll. Die Verwendung von `-ti` hat keine Auswirkung auf Shared Memory-Verbindungen mit einem Personal Server, aber Sie können ein Timeout für die Verbindung angeben, das für Shared Memory-Verbindungen gilt. Standardmäßig wird vom Personal Datenbankserver TCP/IP nicht gestartet. Siehe „[Datenbankserveroption -x](#)“ auf Seite 305.

Das Einstellen des Werts auf Null deaktiviert die Suche nach inaktiven Verbindungen, daher werden keine Verbindungen getrennt. Wenn der Idle-Verbindungsparameter nicht verwendet wird, hängt der Inaktivitäts-Timeoutwert für TCP/IP-Verbindungen von der Datenbankserveroption `-ti` ab. Wenn die Datenbankserveroption `-ti` und der Idle-Verbindungsparameter angegeben werden, hängt der Inaktivitäts-Timeoutwert vom Verbindungsparameter ab.

### Siehe auch

- [IdleTimeout-Servereigenschaft auf Seite 751](#)
- [„Datenbankserveroption -tl“ auf Seite 292](#)
- [„sa\\_server\\_option-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Timeoutwerte anpassen“ auf Seite 1114](#)
- [„Verbindungsparameter Idle“ auf Seite 365](#)

## Datenbankserveroption -tl

Stellt das Intervall ein, in dem Verfügbarkeitspakete versendet werden sollen

### Syntax

**dbsrv16 -tl** *seconds* ...

### Gilt für

Alle Datenbankserver, die TCP/IP verwenden.

### Bemerkungen

Ein Verfügbarkeitspaket wird regelmäßig über ein Client/Server TCP/IP-Kommunikationsprotokoll gesendet, um zu bestätigen, dass eine Verbindung besteht. Wenn der Server während einer LivenessTimeout-Periode (Standard 2 Minuten) läuft, ohne ein Verfügbarkeitspaket zu erhalten, wird die Kommunikation getrennt und der Server löscht die diesem Client zugeordnete Verbindung. Unix-Clients ohne Threading und TDS-Verbindungen führen keine Überprüfung mit Verfügbarkeitspaketen durch.

Die Option `-tl` auf dem Server legt den Wert für LivenessTimeout für alle Clients fest, für die keine Verfügbarkeitsperiode angegeben wurde.

Verfügbarkeitspakete werden gesendet, wenn eine Verbindung während eines bis zwei Dritteln der LivenessTimeout-Periode keine Pakete übertragen hat.

Wenn mehr als 200 Verbindungen vorhanden sind, berechnet der Server automatisch einen höheren LivenessTimeout-Wert basierend auf dem ermittelten LivenessTimeout-Wert, damit der Server eine große Anzahl von Verbindungen effizienter abwickeln kann. Verfügbarkeitspakete werden zwischen einem

Drittel und zwei Dritteln der LivenessTimeout-Periode auf jeder stillstehenden Verbindung gesendet. Eine große Anzahl von Verfügbarkeitspaketen wird nicht gleichzeitig gesendet. Verfügbarkeitspakete, deren Versendung viel Zeit in Anspruch nimmt, könnten nach Ablauf von zwei Dritteln der LivenessTimeout-Zeit versendet werden. Eine Warnung erscheint im Datenbankserver-Meldungslog, wenn die Netzverfügbarkeits-Sendungen lange Zeit benötigen. Wenn diese Warnung erscheint, sollten Sie den LivenessTimeout-Wert erhöhen.

Obwohl dies im Allgemeinen nicht empfohlen wird, können Sie die Verfügbarkeitsprüfung wie folgt deaktivieren:

```
dbsrv16 -tl 0 -n my_server
```

Anstatt die LivenessTimeout-Option zu deaktivieren, sollten Sie den Wert folgendermaßen auf eine Stunde erhöhen:

```
dbsrv16 -tl 3600 -n my_server
```

### Siehe auch

- [LivenessTimeout-Servereigenschaft auf Seite 753](#)
- [„Datenbankserveroption -ti “ auf Seite 291](#)
- [„sa\\_server\\_option-Systemprozedur“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [„Timeoutwerte anpassen“ auf Seite 1114](#)

## Datenbankserveroption -tmf

Erzwingt die Transaktions-Manager-Wiederherstellung bei verteilten Transaktionen.

### Syntax

```
dbsrv16 -tmf ...
```

### Gilt für

Windows.

### Bemerkungen

Diese Option wird während der Wiederherstellung von verteilten Transaktionen verwendet, wenn der Koordinator für verteilte Transaktionen nicht zur Verfügung steht. Wenn DTC nicht geladen werden kann, werden die ausstehenden Vorgänge zurückgesetzt und die Wiederherstellung wird fortgesetzt. Sie kann auch verwendet werden, wenn eine Datenbank mit verteilten Transaktionen im Transaktionslog auf einer Plattform gestartet wird, auf der DTC nicht verfügbar ist.

#### **Vorsicht**

Wenn Sie diese Option verwenden, werden verteilte Transaktionen nicht korrekt wiederhergestellt. Diese Option ist nicht für Routineanwendungen gedacht.

### Siehe auch

- [„Datenbankserveroption -tmt “ auf Seite 294](#)
- [„Wiederherstellung nach verteilten Transaktionen“ \[\*SQL Anywhere Server - Programmierung\*\]](#)

## Datenbankserveroption -tmt

Legt ein Wiederaufnahme-Timeout bei der Teilnahme an verteilten Transaktionen fest.

### Syntax

**dbsrv16 -tmt** *milliseconds* ...

### Gilt für

Windows.

### Bemerkungen

Wird während der Wiederherstellung von verteilten Transaktionen verwendet. Der Wert legt fest, wie lange der Datenbankserver warten soll, um wieder aufgenommen zu werden. Standardmäßig gibt es kein Timeout. (Der Datenbankserver wartet unbegrenzt.)

### Siehe auch

- „Datenbankserveroption -tmf“ auf Seite 293
- „Wiederherstellung nach verteilten Transaktionen“ [[SQL Anywhere Server - Programmierung](#)]

## Datenbankserveroption -tq

Führt den Server zu einem festgelegten Zeitpunkt herunter.

### Syntax

**dbsrv16 -tq** { *datetime* | *time* } ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option ist beim Einrichten von automatischen Sicherungsprozeduren nützlich. Siehe „[Sicherung und Datenwiederherstellung](#)“ auf Seite 1027.

Das Format für die Uhrzeit ist *hh:mm* (24 Stunden). Optional kann ein Datum vorangestellt werden. Wenn ein Datum angegeben wird, müssen Datum und Uhrzeit in Anführungszeichen gesetzt werden und das Format *YYYY/MM/DD HH:MM* aufweisen.

### Siehe auch

- [QuittingTime-Servereigenschaft](#) auf Seite 759
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Datenbankserveroption -ts

Richtet eine Datenbankserver-Protokollierungssitzung ein.

**Syntax**

**dbsrv16 -ts** *session-name* ( *session-option=option-value* [ ;... ] )

Sitzungsoption	Optionswert
<b>events</b>	Kommagetrennte Liste der System-Trace-Ereignisse. Rufen Sie die <code>sp_trace_events</code> -Systemprozedur auf, um eine Liste der systemdefinierten Trace-Ereignisse abzurufen. Siehe „ <a href="#">sp_trace_events-Systemprozedur</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>targets</b>	<i>Zieltyp</i> ( <i>Zieloption=Wert</i> [ ;... ] ), wobei <i>Zieltyp</i> nur <b>file</b> sein kann.

Die Zieldatei kann die folgenden Optionen aufweisen:

Zieloption	Optionswert
<b>filename_prefix</b>	Ein ETD-Dateinamenpräfix mit oder ohne Pfad. Alle ETD-Dateien haben die Erweiterung <i>.etd</i> . Dieser Parameter ist erforderlich.
<b>max_size</b>	Die maximale Größe der Datei in Byte. Der Standardwert ist 0, was bedeutet, dass es keine Grenze für die Dateigröße gibt und die Datei größer wird, solange Speicherplatz verfügbar ist. Sobald die angegebene Größe erreicht ist, wird eine neue Datei gestartet.
<b>num_files</b>	Die Anzahl der Dateien, in die Informationen zur Ereignisprotokollierung geschrieben werden. Diese Option wird nur verwendet, wenn <code>max_size</code> eingestellt ist. Wenn alle Dateien die maximale angegebene Größe erreichen, beginnt der Datenbankserver, die älteste Datei zu überschreiben.
<b>flush_on_write</b>	Ein Wert, der steuert, ob Festplattenpuffer für jedes protokollierte Ereignis geleert werden. Die Werte YES, TRUE, NO und FALSE werden akzeptiert. Der Standardwert ist FALSE. Bei aktiviertem Parameter kann die Performance des Datenbankservers vermindert sein, wenn viele Trace-Ereignisse protokolliert werden.
<b>compressed</b>	Ein Wert, der die Komprimierung der ETD-Datei zum Einsparen von Speicherplatz steuert. Die Werte "on" und "off" werden akzeptiert. Der Standardwert ist "off".

**Gilt für**

Alle Betriebssysteme und Datenbankserver, ausgenommen SAP Sybase IQ-Datenbankserver.

**Bemerkungen**

Server-Trace-Ereignissitzungen können verwendet werden, um Trace-Ereignisse in Bezug auf das Systemverhalten oder für einen bestimmten Benutzer zu erfassen. Server-Trace-Ereignissitzungen werden im Speicher gespeichert und werden beim Stoppen des Datenbankservers gelöscht, sofern sie nicht explizit gelöscht wurden.

### Siehe auch

- „Ereignisprotokollierung“ auf Seite 1101
- „CREATE TEMPORARY TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE TEMPORARY TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „NOTIFY TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_events-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_fields-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_sessions-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_events-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_targets-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_target\_options-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm für die Verwaltung von ETD-Dateien (dbmanageetd)“ auf Seite 918
- „Systemereignisse“ auf Seite 1091
- „Datenbankserveroption -sf “ auf Seite 280

## Datenbankserveroption -u

Öffnet Dateien, wobei der Festplattencache des Betriebssystems verwendet wird

### Syntax

**dbsrv16 -u ...**

### Gilt für

Windows, Unix.

### Bemerkungen

Dateien werden geöffnet, indem der Festplattencache des Betriebssystems zusätzlich zum Datenbankcache verwendet wird.

Während die Leistung des Festplattencaches des Betriebssystems verbessert werden kann, wird eine bessere Performance häufig dadurch erreicht, dass nur der Datenbankcache verwendet wird.

Wenn der Server auf einem ausschließlich für ihn vorgesehenen Computer läuft, sollten Sie nicht die Option -u verwenden, da der Datenbankcache allein normalerweise effizienter ist. Es kann sinnvoll sein, die Option -u zu verwenden, wenn der Server auf einem Computer mit mehreren anderen Anwendungen läuft (sodass ein umfangreicher Datenbankcache andere Anwendungen möglicherweise beeinträchtigt), und dennoch I/O-intensive Tasks auf dem Server zeitweilig ausgeführt werden (sodass ein umfangreicher Cache die Performance erhöht).

## Datenbankserveroption -ua

Deaktiviert die Verwendung von asynchronen I/O-Vorgängen

### Syntax

**dbsrv16 -ua ...**

### Gilt für

Linux

### Bemerkungen

Standardmäßig verwendet der Datenbankserver unter Linux asynchrone I/O-Vorgänge, sofern möglich. Zum Ausführen von asynchronen I/O-Vorgängen müssen die folgenden Bedingungen erfüllt sein:

1. Die Bibliothek *libaio.so* kann während der Laufzeit geladen werden.
2. Der Kernel unterstützt asynchrone I/O-Vorgänge.

Wenn Sie die Verwendung asynchroner I/O-Vorgänge deaktivieren möchten, geben Sie die Datenbankserveroption -ua an.

## Datenbankserveroption -uc

Startet den Datenbankserver im Shell-Modus. Dies ist die Standardeinstellung.

### Syntax

**dbsrv16 -uc ...**

### Gilt für

Unix, Mac OS X

### Bemerkungen

Startet den Datenbankserver im Shell-Modus. Sie können nur jeweils eine der Optionen -uc, -ui, -um oder -ux angeben. Wenn Sie -uc angeben, wird der Datenbankserver auf dieselbe Weise wie bei früheren Versionen der Software gestartet.

Weitere Informationen zum Starten des Datenbankservers als Daemon finden Sie unter [„Datenbankserveroption -ud“](#) auf Seite 298.

### Siehe auch

- [„Datenbankserveroption -ui“](#) auf Seite 300
- [„Datenbankserveroption -um“](#) auf Seite 300
- [„Datenbankserveroption -ux“](#) auf Seite 302

## Datenbankserveroption -ud

Führt den Datenbankserver als Daemon aus.

### Syntax

**dbsrv16 -ud ...**

### Gilt für

Unix, Mac OS X

### Bemerkungen

Mit dieser Option können Sie den Server so ausführen, dass er weiter läuft, nachdem die aktuelle Benutzersitzung beendet wurde.

Wenn Sie den Daemon direkt mit der Option -ud starten, erstellt der Datenbankserver den Daemonprozess und kehrt sofort zurück (d.h., er wird beendet und der nächste Befehl kann ausgeführt werden), bevor der Daemon sich initialisiert oder versucht, eine der im Befehl angegebenen Datenbanken zu öffnen.

Ein Vorteil der Verwendung von "dbspawn" statt der Option -ud besteht darin, dass der dbspawn-Prozess nicht herunterfährt, bis er bestätigt hat, dass der Daemon gestartet wurde und bereit ist, Anforderungen entgegenzunehmen. Wenn aus irgendeinem Grund der Daemon nicht startet, ist der Exit-Code für "dbspawn" ein von Null verschiedener Wert.

Wenn Sie den Datenbankserver als Daemon starten, werden seine Berechtigungen durch die unmask-Einstellung des aktuellen Benutzers gesteuert. Es wird empfohlen, den unmask-Wert vor dem Start des Datenbankservers festzulegen, um sicherzustellen, dass der Datenbankserver die entsprechenden Berechtigungen hat.

Geben Sie nicht die Option -um zusammen mit der Option -ud an.

### Siehe auch

- „Dienstprogramm für den Serverstart im Hintergrund (dbspawn)“ auf Seite 983
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]
- „Datenbankserver als Dienst oder Daemon ausführen“ auf Seite 180
- „Allgemeine Sicherheitstipps“ auf Seite 1406

## Datenbankserveroption -uf

Legt die Aktion fest, die der Datenbankserver ausführt, wenn ein schwerwiegender Fehler oder ein Assertierungsfehler auf einem Datenbankserver auftritt.

### Syntax

**dbsrv16 -uf action ...**

### Standardwert

default

**Zulässige Werte**

- **abort** Der Datenbankserver wird heruntergefahren und eine Kerndatei wird generiert.
- **default** Der Datenbankserver verhält sich genauso wie bei "abort", außer wenn ein schwerwiegender Fehler aufgrund eines vollen Geräts auftritt. In diesem Fall verhält er sich genauso wie bei "defunct". Dadurch wird verhindert, dass das System versucht, eine Kerndatei auf ein volles Gerät zu schreiben.
- **defunct** Der Datenbankserver läuft weiter, ohne "abort" aufzurufen. Bei jedem neuen Verbindungsversuch mit dem Datenbankserver wird der ursprüngliche Fehler gemeldet.

**Gilt für**

Alle Betriebssysteme.

**Siehe auch**

- „Datenbankserveroption -oe“ auf Seite 269
- „Dienstprogramm für Supportanfragen (dbsupport)“ auf Seite 987
- „Fehlerbehandlung: Fehler in SQL Anywhere melden“ auf Seite 1108
- „Protokollieren von Datenbankserver-Aktionen“ auf Seite 163
- „Datenbankserveroption -ufd“ auf Seite 299

## Datenbankserveroption -ufd

Legt die Aktion fest, die der Datenbankserver ausführt, wenn ein schwerwiegender Fehler oder ein Assertierungsfehler in einer Datenbank auftritt.

**Syntax**

**dbsrv16 -ufd** *action* ...

**Standardwert**

abort

**Zulässige Werte**

- **abort** Die betroffene Datenbank wird heruntergefahren. Der Status des Datenbankservers und der anderen Datenbanken bleiben unverändert.
- **restart** Die betroffene Datenbank wird heruntergefahren und es wird versucht, die Datenbank neu zu starten. Wenn der Neustartversuch fehlschlägt, wird ein Datenbankserver-Assertierungsfehler gemeldet.
- **escalate** Der Datenbank-Assertierungsfehler oder schwerwiegende Datenbankfehler wird als Datenbankserver-Assertierungsfehler bzw. schwerwiegender Datenbankserverfehler behandelt. Der Datenbankserver verarbeitet die Assertierung bzw. den Fehler wie durch die Datenbankserveroption -uf angegeben.

**Gilt für**

Alle Betriebssysteme.

### Bemerkungen

Die Datenbankserveroption `-ufd` muss einer Spezifikation der Datenbankdatei vorangehen.

### Siehe auch

- [„Datenbankserveroption -oe“ auf Seite 269](#)
- [„Dienstprogramm für Supportanfragen \(dbsupport\)“ auf Seite 987](#)
- [„Fehlerbehandlung: Fehler in SQL Anywhere melden“ auf Seite 1108](#)
- [„Protokollieren von Datenbankserver-Aktionen“ auf Seite 163](#)
- [„Datenbankserveroption -uf“ auf Seite 298](#)

## Datenbankserveroption -ui

Öffnet das Fenster **Startoptionen für den Server**, zeigt das Meldungsfenster des Datenbankservers an und startet den Datenbankserver, unabhängig davon, ob der X Window-Server gestartet wird.

### Syntax

`dbsrv16 -ui ...`

### Gilt für

Linux mit X Window-Server-Unterstützung

### Bemerkungen

Mithilfe der Option `-ui` können Sie das Fenster **Startoptionen für den Server** verwenden, um beim Starten des Datenbankservers Serveroptionen anzugeben und um das Meldungsfenster des Datenbankservers anzuzeigen, sobald der Server gestartet wurde.

Wenn die Datenbankserveroption `-ui` die einzige angegebene Option ist, wird das Fenster **Startoptionen für den Server** angezeigt, in dem Sie Optionen zum Starten des Datenbankservers eingeben können.

Der Datenbankserver versucht, eine verwendbare Anzeige zu finden, wenn `-ui` angegeben wird. Wenn er keine findet, weil z.B. die `DISPLAY`-Umgebungsvariable nicht eingestellt ist oder der X Window-Server nicht läuft, startet der Datenbankserver im Shell-Modus. Wenn der Datenbankserver nicht gestartet werden soll, falls keine benutzbare Anzeige gefunden wird, geben Sie die Option `-ux` anstelle von `-ui` an. Sie können nur jeweils eine der Optionen `-uc`, `-ui`, `-um` oder `-ux` angeben.

Weitere Informationen zum Starten des Datenbankservers als Daemon finden Sie unter [„Datenbankserveroption -ud“ auf Seite 298](#).

### Siehe auch

- [„Datenbankserveroption -uc“ auf Seite 297](#)
- [„Datenbankserveroption -um“ auf Seite 300](#)
- [„Datenbankserveroption -ux“ auf Seite 302](#)

## Datenbankserveroption -um

Zeigt Datenbankservermeldungen in einem neuen Fenster in *DBLauncher.app* an.

**Syntax****dbsrv16 -um ...****Gilt für**

Mac OS X

**Bemerkungen**

Die Option -um ermöglicht eine Verbindung mit der *DBLauncher.app*-Instanz, wenn diese läuft, und zeigt Meldungen in einem neuen Fenster in *DBLauncher.app* an. Die Option -um muss mit den anderen Optionen beim Start des Datenbankservers benutzt werden. Servermeldungen erscheinen in diesem Fenster und nicht in der Shell. Das Schließen dieses Fenster bewirkt das Herunterfahren des Datenbankservers. Wenn eine Verbindung mit der *DBLauncher.app*-Instanz nicht eingerichtet werden kann, startet der Datenbankserver nicht.

Damit sich der Datenbankserver mit einer *DBLauncher.app*-Instanz verbinden kann, müssen beide in demselben Mac OS X-Sicherheitskontext laufen. Beispiel: Ein aus einer SSH-Sitzung gestarteter Datenbankserver kann keine *DBLauncher.app*-Instanz finden, die von Launch Services gestartet wurde.

Geben Sie nicht die Option -um zusammen mit der Option -ud an.

Weitere Informationen zum Starten des Datenbankservers als Daemon finden Sie unter [„Datenbankserveroption -ud“](#) auf Seite 298.

**Siehe auch**

- [„Datenbankserveroption -uc“](#) auf Seite 297
- [„Datenbankserveroption -ui“](#) auf Seite 300

## Datenbankserveroption -ut

Ändert den Zeitstempel temporärer Dateien

**Syntax****dbsrv16 -ut minutes ...****Standardwert**

Der Standardwert ist 30 Minuten.

**Gilt für**

Unix, Mac OS X

**Bemerkungen**

Dieser Parameter bewirkt, dass der Server den Zeitstempel für temporäre Dateien in bestimmten Intervallen ändert.

## Datenbankserveroption -ux

Öffnet das Fenster **Server-Startoptionen** oder zeigt das Fenster Meldungsfenster des Datenbankservers unter Linux an (wenn X Window-Server benutzt wird).

### Syntax

**dbsrv16 -ux ...**

### Gilt für

Linux mit X Window-Server-Unterstützung

### Bemerkungen

Mit der Option -ux haben Sie beim Start des Datenbankservers zwei Möglichkeiten: Entweder Sie verwenden das Fenster **Server-Startoptionen**, um Serveroptionen anzugeben, wenn der Datenbankserver gestartet wird, oder Sie lassen das Meldungsfenster des Datenbankservers anzeigen, sobald der Server gestartet ist.

Wenn die Datenbankserveroption -ux die einzige angegebene Option ist, wird das Fenster **Startoptionen für den Server** angezeigt, in dem Sie Optionen zum Starten des Datenbankservers eingeben können.

Der Server muss in der Lage sein, eine verwendbare Anzeige zu finden, wenn "-ux" angegeben ist. Wenn er keine findet, weil z.B. die DISPLAY-Umgebungsvariable nicht eingestellt ist oder der X Window-Server nicht läuft, schlägt der Start des Datenbankservers fehl. Wenn der Datenbankserver gestartet werden soll, auch wenn keine benutzbare Anzeige gefunden wird, geben Sie die Option -ui anstelle von -ux an.

Wenn Sie zusätzlich zu "-ux" weitere Serveroptionen angeben, wird das Meldungsfenster des Datenbankservers angezeigt, sobald der Datenbankserver gestartet ist. Sie können nur jeweils eine der Optionen -uc, -ui oder -ux angeben.

Weitere Informationen zum Starten des Datenbankservers als Daemon finden Sie unter [„Datenbankserveroption -ud“ auf Seite 298](#).

### Siehe auch

- [„Datenbankserveroption -uc“ auf Seite 297](#)
- [„Datenbankserveroption -ui“ auf Seite 300](#)
- [„Datenbankserveroption -qn“ auf Seite 274](#)

### Beispiel

Der folgende Befehl zeigt das Fenster **Server-Startoptionen**, in das Sie Optionen für das Starten des Datenbankservers eingeben können:

```
dbsrv16 -ux
```

Der folgende Befehl startet den Datenbankserver und zeigt das Meldungsfenster des Datenbankservers an:

```
dbsrv16 -ux sample.db
```

## Datenbankserveroption -v

Zeigt die Softwareversion an

### Syntax

**dbsrv16 -v ...**

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Zeigt die Datenbankserver-Version in einem Fenster an und stoppt dann.

## Datenbankserveroption -vss

Aktiviert und deaktiviert den Volume Shadow Copy Service (VSS, Schattenkopiedienst).

### Syntax

**dbsrv16 -vss{ + | - } ...**

### Gilt für

Microsoft Windows XP 32-Bit und Microsoft Windows 2003 32-Bit und 64-Bit sowie spätere Betriebssysteme.

### Bemerkungen

Standardmäßig können, wenn das SQL Anywhere-VSS-Schreibprogramm (*dbvss16.exe*) läuft, alle SQL Anywhere-Datenbanken den VSS-Dienst für Sicherungen verwenden. Sie können VSS ohne das SQL Anywhere-VSS-Schreibprogramm verwenden, um Datenbanken zu sichern. Sie benötigen aber vielleicht die kompletten SQL Anywhere-Wiederherstellungsprozeduren, um die Datenbanken wiederherzustellen. Wenn ein Datenbankserver am Schattenkopiedienst nicht teilnehmen soll, verwenden Sie beim Start des Datenbankservers **-vss-**.

### Siehe auch

- [„SQL Anywhere-Volumeschattenkopie-Dienst \(VSS\)“ auf Seite 1042](#)
- [„Dienstprogramm für Dienste \(dbsvc\) für Windows“ auf Seite 974](#)
- [„Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler“ auf Seite 1057](#)

### Beispiel

Der folgende Befehl startet die Datenbank *mydatabase.db* und weist den Datenbankserver an, nicht an VSS-Vorgängen teilzunehmen, auch wenn das SQL Anywhere-VSS-Schreibprogramm (*dbvss16.exe*) läuft:

```
dbsrv16 -vss- mydatabase.db
```

## Datenbankserveroption -wc

Steuert, ob Prüfsummen auf Schreibvorgängen für alle Datenbanken auf diesem Datenbankserver aktiviert sind, wenn die Datenbanken standardmäßig keine Prüfsummen aktiviert haben.

### Syntax

```
dbsrv16 -wc[ + | - ] ...
```

### Gilt für

Alle Betriebssysteme und Server

### Bemerkungen

Der Unterschied zwischen Schreib-Prüfsummen (mit der Option -wc aktiviert) und globalen Prüfsummen (eine Datenbank mit aktivierten Prüfsummen erstellen) ist, dass mit -wc Datenbankseiten nur Prüfsummen erhalten, wenn sie auf die Festplatte ausgeschrieben werden. Seiten, die von der Festplatte gelesen werden, werden nur überprüft, wenn ein Prüfsummenwert berechnet wurde, bevor die Seiten geschrieben wurden. Wenn eine Datenbank über aktivierte Prüfsummen verfügt, werden Prüfsummen für alle Seiten berechnet, während sie geschrieben werden, und Prüfsummen werden für alle Seiten überprüft, wenn sie gelesen werden.

Falls der Datenbankserver feststellt, dass die Datenbank unter Windows Mobile oder auf einem mobilen Speichermedium, z.B. einer Netzwerkfreigabe oder einem USB-Gerät, ausgeführt wird, aktiviert der Datenbankserver automatisch globale Prüfsummen für alle Datenbankseiten.

Standardmäßig sind für Datenbanken, die mit Version 10 und 11 von SQL Anywhere erstellt wurden, keine globalen Prüfsummen aktiviert. Wenn Sie eine Datenbank starten, die mit SQL Anywhere 11 auf einem Datenbankserver der Version 12 oder später eingerichtet wurde, erstellt der Datenbankserver standardmäßig Schreib-Prüfsummen für Seiten, wenn sie auf die Festplatte geschrieben werden (-wc+). Datenbanken der Version 12 oder später haben globale Prüfsummen standardmäßig aktiviert, sodass der Datenbankserver bei diesen Datenbanken standardmäßig auf -wc gesetzt wird, weil standardmäßig alle Datenbankseiten Prüfsummen haben. Sie können entweder die Option -wc oder die START DATABASE-Anweisung verwenden, um das Prüfsummenverhalten des Datenbankservers zu ändern, wenn Sie nicht die Standardeinstellungen für Prüfsummen verwenden wollen.

Sie können überprüfen, ob eine Datenbank mit aktivierten globalen Prüfsummen erstellt wurde, indem Sie die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'Checksum' );
```

Sie können überprüfen, ob Schreib-Prüfsummen für I/O-Schreibvorgänge aktiviert sind, indem Sie nur die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'WriteChecksum' );
```

### Siehe auch

- „Erkennung von Beschädigungen mithilfe von Prüfsummen“ auf Seite 1084
- „Datenbankserveroption -wc “ auf Seite 304
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption -x

Gibt serverseitige Netzwerk-Kommunikationsprotokolle an.

### Syntax

```
dbsrv16 -x { all | none | tcpip [ ( parm=value;...) } ...
```

### Zulässige Werte

Unabhängig davon, welche Einstellungen Sie für die Option -x wählen, der Datenbankserver akzeptiert immer Verbindungen über Shared Memory.

Standardmäßig startet der Personal Datenbankserver nur das Shared Memory-Protokoll.

Standardmäßig startet der Netzwerk-Datenbankserver das Shared Memory- und TCP/IP-Protokoll.

Sie können auch die folgenden Werte für die Option -x angeben:

- **TCP/IP (TCP)** Wartet auf Verbindungsversuche des Clients über das Shared Memory- und TCP/IP-Protokoll.

Das TCP/IP-Protokoll wird vom Netzwerkservers und vom Personal Datenbankserver für die Kommunikation auf demselben Computer unterstützt.

- **NONE** Hört die Verbindungsversuche des Clients nur anhand des Protokolls des Shared Memorys ab
- **ALL** Wartet auf Verbindungsversuche des Clients über das Shared Memory- und TCP/IP-Protokoll.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Mit der Option -x geben Sie an, welche Kommunikationsprotokolle verwendet werden sollen, um auf Clientverbindungen zu warten.

Hinweise zur Sicherung von Shared Memory-Verbindungen unter Unix finden Sie unter „[Allgemeine Sicherheitstipps](#)“ auf Seite 1406.

Beim TCP/IP- Protokoll werden gegebenenfalls zusätzliche Parameter im folgenden Format festgelegt:

```
-x tcpip(PARM1=value1;PARM2=value2;...)
```

Weitere Informationen über die verfügbaren Parametern finden Sie unter „[Netzwerkprotokolloptionen](#)“ auf Seite 388.

Unter Unix sind Anführungszeichen erforderlich, wenn mehr als ein Parameter übergeben wird oder bestimmte Satzzeichen (z. B. runde Klammern) verwendet werden. Zum Beispiel:

```
-x "tcpip(PARM1=value1;PARM2=value2;...)"
```

Wenn der Datenbankserver auf TCP/IP-Verbindungen wartet, prüft er standardmäßig alle Netzwerkkarten auf Port 2638. Siehe „[Netzwerkprotokolloptionen](#)“ auf Seite 388.

### Siehe auch

- [Nachfolgend finden Sie Beispiele zum Starten eines Datenbankservers auf Seite 153](#)
- [„Datenbankserveroption -xd “ auf Seite 307](#)
- [„Datenbankoption -xp“ auf Seite 335](#)
- [„Datenbankserveroption -xs “ auf Seite 310](#)
- [„Verbindungsparameter CommLinks \(LINKS\)“ auf Seite 345](#)
- [„TCP/IP-Protokoll“ auf Seite 105](#)

### Beispiele

Gestatten Sie Shared Memory- und TCP/IP- Verbindungen auf dem Netzwerkservers:

```
dbsrv16 -n server_name "%SQLANYAMP16%\demo.db"
```

Verwenden Sie die Option -x, um Protokolloptionen zum Optimieren des Verhaltens von TCP/IP anzugeben. Gestatten Sie dem Netzwerkservers, zwei bestimmte Netzwerkkarten zu verwenden:

```
dbsrv16 -x "tcpip(MyIP=192.75.209.12,192.75.209.32)" "%SQLANYAMP16%\demo.db"
```

Gestatten Sie Shared Memory- und TCP/IP- Verbindungen auf dem Personal Server:

```
dbeng16 -x tcpip "%SQLANYAMP16%\demo.db"
```

## Datenbankserveroption -xa

Gibt eine durch Kommas getrennte Liste von Datenbanknamen und Authentifizierungszeichenfolgen für einen Arbiterservers an

### Syntax

```
dbsrv16 -xa [ auth=auth-string [, auth-string... ]; ];DBN={ * | database-name [, database-name... ] }
```

### Gilt für

Alle Betriebssysteme (ausgenommen Windows Mobile)

Nur Netzwerkservers

### Bemerkungen

Diese Option wird nur angegeben, wenn der Arbiterservers in einem Datenbankspiegelungssystem gestartet wird.

**auth-Parameter** Das Weglassen der Authentifizierungszeichenfolge bedeutet, dass keine Validierung der von einem Partnerservers angegebenen Authentifizierungszeichenfolge erfolgt.

Wenn nur eine Authentifizierungszeichenfolge angegeben wird, müssen alle Datenbanken diese Authentifizierungszeichenfolge verwenden.

Wenn in der Liste der Authentifizierungszeichenfolgen mehr als eine Authentifizierungszeichenfolge angegeben wird, muss die Liste der Datenbanknamen dieselbe Anzahl von Einträgen enthalten. Die Authentifizierungszeichenfolge wird bei der entsprechenden Datenbank in der DBN-Liste überprüft.

Die Authentifizierungszeichenfolge muss für alle Datenbanken, die diesen Server als Arbitr verwenden, mit dem Wert SET MIRROR OPTION *Authentifizierungszeichenfolge* übereinstimmen.

**DBN-Parameter** Dieser Parameter listet die Datenbanken auf, die diesen Server als Arbitr verwenden können. Damit eine beliebige Datenbank den Server als Arbitr verwenden kann, geben Sie **DBN=\*** an.

### Beispiel

Der folgende Befehl startet den Arbitr-Datenbankserver und gibt an, dass jede beliebige Datenbank den Server als Arbitr verwenden kann:

```
dbsrv16
-n arbiter
-su sql
-x tcpip(port=6870)
-xf c:\arbiter\arbiterstate.txt
-xa "AUTH=abc;DBN=*" 
```

Der folgende Befehl startet den Arbitr-Datenbankserver und gibt die beiden Datenbanken an, die den Server als Arbitr verwenden können:

```
dbsrv16
-n arbiter
-su sql
-x tcpip(port=6870)
-xf c:\arbiter\arbiterstate.txt
-xa "AUTH=abc,xyz;DBN=database1,database2" 
```

In diesem Beispiel verwendet database1 die Authentifizierungszeichenfolge "abc" und database2 verwendet die Authentifizierungszeichenfolge "xyz".

### Siehe auch

- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Praktische Einführung: Datenbankspiegelungssysteme erstellen“ auf Seite 1509
- „Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen“ auf Seite 1516
- „Verbindungsparameter DatabaseName (DBN)“ auf Seite 354
- „Datenbankserveroption -xf“ auf Seite 308
- „Datenbankoption -xp“ auf Seite 335
- „Gespiegelte Datenbanken zu laufenden Spiegelungssystemen hinzufügen“ auf Seite 1492

## Datenbankserveroption -xd

Verhindert, dass der Datenbankserver der Standarddatenbankserver wird.

### Syntax

```
dbsrv16 -xd ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn ein Datenbankserver startet, versucht er, auf diesem Computer zum Standarddatenbankserver zu werden. Der erste Datenbankserver, der startet, wenn kein Standardserver vorhanden ist, wird zum Standarddatenbankserver. Shared Memory-Verbindungen auf diesem Computer, die nicht ausdrücklich einen Datenbankservernamen angeben, erfolgen mit dem Standardserver.

Wenn diese Option angegeben wird, verhindert sie, dass der Datenbankserver der Standarddatenbankserver wird. Diese Option bewirkt, dass Clients, die keinen Datenbankservernamen angeben, den Datenbankserver über das Shared Memory nicht finden können. Die Option -xd verhindert auch, dass der Datenbankserver den Standard-TCP-Port verwendet. Wenn kein TCP-Port angegeben ist, benutzt der Datenbankserver einen anderen Port als 2638.

### Siehe auch

- „Datenbankserveroption -n “ auf Seite 266
- „Verbindungsparameter StartLine (START)“ auf Seite 385
- „Datenbankserveroption -x “ auf Seite 305
- „Verbindungsparameter ServerName (Server)“ auf Seite 383
- „Fehlerbehandlung: Datenbankserver suchen“ auf Seite 83

## Datenbankserveroption -xf

Gibt den Speicherort der Datei an, die zur Aufrechterhaltung von Statusinformationen über Ihr Datenbank-Spiegelungssystem verwendet wird. Diese Option wird nur im Befehl zum Starten des Arbiterservers in einem Datenbankspiegelungssystem verwendet.

### Syntax

**dbsrv16 -xf** *state-file* ...

### Gilt für

Alle Betriebssysteme, nur Netzwerkservers

### Bemerkungen

Verwenden Sie CREATE MIRROR SERVER, um den Speicherort der Statusinformationsdatei für den Partnerserver zu definieren.

Die Option -xf gibt den Standort der Datei an, die zur Aufrechterhaltung von Statusinformationen über das Spiegelungssystem verwendet wird. Diese Option ist bei der Datenbankspiegelung erforderlich.

Weitere Hinweise zur Statusinformationsdatei bei der Datenbankspiegelung finden Sie unter „Fehlerbehandlung: Statusinformationsdateien von Partner und Arbitr“ auf Seite 1498.

**Siehe auch**

- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Praktische Einführung: Datenbankspiegelungssysteme erstellen“ auf Seite 1509
- „Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen“ auf Seite 1516
- „Datenbankserveroption -xa “ auf Seite 306
- „Datenbankoption -xp“ auf Seite 335

**Beispiel**

Der folgende Befehl (in einer Zeile eingegeben) startet einen Datenbankserver namens "myarbiter", der die Statusinformationsdatei `c:\arbiter\arbiter.state` verwendet.

```
dbsrv16 -n myarbiter -su sql  
-x "TCPIP(PORT=6870;DOBROAD=no)" -xf "c:\arbiter\arbiter.state"  
-xa "AUTH=abc;DBN=mirror_demo"
```

## Datenbankserveroption -xm

Legt fest, wie häufig der Datenbankserver eine Prüfung auf neue IP-Adressen durchführt.

**Syntax**

```
dbsrv16 -xm seconds
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Wenn der Computer, auf dem der Datenbankserver läuft, mit einem neuen Netzwerk verbunden ist und die Option -xm angegeben ist, wird die Änderung erkannt und der Datenbankserver beginnt mit dem Warten auf Verbindungen im neuen Netzwerk. Wenn der Computer von einem Netzwerk getrennt wird, stellt der Datenbankserver das Warten auf Verbindungen im entsprechenden Netzwerk ein.

Die Option -xm ist standardmäßig auf 0 gesetzt, wenn die SQL Anywhere-Anwendung nicht auf einem tragbaren Gerät ausgeführt wird. Die Standardeinstellung auf tragbaren Geräten ist 120 Sekunden. Geben Sie zum Deaktivieren der Option -xm den Wert 0 an. Verwenden Sie die IsPortableDevice-Eigenschaft, um zu prüfen, ob die SQL Anywhere-Anwendung auf einem tragbaren Gerät ausgeführt wird.

Die Angabe dieser Option wirkt sich nicht auf die Performance von HTTP- oder HTTPS-Listnern aus.

Wenn Sie die Netzwerkprotokolloption MyIP (ME) angegeben haben, ist die Überwachung mit der Option -xm deaktiviert.

Wenn eine Netzwerkschnittstelle getrennt wird, werden alle mit der Netzwerkschnittstelle verknüpften Listener heruntergefahren.

Verwenden Sie die Systemprozedur `sa_server_option`, um die Einstellung dieser Option zu ändern, ohne den Datenbankserver herunterzufahren.

### Siehe auch

- [IsPortableDevice-Servereigenschaft auf Seite 752](#)
- [„sa\\_server\\_option-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„MyIP-Protokolloption \(ME\)“ auf Seite 414](#)
- [IPAddressMonitorPeriod-Servereigenschaft auf Seite 751](#)

### Beispiel

Der folgende Befehl startet einen Datenbankserver der alle 60 Sekunden eine Prüfung auf neue IP-Adressen durchführt.

```
dbsrv16 -xm 60;
```

## Datenbankserveroption -xs

Gibt serverseitige Webdienst-Kommunikationsprotokolle an

### Syntax

```
dbsrv16 -xs [...] { protocol[,...] }
```

*protocol* : {

**NONE**

| **HTTP** [ ( *option=value*;... ) ]

| **HTTPS** [ ( *option=value*;... ) ]

☛ **Cloud-Hinweis:** Die Option -xs kann für Cloud-Server mit OnDemand Edition-Lizenz mehrfach angegeben werden.

### Zulässige Werte

Sie können folgende Parameter festlegen:

- **option** Eine Netzwerkprotokolloption

Eine Liste der bei den einzelnen Protokollen unterstützten Werte für *option* finden Sie unter [„Netzwerkprotokolloptionen“ auf Seite 388](#).

- **HTTP** Wartet auf Webanforderungen des Clients über das HTTP-Protokoll. Der Standardport zum Warten auf Anforderungen ist 80.
- **HTTPS** Wartet auf Webanforderungen des Clients über das HTTPS-Protokoll. Der Standardport zum Warten auf Anforderungen ist 443. Um HTTPS zu verwenden, müssen Sie das Zertifikat und das Kennwort des Servers angeben. Das Kennwort muss ein RSA-Zertifikat sein, da HTTPS RSA-Verschlüsselung verwendet.

Der HTTP-Server unterstützt HTTPS-Verbindungen mit SSL-Version 3.0 und den TLS-Versionen 1.0 und 1.1.

Bei FIPS-zertifizierter RSA-Verschlüsselung können Sie **HTTPS** oder **HTTPS** mit **FIPS=Y** angeben. FIPS-zertifiziertes HTTPS verwendet eine separate zertifizierte Bibliothek, ist aber mit HTTPS kompatibel.

Hinweise zum Erzwingen von FIPS-zertifizierten Algorithmen finden Sie unter [„Datenbankserveroption -fips“](#) auf Seite 237.

- **NONE** Nicht auf Webanforderungen warten. Dies ist die Standardeinstellung.

Weitere Informationen über die verfügbaren Parameter finden Sie unter [„Netzwerkprotokolloptionen“](#) auf Seite 388.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Verwenden Sie die Option -xs, wenn Sie angeben wollen, welche Webprotokolle verwendet werden sollen, um Anforderungen abzuhören.

Wenn Sie die Option -xs nicht angeben, wartet der Datenbankserver nicht auf Webanforderungen.

Wenn Sie mehrere Protokolle angeben möchten, können Sie entweder die Option -xs für jedes Protokoll angeben oder mehrere Protokolle mit einer Option -xs angeben. Der Server wartet mit allen angegebenen Protokollen auf Webanforderungen.

#### Hinweis

Wenn Sie gleichzeitig mehrere Webserver starten möchten, müssen Sie unterschiedliche Ports einstellen, weil die Server denselben Standardport haben.

Bei Transportschichtssicherheit können Sie HTTPS- oder FIPS-zertifizierte HTTPS-Protokolle verwenden. Siehe [„Verschlüsselung für SQL Anywhere-Webdienste“](#) auf Seite 1458.

Unter Unix sind Anführungszeichen erforderlich, wenn mehr als ein Parameter übergeben wird:

```
-xs "HTTP(OPTION1=value1;OPTION2=value2;...)"
```

#### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe [„Getrennt lizenzierbare Komponenten“](#) [*SQL Anywhere 16 - Einführung*].

### Beispiel

Auf HTTP-Webanforderungen auf Port 80 warten:

```
dbsrv16 web.db -xs HTTP(PORT=80)
```

Auf Webanforderungen mithilfe von HTTPS warten:

```
dbsrv16 web.db -xs
HTTPS(FIPS=N;PORT=82;IDENTITY=ecserver.id;IDENTITY_PASSWORD=test)
```

Ports 80 und 8080 abhören:

```
dbsrv16 -xs HTTP(port=80),HTTP(PORT=8080)
```

oder

```
dbsrv16 -xs HTTP(port=80) -xs HTTP(PORT=8080)
```

### Siehe auch

- „Datenbankoption -sn “ auf Seite 332
- „Datenbankserveroption -x “ auf Seite 305
- „Datenbankserveroption -xa “ auf Seite 306
- „Datenbankserveroption -xf “ auf Seite 308
- „Datenbankoption -xp“ auf Seite 335
- „FIPS-Protokolloption“ auf Seite 404
- „SQL Anywhere als HTTP-Webserver“ [*SQL Anywhere Server - Programmierung*]

## Datenbankserveroption -z

Zeigt Kommunikationsdiagnosemeldungen und andere Meldungen zum Zweck der Fehlerbehandlung an

### Syntax

```
dbsrv16 -z ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option sollte nur zum Aufspüren von Fehlern verwendet werden. Die Informationen werden im Meldungsfenster des Datenbankservers angezeigt.

### Siehe auch

- *DebuggingInformation-Servereigenschaft* auf Seite 748
- „Datenbankserveroption -z “ auf Seite 312
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankserveroption -ze

Zeigt Datenbankserver-Umgebungsvariable im Meldungsfenster des Datenbankservers an.

### Syntax

```
dbsrv16 -ze ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver, ausgenommen Windows Mobile.

## Bemerkungen

Wenn Sie die Option `-ze` angeben, werden beim Start Umgebungsvariable im Meldungsfenster des Datenbankservers aufgelistet. Sie können den Inhalt des Meldungsfenster des Datenbankservers in einer Datei protokollieren, indem Sie beim Start des Datenbankservers die Option `-o` angeben.

## Siehe auch

- „SQL Anywhere-Umgebungsvariablen“ auf Seite 467
- „Datenbankserveroption `-o`“ auf Seite 268
- „Datenbankserveroption `-z`“ auf Seite 312

## Beispiel

Der folgende Befehl startet einen Datenbankserver namens "myserver" und gibt die für den Server gesetzten Umgebungsvariablen im Meldungsfenster des Datenbankservers und in der Datei *server-log.txt* aus.

```
dbsrv16 -n myserver -ze -o server-log.txt
```

## Datenbankserveroption `-zl`

Aktiviert das Aufzeichnen der zuletzt vorbereiteten SQL-Anweisung für jede einzelne Verbindung zu Datenbanken auf dem Server

## Syntax

```
dbsrv16 -zl ...
```

## Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Diese Funktion kann auch mit der `RememberLastStatement`-Servereinstellung aktiviert werden. Sie erhalten die zuletzt vorbereitete SQL-Anweisung für eine Verbindung, indem Sie den `LastStatement`-Wert der `CONNECTION_PROPERTY`-Funktion verwenden. Mit der gespeicherten Prozedur `sa_conn_activity` können Sie die zuletzt vorbereitete SQL-Anweisung für alle aktuellen Verbindungen mit Datenbanken auf dem Server erhalten.

Der `LastStatement`-Wert wird gesetzt, wenn eine Anweisung vorbereitet wird, und gelöscht, wenn eine Anweisung gelöscht wird. Bei jeder Verbindung ist jeweils nur eine Anweisungszeichenfolge verfügbar.

Wenn `sa_conn_activity` einen nicht-leeren Wert bei einer Verbindung meldet, ist dies höchstwahrscheinlich die Anweisung, die die Verbindung derzeit ausführt. Wenn die Anweisung abgeschlossen wäre, wäre sie wahrscheinlich gelöscht und der Eigenschaftswert bereinigt worden. Wenn eine Anwendung mehrere Anweisungen vorbereitet und ihre Anweisungs-Handles aufbewahrt, spiegelt der `LastStatement`-Wert nicht wieder, was eine Verbindung derzeit ausführt.

Bei Aufrufen von gespeicherten Prozeduren erscheint nur der äußere Prozeduraufruf, nicht die Anweisungen innerhalb der Prozedur.

### Vorsicht

Wenn "-zl" angegeben oder die RememberLastStatement-Servereinstellung aktiviert ist, kann jeder Benutzer die sa\_conn\_activity-Systemprozedur aufrufen oder den Wert der LastStatement-Verbindungseigenschaft erhalten, um die zuletzt vorbereitete SQL-Anweisung eines jeden anderen Benutzers herauszufinden. Diese Option sollte mit Umsicht verwendet und ausgeschaltet werden, wenn sie nicht mehr benötigt wird.

### Siehe auch

- [RememberLastStatement-Servereigenschaft auf Seite 760](#)
- [LastStatement-Verbindungseigenschaft auf Seite 723](#)
- [„sa\\_conn\\_activity-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„sa\\_server\\_option-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Datenbankserveroption -zn

Gibt die Anzahl der aufzubewahrenden Kopien der Anforderungs-Logdatei an

### Syntax

**dbsrv16 -zn** *integer*

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn die Protokollierung von Anforderungen über längere Zeit aktiviert ist, kann die Logdatei umfangreich werden. Mit der Option -zn können Sie die Anzahl der Kopien der Anforderungs-Logdatei angeben, die aufbewahrt werden sollen. Sie wirkt sich nur aus, wenn auch -zs angegeben ist. Mit der Option -zs erstellen Sie eine neue Logdatei und benennen die ursprüngliche Logdatei um, wenn diese eine bestimmte Größe erreicht.

Wenn Sie beispielsweise Informationen der Anforderungsprotokollierung in die Datei *req.out* umleiten und fünf Kopien der Anforderungs-Logdatei mit der Option -zn angeben, erstellt der Server Dateien in der folgenden Reihenfolge: *req.out.1*, *req.out.2*, *req.out.3*, *req.out.4* und *req.out.5*. Wenn diese Dateien bereits existieren und sich das aktive Anforderungslog wieder anfüllt, passiert Folgendes:

- *req.out.1* wird gelöscht.
- Die Dateien *req.out.2* bis *req.out.5* werden in *req.out.1* bis *req.out.4* umbenannt.
- Die Kopie des aktiven Logs wird in *req.out.5* umbenannt.

Die Anforderungsprotokollierung wird mit der Option -zr aktiviert und in eine separate Datei unter Verwendung der Option -zo umgeleitet. Sie können auch die Anzahl der Anforderungslogs mit der sa\_server\_option-Systemprozedur einstellen, wobei *nn* die Anzahl der Kopien der Anforderungs-Logdatei angibt:

```
CALL sa_server_option('RequestLogNumFiles',nn);
```

**Siehe auch**

- „Datenbankserveroption -zs “ auf Seite 319
- RequestLogNumFiles-Servereigenschaft auf Seite 761
- „Datenbankserveroption -zo “ auf Seite 315
- „Datenbankserveroption -zr “ auf Seite 317
- „Datenbankserveroption -zs “ auf Seite 319
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Anforderungsprotokollierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

**Beispiel**

Im folgenden Beispiel, das in einer Zeile eingegeben werden muss, werden Informationen der Anforderungsprotokollierung in eine Anforderungs-Logdatei namens *mydatabase.log* ausgegeben, die eine maximale Größe von 10 kB hat. Drei Kopien des Anforderungslogs werden aufbewahrt:

```
dbsrv16 "c:\my data\mydatabase.db" -zr all -zn 3  
      -zs 10 -zo mydatabase.log
```

## Datenbankserveroption -zo

Leitet Informationen der Anforderungsprotokollierung in eine andere als die reguläre Logdatei um

**Syntax**

```
dbsrv16 -zo filename ...
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Die Anforderungsprotokollierung wird mit der Option -zr aktiviert. Sie können die Ausgabe von dieser Datei in eine andere Datei umleiten, die nicht die reguläre Logdatei ist, indem Sie die Option -zo verwenden.

Diese Option verhindert, dass die Anforderungsprotokollierung im Meldungsfenster des Datenbankservers angezeigt wird.

**Siehe auch**

- RequestLogFile-Servereigenschaft auf Seite 761
- „Datenbankserveroption -zn “ auf Seite 314
- „Datenbankserveroption -zr “ auf Seite 317
- „Datenbankserveroption -zs “ auf Seite 319
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Anforderungsprotokollierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Datenbankserveroption -zoc

Leitet Webdienst-Clientinformationen in eine Datei um.

### Syntax

**dbsrv16 -zoc** *filename* ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die Webdienst-Clientlogdatei enthält HTTP-Anforderungen und Transportdaten, die für ausgehende Clientaufrufe an den Webdienst aufgezeichnet werden. Die Webdienst-Clientlogdatei kann auch mit der `sa_server_option`-Systemprozedur angegeben werden:

```
CALL sa_server_option( 'WebClientLogFile', 'clientinfo.txt' );
```

Die Protokollierung wird automatisch aktiviert, wenn sie die Serveroption `-zoc` festlegen. Sie können das Protokollieren in diese Datei aktivieren und deaktivieren, indem Sie die `sa_server_option`-Systemprozedur verwenden:

```
CALL sa_server_option( 'WebClientLogging', 'ON' );
```

### Siehe auch

- [WebClientLogFile-Servereigenschaft auf Seite 765](#)
- [WebClientLogging-Servereigenschaft auf Seite 765](#)
- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL Anywhere als HTTP-Webserver“ [*SQL Anywhere Server - Programmierung*]
- „CREATE FUNCTION-Anweisung [Webdienst]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE PROCEDURE-Anweisung [Webdienste]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

### Beispiel

Der nachstehende Befehl startet den Datenbankserver, damit er an Port 80 auf HTTP-Webanforderungen wartet und ausgehenden Webdienst-Clientinformationen in der Datei *clientinfo.txt* protokolliert:

```
dbsrv16 web.db -xs HTTP(PORT=80) -zoc clientinfo.txt
```

## Datenbankserveroption -zp

Aktiviert die Aufzeichnung des zuletzt vom Abfrageoptimierer verwendeten Plans

### Syntax

**dbsrv16 -zp** ...

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Verwenden Sie diese Option, wenn der Datenbankserver den Abfrageausführungsplan speichern soll, der zuletzt von den einzelnen Verbindungen verwendet wurde. Diese Funktion kann auch unter Verwendung

der Servereinstellung RememberLastPlan mit der sa\_server\_option-Systemprozedur aktiviert werden.. Sie können den Text des zuletzt benutzten Plans unter Verwendung der Verbindungseigenschaft LastPlanText anzeigen.

**Siehe auch**

- [RememberLastPlan-Servereigenschaft auf Seite 760](#)
- [LastPlanText-Verbindungseigenschaft auf Seite 723](#)
- „sa\_conn\_activity-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Datenbankserveroption -zr

Aktiviert die Anforderungsprotokollierung von Vorgängen

**Syntax**

```
dbsrv16 -zr { SQL | HOSTVARS | PLAN | PROCEDURES | TRIGGERS | OTHER | BLOCKS |  
REPLACE | ALL | NONE } ...
```

**Zulässige Werte**

- **SQL** Aktiviert die Protokollierung des Folgenden:
  - START DATABASE-Anweisungen
  - STOP DATABASE-Anweisungen
  - STOP SERVER-Anweisungen
  - Anweisungsvorbereitung und -ausführung
  - EXECUTE IMMEDIATE-Anweisung
  - Optionseinstellungen
  - COMMIT-Anweisungen
  - ROLLBACK-Anweisungen
  - PREPARE TO COMMIT-Vorgänge
  - Herstellen und Trennen von Verbindungen
  - Anfänge von Transaktionen
  - DROP STATEMENT-Anweisungen
  - Cursor-Deklarationen
  - Öffnen, Schließen und Wiederaufnahme von Cursorn
  - Fehler
- **PLAN** Aktiviert die Protokollierung von Ausführungsplänen (Kurzform). Ausführungspläne für Prozeduren werden auch aufgezeichnet, wenn das Protokollieren von Prozeduren (PROCEDURES) aktiviert ist.
- **HOSTVARS** Aktiviert die Protokollierung von Hostvariablenwerten. Wenn Sie HOSTVARS angeben, werden die für SQL aufgelisteten Informationen ebenfalls protokolliert.
- **PROCEDURES** Aktiviert die Protokollierung von Anweisungen, die innerhalb von Prozeduren und benutzerdefinierten Funktionen ausgeführt werden.

- **TRIGGERS** Aktiviert die Protokollierung von Anweisungen, die innerhalb von Triggern ausgeführt werden.
- **OTHER** Aktiviert die Protokollierung von zusätzlichen, nicht in SQL enthaltenen Anforderungstypen, z.B. FETCH und PREFETCH. Wenn Sie allerdings OTHER, aber nicht SQL angeben, ist dies äquivalent mit der Angabe von SQL+OTHER. Das Einbeziehen von OTHER kann zu einem schnellen Anwachsen der Logdatei führen und sich negativ auf die Server-Performance auswirken.
- **BLOCKS** Aktiviert die Protokollierung von Details, die anzeigen, wenn eine Verbindung an einer anderen Verbindung blockiert bzw. entblockiert ist.
- **REPLACE** Ersetzt bei Beginn der Protokollierung das vorhandene Anforderungslog durch ein neues (leeres) mit demselben Namen. Ansonsten wird das vorhandene Anforderungslog geöffnet und die neuen Einträge werden an das Ende der Datei angehängt.
- **ALL** Protokolliert die gesamten unterstützten Informationen. Diese Einstellung ist äquivalent mit der Angabe von SQL+PLAN+HOSTVARS+PROCEDURES+TRIGGERS+OTHER+BLOCKS. Diese Einstellung kann zu einem schnellen Anwachsen der Logdatei führen und sich negativ auf die Server-Performance auswirken.
- **NO oder NONE** Deaktiviert die Protokollierung in das Anforderungslog.

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Diese Option sollte nur zum Aufspüren von Fehlern verwendet werden. Die Informationen werden im Meldungsfenster des Datenbankservers angezeigt oder in die Logdatei gesendet. Bei Angabe von mehreren Werten werden sie durch , oder + voneinander getrennt.

Wenn der Datenbankserver gestartet ist, können Sie die Anforderungslog-Einstellungen mithilfe der sa\_server\_option-Systemprozedur anpassen, um mehr bzw. weniger Informationen zu protokollieren.

Sie können den aktuellen Wert für die RequestLogging-Einstellung mithilfe der folgenden Abfrage abrufen:

```
SELECT PROPERTY( 'RequestLogging' );
```

### Siehe auch

- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- RequestLogging-Servereigenschaft auf Seite 761
- „Datenbankserveroption -zn “ auf Seite 314
- „Datenbankserveroption -zo “ auf Seite 315
- „Datenbankserveroption -zs “ auf Seite 319
- „Anforderungsprotokollierung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Datenbankserveroption -zs

Begrenzt die Größe des Anforderungsprotokolls.

### Syntax

```
dbsrv16 -zs { size[ k | m | g ] } ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die Anforderungsprotokollierung wird mit der Option -zr aktiviert und in eine separate Datei unter Verwendung der Option -zo umgeleitet. Sie können die Größe der Datei begrenzen, indem Sie die Option -zs verwenden.

Die *Größe* ist die maximale Dateigröße für das Anforderungslog, in Byte. Verwenden Sie **k**, **m** oder **g**, um die Einheit in kB, MB bzw. GB anzugeben.

Wenn Sie -zs 0 angeben, gibt es keine maximale Dateigröße für die Anforderungsprotokollierungsdatei und die Datei wird niemals umbenannt. Dies ist der Standardwert.

Wenn die Anforderungs-Logdatei die Größe erreicht, die mit der Option -zs oder mit der Systemprozedur `sa_server_option` angegeben wurde, wird die Datei mit der Erweiterung `.old` umbenannt (eine gleichnamige bereits vorhandene Datei wird überschrieben). Anschließend wird die Anforderungs-Logdatei neu gestartet.

### Siehe auch

- [RequestLogMaxSize-Servereigenschaft auf Seite 761](#)
- [„Datenbankserveroption -zn“ auf Seite 314](#)
- [„Datenbankserveroption -zo“ auf Seite 315](#)
- [„Datenbankserveroption -zr“ auf Seite 317](#)
- [„sa\\_server\\_option-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Anforderungsprotokollierung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)

### Beispiel

Am folgenden Beispiel ist ersichtlich, wie die Option -zs zur Steuerung der Logdateigröße eingesetzt wird. Angenommen, Sie starten einen Datenbankserver mit folgendem Befehl:

```
dbsrv16 -zr all -zs 10k -zo mydatabase.log
```

Es wird eine neue Logdatei `mydatabase.log` eingerichtet. Wenn diese Datei 10 kB groß ist, wird eine eventuell vorhandene Datei `mydatabase.old` gelöscht, `mydatabase.log` wird in `mydatabase.old` umbenannt und eine neue Datei `mydatabase.log` wird gestartet. Dieses Verfahren wird jedes Mal wiederholt, wenn `mydatabase.log` die angegebene Größe erreicht (in diesem Fall 10 kB).

## Datenbankserveroption -zt

Aktiviert die Protokollierung der Anforderungszeitinformationen

### Syntax

**dbsrv16 -zt ...**

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Mit der Option **-zt** setzen Sie die RequestTiming-Eigenschaft auf "On". Wenn RequestTiming aktiviert ist, können Sie mithilfe der `sa_performance_diagnostics`-Systemprozedur alle Werte der Eigenschaften abrufen, in denen Anforderungszeitinformationen gespeichert werden.

Die folgenden Eigenschaften geben nur dann Anforderungszeitinformationen zurück, wenn RequestTiming aktiviert ist. Andernfalls geben die Eigenschaften NULL zurück. Alle Eigenschaften außer ReqStatus sind Verbindungs-, Datenbank- und Servereigenschaften. Die Datenbank- und Servereigenschaften sind eine Zusammenfassung der Verbindungswerte seit dem Start der Datenbank bzw. des Servers. Diese Datenbank- und Servereigenschaften geben nur dann Informationen zurück, wenn RequestTiming aktiviert ist.

- ReqCountActive-Verbindungseigenschaft
- ReqCountBlockContention-Verbindungseigenschaft
- ReqCountBlockLock-Verbindungseigenschaft
- ReqCountUnscheduled-Verbindungseigenschaft
- ReqStatus-Verbindungseigenschaft
- ReqTimeActive-Verbindungseigenschaft
- ReqTimeBlockContention-Verbindungseigenschaft
- ReqTimeBlockLock-Verbindungseigenschaft
- ReqTimeUnscheduled-Verbindungseigenschaft

### Beispiel

Sie können den aktuellen Wert für die RequestTiming-Einstellung mithilfe der folgenden Abfrage abrufen:

```
SELECT PROPERTY( 'RequestTiming' );
```

**Siehe auch**

- [RequestTiming-Servereigenschaft auf Seite 761](#)
- [„sa\\_performance\\_diagnostics-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„sa\\_performance\\_statistics-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Anforderungsprotokollierung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [ReqCountActive-Verbindungseigenschaft](#)
- [ReqCountBlockContention-Verbindungseigenschaft](#)
- [ReqCountBlockLock-Verbindungseigenschaft](#)
- [ReqCountUnscheduled-Verbindungseigenschaft](#)
- [ReqStatus-Verbindungseigenschaft](#)
- [ReqTimeActive-Verbindungseigenschaft](#)
- [ReqTimeBlockContention-Verbindungseigenschaft](#)
- [ReqTimeBlockLock-Verbindungseigenschaft](#)
- [ReqTimeUnscheduled-Verbindungseigenschaft](#)

## Datenbankoptionen (Datenbank)

Diese Optionen werden nach der Datenbankdatei angegeben und gelten nur für diese Datenbank.

### Datenbankoption -a

Wendet die benannte Transaktionslogdatei an.

**Syntax**

**dsrv16** [ *server-options* ] *database-file* **-a** *log-filename* ...

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Diese Option wird zur Wiederherstellung bei Datenträgerfehlern in der Datenbankdatei verwendet. Wenn diese Option angegeben ist, wendet der Datenbankserver das Log an und fährt herunter. Wenn mehrere Transaktionslogs angewendet werden sollen und "-a" verwendet wird, müssen Sie die korrekte Reihenfolge ihrer Anwendung kennen. Der Datenbankserver wendet mehrere Transaktionslogs automatisch in der korrekten Reihenfolge an, wenn Sie die Option -ad bzw. -ar verwenden.

Die Datenbankoption -a muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

Wenn Sie beim Starten des Servers eine Cachegröße angeben, kann sich die Wiederherstellungszeit verkürzen.

### Siehe auch

- „Sicherung und Datenwiederherstellung“ auf Seite 1027
- „Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler“ auf Seite 1057
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Datenbankoption -ad “ auf Seite 322
- „Datenbankoption -ar “ auf Seite 323
- „Datenbankoption -as “ auf Seite 324

### Beispiel

Mit dem folgenden Beispiel (in einer Zeile eingegeben) wird die Logdatei *mydemo.log* auf eine Sicherungskopie der Beispieldatenbank angewendet.

```
dbsrv16 "c:\backup\mydemo.db" -a "c:\backup\mydemo.log"
```

## Datenbankoption -ad

Gibt das Logverzeichnis an, das die in der Datenbank verwendeten Transaktionslogdateien enthält.

### Syntax

```
dbsrv16 [ server-options ] database-file -ad log-directory ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn Sie die Option -ad verwenden, wird das angegebene Verzeichnis nach Transaktionslogdateien durchsucht, die der Datenbank zugeordnet sind. Transaktionslogdateien mit Start-Offsets größer oder gleich dem in der Datenbankdatei gespeicherten Log-Start-Offset werden in der Reihenfolge der Log-Offsets angewendet. Wenn die Transaktionslogdateien angewendet wurden, wird die Datenbank gestoppt. Sie müssen auch die Option -as angeben, wenn die Datenbank weiter laufen soll, nachdem die Transaktionslogdateien angewendet wurden.

Wenn das angegebene Logverzeichnis einen relativen Pfad verwendet, wird dieses Verzeichnis relativ zum *database-file*-Verzeichnis gelesen.

Die Datenbankoption -ad muss nach der *database-file* angegeben werden und gilt nur für diese Datenbank.

### Siehe auch

- „Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler“ auf Seite 1057
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Datenbankoption -a “ auf Seite 321
- „Datenbankoption -ar “ auf Seite 323
- „Datenbankoption -as “ auf Seite 324

### Beispiel

Der Datenbankserver wendet die Logdateien im *backup*-Verzeichnis an der *mysample.db*-Datenbank an und stoppt danach die Datenbank.

```
dbsrv16 "c:\mysample.db" -ad "c:\backup"
```

Der Datenbankserver wendet die Logdateien im *backup*-Verzeichnis an der *mysample.db*-Datenbank an, wobei die Datenbank nach der Anwendung der Logdateien weiter läuft.

```
dbsrv16 "c:\mysample.db" -ad "c:\backup" -as
```

## Datenbankoption -al

Lässt die Standard-Benutzerauthentifizierung für angegebene Benutzer der angegebenen Datenbank zu.

### Syntax

```
dbsrv16 [ server-options ] database-file -al userid[ ;userid ... ] ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Lässt die Standard-Benutzerauthentifizierung für die in der durch Semikola getrennten Liste von Benutzer-IDs angegebenen Benutzer zu, und zwar bei der Datenbank, auf die die Option folgt. Es können höchstens 5 Benutzer-IDs angegeben werden.

Diese Option ist nützlich, wenn die *login\_mode*-Option keine Standard-Authentifizierung umfasst und der Benutzer keine Möglichkeit hat, sich mit anderen Methoden zu authentifizieren. Benutzer mit vollen DBA-Privilegien können immer die Standard-Authentifizierung verwenden.

### Siehe auch

- „*login\_mode*-Option“ auf Seite 623

## Datenbankoption -ar

Gibt an, dass etwaige Transaktionslogdateien, die sich in demselben Verzeichnis wie das aktuelle Transaktionslog befinden, auf die Datenbank angewendet werden sollen.

### Syntax

```
dbsrv16 [ server-options ] database-file -ar ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Wenn Sie die Option *-ar* verwenden, sucht der Datenbankserver nach der Datenbank zugeordneten Transaktionslogdateien, die sich in demselben Verzeichnis wie das aktuelle Transaktionslog befinden.

Der Transaktionslog-Speicherort wird von der Datenbank bezogen. Transaktionslogdateien mit Start-Offsets größer oder gleich dem in der Datenbankdatei gespeicherten Log-Start-Offset werden in der Reihenfolge der Log-Offsets angewendet. Wenn die Transaktionslogdateien angewendet wurden, wird die Datenbank gestoppt. Sie müssen auch die Option `-as` angeben, wenn die Datenbank weiter laufen soll, nachdem die Transaktionslogdateien angewendet wurden.

Die Datenbankoption `-ar` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

### Siehe auch

- „Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler“ auf Seite 1057
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Datenbankoption `-a`“ auf Seite 321
- „Datenbankoption `-ad`“ auf Seite 322
- „Datenbankoption `-as`“ auf Seite 324

### Beispiel

Der Datenbankserver wendet die Transaktionslogdateien (deren Speicherort von der Datenbank bezogen wird) an der *mysample.db*-Datenbank an. Die Datenbank läuft weiter, nachdem die Transaktionslogdateien angewendet wurden.

```
dbsrv16 "c:\mysample.db" -ar -as
```

## Datenbankoption `-as`

Gibt an, dass die Datenbank weiter ausführen soll, nachdem Transaktionslogs übernommen wurden (zusammen mit `-ad` oder `-ar` verwendet).

### Syntax

```
dbsrv16 [ server-options ] database-file { -ad log-dir | -ar } -as ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Die Option `-as` muss zusammen mit der Option `-ad` bzw. `-ar` angegeben werden. Wenn Sie `-as` verwenden, läuft die Datenbank weiter, nachdem die Transaktionslogs an ihr angewendet wurden.

Die Datenbankoption `-as` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

**Siehe auch**

- „Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler“ auf Seite 1057
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Datenbankoption -a “ auf Seite 321
- „Datenbankoption -ad “ auf Seite 322
- „Datenbankoption -ar “ auf Seite 323

**Beispiel**

Der Datenbankserver wendet die Transaktionslogdateien an der *mysample.db*-Datenbank an. Weil "-ar" angegeben ist, bezieht der Datenbankserver in diesem Fall den Standort der Transaktionslogs von der Datenbank. Die Datenbank läuft weiter, nachdem die Logdateien angewendet wurden.

```
dbsrv16 "c:\mysample.db" -ar -as
```

Der Datenbankserver wendet die Logdateien im *backup*-Verzeichnis an der *mysample.db*-Datenbank an. Die Datenbank läuft weiter, nachdem die Logdateien angewendet wurden.

```
dbsrv16 "c:\mysample.db" -ad "c:\backup" -as
```

## Datenbankoption -ds

Gibt das Verzeichnis an, in dem sich die DBSpaces für die Datenbank und das Transaktionslog befinden.

**Syntax**

```
dbsrv16 database-file -ds dbspace-directory ...
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

**Bemerkungen**

Wenn ein DBSpace-Verzeichnis angegeben ist, sucht der Datenbankserver nur in diesem Verzeichnis nach DBSpaces. Der Standort des DBSpaces erscheint im Meldungsfenster des Datenbankservers.

Wenn Ihre Sicherung DBSpaces mit vollständigen Pfadnamen enthält, können Sie diese Option verwenden, um die gesicherte Kopie der Datenbank auf dem Computer der ursprünglichen Datenbank zu starten, während die ursprüngliche Datenbank weiterhin läuft.

Die Datenbankoption -ds muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

Wenn eine Transaktionslogdatei nicht im durch diese Option angegebenen Verzeichnis gefunden werden kann, wird an diesem Speicherort eine solche Datei erstellt.

**Vorsicht**

Die Option -ds sollte ausschließlich für die Wiederherstellung verwendet werden. Wenn Sie diese Option angeben und die Datenbank über ein aktuelles, aktives Transaktionslog verfügt, das sich nicht im durch die Option -ds angegebenen Verzeichnis befindet, wird am angegebenen Speicherort ein neues Transaktionslog erstellt.

### Siehe auch

- „Zusätzliche Hinweise zu DBSpaces“ auf Seite 128
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „STOP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „default\_dbspace-Option“ auf Seite 604

### Beispiel

Das folgende Beispiel startet einen Datenbankserver, der nach DBSpaces im Verzeichnis *c:\backup\Nov15* sucht:

```
dbsrv16 c:\backup\Nov15\my.db -ds c:\backup\Nov15\
```

Das folgende Beispiel startet einen Datenbankserver, der nach DBSpaces im aktuellen Verzeichnis sucht:

```
dbsrv16 my.db -ds .
```

## Datenbankoption -dh

Verhindert, dass diese Datenbank angezeigt wird, wenn das Dienstprogramm für die Serverauflistung (dblocate) auf diesem Server verwendet wird.

### Syntax

```
dbsrv16 [ server-options ] database-file -dh ...
```

### Gilt für

Alle Plattformen

### Bemerkungen

Die Option -dh macht eine Datenbank unauffindbar, wenn das Dienstprogramm für die Serverauflistung (dblocate) auf diesem Server verwendet wird. Daher wird die Datenbank nicht aufgelistet, wenn dblocate mit der Option -d, -dn bzw. -dv verwendet wird.

Die Datenbankoption -dh muss nach der *database-file* angegeben werden und gilt nur für diese Datenbank.

### Siehe auch

- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960

## Datenbankoption -ek

Gibt den Schlüssel für eine stark verschlüsselte Datenbank an.

### Syntax

```
dbsrv16 [ server-options ] database-file -ek key ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Den Schlüsselwert müssen Sie mit der Option `-ek` angeben, damit eine verschlüsselte Datenbank gestartet wird. Der Schlüssel ist eine Zeichenfolge mit einer Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Wenn Sie den Chiffrierschlüssel in einem Fenster so eingeben möchten, dass er nicht als lesbarer Text erscheint, verwenden Sie die Serveroption `-ep`.

Um Kommunikationspakete zwischen Clientanwendungen und dem Datenbankserver zu sichern, verwenden Sie die Serveroption `-ec` und Transportschichtssicherheit. Siehe [„Transportschichtssicherheit“ auf Seite 1444](#).

Die Datenbankoption `-ek` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

## Siehe auch

- [„Datenbankserveroption -ec“ auf Seite 230](#)
- [„Datenbankserveroption -ep“ auf Seite 233](#)
- [„Verbindungsparameter DatabaseKey \(DBKEY\)“ auf Seite 353](#)
- [„Datenbankverschlüsselung und -entschlüsselung“ auf Seite 1424](#)

## Beispiel

Mit dem folgenden Beispiel wird eine Datenbank gestartet und der Chiffrierschlüssel in der Befehlszeile angegeben.

```
dbsrv16 -x tcpip mydata.db -ek "Akmm9u70y"
```

## Datenbankoption -m

Kürzt das Transaktionslog, wenn ein Checkpoint gesetzt wurde.

## Syntax

```
dbsrv16 [ server-options ] database-file -m ...
```

## Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Die Option kürzt das Transaktionslog, wenn ein Checkpoint ausgeführt wurde, entweder beim Herunterfahren, oder als Ergebnis eines vom Server geplanten Checkpoints. Mit dieser Option kann das Wachstum von Transaktionslogs begrenzt werden. Die Checkpoint-Häufigkeit wird weiterhin durch die Optionen `checkpoint_time` und `recovery_time` (bzw. die Datenbankserveroptionen `-gc` und `-gr`) gesteuert.

Die Option `-m` ist beim Bearbeiten von sehr umfangreichen Transaktionen hilfreich, die schnelle Antwortzeiten erfordern, und wenn Sie sich für die Wiederherstellung oder Replikation nicht auf den Inhalt des Transaktionslogs verlassen können. Wenn diese Option gewählt ist, gibt es keinen Schutz gegen Datenträgerausfall auf dem Gerät, das die Datenbankdatei enthält.

Um Datenbankdatei-Fragmentierung zu vermeiden, wird empfohlen, das Transaktionslog beim Verwenden dieser Option auf ein anderes Gerät oder eine andere Partition als die Datenbank selbst zu legen.

Diese Option entspricht der Serveroption `-m`, gilt aber nur für die aktuelle Datenbank bzw. für die durch die Variable *Datenbankname* angegebene Datenbank.

### **Vorsicht**

Verwenden Sie die Option `-m` nicht bei Datenbanken, die repliziert oder synchronisiert werden. Replikation und Synchronisation, die von SQL Remote und MobiLink verwendet werden, hängen von den Informationen aus dem Transaktionslog ab.

Die Datenbankoption `-m` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

### **Siehe auch**

- „Datenbankserveroption `-m`“ auf Seite 265
- „Das Transaktionslog“ auf Seite 135
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998

### **Beispiel**

Mit dem folgenden Beispiel wird ein Datenbankserver mit dem Namen "silver" gestartet und die *salesdata.db*-Datenbank geladen. Wenn ein Checkpoint ausgeführt wurde, wird der Transaktionsloginhalt gelöscht.

```
dbsrv16 -n silver "c:\inventory details\salesdata.db" -m
```

## **Datenbankoption -n**

Legt den Namen der Datenbank fest.

### **Syntax**

```
dbsrv16 [ server-options ] database-file -n string ...
```

### **Standardwert**

Die Datenbank erhält den Namen der Datenbankdatei ohne Suchpfad und Erweiterung.

### **Gilt für**

Alle Betriebssysteme und Datenbankserver.

### **Bemerkungen**

Sowohl der Datenbankserver als auch Datenbanken können benannt werden. Da ein Datenbankserver mehrere Datenbanken laden kann, wird der Datenbankname zur Unterscheidung der verschiedenen Datenbanken verwendet.

Datenbanknamen dürfen Folgendes nicht:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.
- Sie dürfen nicht länger als 250 Byte sein.

Die Datenbankoption `-n` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

Sie können nur den Datenbanknamen `utility_db` verwenden, um eine Verbindung mit der Dienstprogrammdatenbank herzustellen.

**Hinweis**

Es gibt zwei Optionen `-n`. Die Option `-n` ist positionsabhängig. Wenn sie vor einem Datenbankdateinamen steht, ist sie eine Serveroption und benennt den Server. Wenn sie nach einem Datenbankdateinamen steht, ist sie eine Datenbankoption und benennt die Datenbank.

Der folgende Befehl benennt beispielsweise den Server `SERV` und die Datenbank `DATA`:

```
dbsrv16 -n SERV c:\mydata.db -n DATA
```

**Beispiel**

Wenn die gestartete Datenbank die Datenbank `%SQLANYAMP16%\demo.db` ist und die Option `-n` nicht angegeben wird, ist der Name der Datenbank `demo`.

Mit dem folgenden Beispiel wird der Datenbankserver mit einer Cachegröße von 3 MB gestartet, die Datenbank wird geladen und erhält den Namen `"test"`. Da kein Datenbankservername angegeben wurde, nimmt der Server seinen Namen von der ersten Datenbank, daher ist der Name des Servers ebenfalls `"test"`.

```
dbsrv16 -c 3MB "c:\mydata.db" -n "test"
```

**Siehe auch**

- „Datenbankservernamen und Datenbanknamen“ auf Seite 161
- „Datenbankserveroption `-n`“ auf Seite 266
- „Die Dienstprogrammdatenbank“ auf Seite 145

## Datenbankoption `-r`

Startet die benannte Datenbank im schreibgeschützten Modus.

**Syntax**

```
dbsrv16 [ server-options ] database-file -r ...
```

**Gilt für**

Alle Betriebssysteme und Datenbankserver.

### Bemerkungen

Öffnet alle Datenbankdateien (Haupt-Datenbankdatei, DBSpaces, Transaktionslog und Transaktionslog-Spiegel) mit Ausnahme der temporären Datei schreibgeschützt, wenn die Option in der Befehlszeile vor Datenbanknamen angegeben wird. Es sind keine Änderungen an den Datenbanken zulässig. Der Datenbankserver ändert weder Datenbankdateien noch Transaktionslogdateien.

Wenn die Option `-r` nach einer Datenbankdatei angegeben wird, behandelt das System nur die betreffende Datenbank als schreibgeschützt. Sie können an temporären Tabellen Änderungen durchführen, aber `ROLLBACK` ist wirkungslos, weil die Transaktions- und Rollback-Logs deaktiviert sind.

Eine auf einer CD-ROM gelieferte Datenbank ist ein Beispiel für eine Datenbankdatei, die nicht geändert werden kann. Sie können auf diese Art von Datenbank nur im schreibgeschützten Modus zugreifen.

Wenn Sie versuchen, die Datenbank zu ändern, zum Beispiel mit einer `INSERT`- oder `DELETE`-Anweisung, wird ein `SQLSTATE_READ_ONLY_DATABASE`-Fehler ausgegeben.

Datenbanken, die eine Wiederherstellung erfordern, können nicht im schreibgeschützten Modus gestartet werden. Dies gilt zum Beispiel für Datenbankdateien, die unter Verwendung einer Online-Sicherung erstellt wurden: Sie können nicht im schreibgeschützten Modus gestartet werden, wenn beim Start der Sicherung offene Transaktionen vorhanden waren, da diese Transaktionen eine Wiederherstellung verlangen, sobald die Sicherungskopie gestartet wird.

Sie können eine Datenbank nicht im schreibgeschützten Modus starten, wenn Auditing aktiviert ist.

### Siehe auch

- „Datenbankserveroption `-r`“ auf Seite 277
- „auditing-Option“ auf Seite 582

### Beispiel

Um zwei Datenbanken im schreibgeschützten Modus zu öffnen, führen Sie folgenden Befehl aus:

```
dbsrv16 -r database1.db database2.db
```

Um nur die erste von zwei Datenbanken im schreibgeschützten Modus zu öffnen, führen Sie folgenden Befehl aus:

```
dbsrv16 database1.db -r database2.db
```

## Datenbankoption `-sbx`

Steuert das Sandboxing für die Datenbank.

### Syntax

```
dbsrv16 [ server-options ] database-file -sbx{ + | - } ...
```

### Gilt für

Alle Betriebssysteme und Datenbankserver.

## Bemerkungen

Durch Aktivieren dieser Option werden die Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse.

Wenn diese Option nicht angegeben wird, werden für das Sandboxing die durch die Datenbankserveroption `-sbx` festgelegten Standardeinstellungen verwendet.

Sie können die Sandboxing-Einstellungen für die Datenbank temporär ändern, während die Datenbank läuft, indem Sie die `DiskSandbox`-Option in der `sa_db_option`-Systemprozedur verwenden.

## Siehe auch

- „`disk_sandbox`-Option“ auf Seite 608
- „Datenbankserveroption `-sbx`“ auf Seite 279
- „`sa_db_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankoption `-sm` (nicht mehr empfohlen)

Stellt einen alternativen Datenbankservernamen bereit, der benutzt werden kann, um auf die schreibgeschützte Spiegeldatenbank zuzugreifen. Diese Option wird nicht mehr empfohlen. Verwenden Sie stattdessen die `CREATE MIRROR SERVER`-Anweisung.

## Syntax

**dbsrv16** [ *server-options* ] *database-file* **-sm** *alternate-server-name*

## Gilt für

- Alle Betriebssysteme
- Nur Netzwerkservers

## Bemerkungen

Der *alternate-server-name* ist nur aktiv, wenn der Datenbankserver als Spiegelserver für die Datenbank fungiert. Durch Verwendung der Befehlszeilenoptionen `-sm` und `-sn` kann sich eine Anwendung immer mit der Datenbank auf dem Primär- oder Spiegelserver verbinden, ohne dass bekannt ist, welcher physische Server als Primärserver bzw. als Spiegelserver fungiert.

Die Datenbankoption `-sm` muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

### Siehe auch

- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verbindungen mit Datenbank in Spiegelungssystemen herstellen“ auf Seite 1472
- „Datenbankserveroption -xa “ auf Seite 306
- „Datenbankserveroption -xf “ auf Seite 308
- „Datenbankoption -xp“ auf Seite 335
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankspiegelung“ auf Seite 1467
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- ReadOnly-Datenbankeigenschaft auf Seite 784

### Beispiel

Der folgende Befehl startet die Datenbanken *satest.db* und *sample.db* auf einem Datenbankserver namens "myserver". Die -sn-Option weist den Datenbankserver an, mysampleprimary als alternativen Servernamen zu verwenden, wenn eine Verbindung mit *sample.db* aufgenommen wird, während die -sm-Option den Datenbankserver anweist, mysamplemirror als alternativen Servernamen für die Verbindung mit der auf dem Spiegelserver laufenden *sample.db* zu verwenden.

```
dbsrv16 -n myserver satest.db sample.db -sn mysampleprimary  
-sm mysamplemirror -xp  
"partner=( Server=server2;LINKS=TCPIP( PORT=2637;TIMEOUT=1 ) );  
auth=abc;arbiter=( Server=arbiter;LINKS=TCPIP( PORT=2639;TIMEOUT=1 ) );mode=s  
ync"  
-xf "c:\arbiter\arbiter.state"
```

Sie können sich mit der Datenbank *sample.db* verbinden, während sie auf dem *Primärserver* läuft, indem Sie einen der folgenden Verbindungsparameter verwenden:

- Server=myserver;DBN=sample
- Server=mysampleprimary
- Server=mysampleprimary;DBN=sample

Sie können mit *satest.db* unter Verwendung von "Server=mysampleprimary" keine Verbindung herstellen.

Sie können sich mit *sample.db* verbinden, während sie auf dem *Spiegelserver* läuft, indem Sie einen der folgenden Verbindungsparameter verwenden:

- Server=myserver;DBN=sample
- Server=mysamplemirror
- Server=mysamplemirror;DBN=sample

Sie können mit *satest.db* unter Verwendung von "Server=mysamplemirror" keine Verbindung herstellen.

## Datenbankoption -sn

Gibt einen alternativen Servernamen für eine einzelne auf einem Datenbankserver laufende Datenbank an.

### Syntax

```
dbsrv16 [ server-options ] database-file -sn alternate-server-name
```

**Gilt für**

- Alle Betriebssysteme
- Nur Netzwerkservers

**Bemerkungen****Hinweis**

Bei einer Datenbankspiegelung muss ein alternativer Servername angegeben werden, damit Clientanwendungen in der Lage sind, sich mit dem aktuellen Primärserver zu verbinden, ohne im Voraus zu wissen, welcher Server der Primärserver und welcher der Spiegelservers ist. Beide Partnerserver müssen denselben Namen als alternativen Servernamen benutzen. Verwenden Sie die CREATE MIRROR SERVER-Anweisung, um die alternativen Servernamen für den Primär- und Spiegelservers in einem Spiegelungssystem zu erstellen. Siehe „CREATE MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Die Datenbankoption -sn muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

Der Datenbankserver kann so konfiguriert werden, dass er auf mehr als auf einen Servernamen bei einem bestimmten Datenbankserver wartet. Andere als der echte Servername werden alternative Servernamen genannt und sind für eine bestimmte Datenbank spezifisch, die auf dem Datenbankserver läuft. Clients können den alternativen Servernamen unter Verwendung des ServerName-Verbindungsparameters (Server) angeben, um Verbindungen mit dieser Datenbank herzustellen.

Alternative Servernamen müssen im Netzwerk eindeutig sein. Wenn Sie versuchen, eine Datenbank über die Befehlszeile zu starten, und der alternative Servername, den Sie angeben, nicht eindeutig ist, schlägt der Start des Datenbankservers fehl. Sie können einen alternativen Servernamen auch mit der START DATABASE-Anweisung liefern.

Clients, die einen alternativen Servernamen angeben, können sich nur mit der Datenbank verbinden, die den alternativen Servernamen angegeben hat. Sie können keine Verbindung zu anderen Datenbanken auf demselben Datenbankserver herstellen oder andere Datenbanken auf demselben Datenbankserver erstellen, stoppen oder löschen. Wenn der DBN- oder DBF-Verbindungsparameter angegeben ist, muss er dem Datenbanknamen bzw. der Datenbankdatei entsprechen. Wenn kein DBN- oder DBF-Verbindungsparameter angegeben ist, agiert die Datenbank als die Standard-Datenbank bei diesem Server.

Das Dienstprogramm für die Serverauflistung (dblocate) erkennt alternative Servernamen.

**Siehe auch**

- „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)]
- „START DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbankspiegelung“ auf Seite 1467
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- AlternateServerName-Datenbankeigenschaft auf Seite 767

### Beispiel

Der folgende Befehl startet die Datenbanken *satest.db* und *sample.db* auf einem Datenbankserver namens "myserver". Die Option `-sn` teilt dem Datenbankserver mit, "mysample" als einen alternativen Servernamen bei der Verbindungsherstellung zu *sample.db* zu verwenden.

```
dbsrv16 -n myserver satest.db sample.db -sn mysample
```

Sie können mit *sample.db* verbinden, indem Sie einen der folgenden Verbindungsparameter verwenden:

- `Server=myserver;DBN=sample`
- `Server=mysample`
- `Server=mysample;DBN=sample`

Sie können mit *satest.db* unter Verwendung von "Server=mysample" keine Verbindung herstellen.

### Datenbankoption -wc

Steuert, ob Prüfsummen auf Schreibvorgängen für die Datenbank aktiviert sind, wenn sie standardmäßig keine Prüfsummen aktiviert hat.

#### Syntax

```
dbsrv16 [ server-options ] database-file -wc[ + | - ]
```

#### Gilt für

Alle Betriebssysteme und Server

#### Bemerkungen

Der Unterschied zwischen Schreib-Prüfsummen (mit der Option `-wc` aktiviert) und globalen Prüfsummen (Erstellen einer Datenbank mit aktivierten Prüfsummen) liegt darin, dass Datenbankseiten mit `-wc` erst dann Prüfsummen erhalten, wenn sie auf die Festplatte ausgeschrieben werden. Seiten, die von der Festplatte gelesen werden, werden nur überprüft, wenn ein Prüfsummenwert berechnet wurde, bevor die Seiten geschrieben wurden. Wenn eine Datenbank über aktivierte Prüfsummen verfügt, werden Prüfsummen für alle Seiten berechnet, während sie geschrieben werden, und Prüfsummen werden für alle Seiten überprüft, wenn sie gelesen werden.

Falls der Datenbankserver feststellt, dass die Datenbank unter Windows Mobile oder auf einem mobilen Speichermedium, z.B. einer Netzwerkfreigabe oder einem USB-Gerät, ausgeführt wird, aktiviert der Datenbankserver automatisch globale Prüfsummen für alle Datenbankseiten.

Standardmäßig sind für Datenbanken, die mit Version 10 und 11 von SQL Anywhere erstellt wurden, keine globalen Prüfsummen aktiviert. Wenn Sie eine Datenbank starten, die mit SQL Anywhere 11 auf einem Datenbankserver der Version 12 oder später eingerichtet wurde, erstellt der Datenbankserver standardmäßig Schreib-Prüfsummen für Seiten, wenn sie auf die Festplatte geschrieben werden (`-wc+`). Datenbanken der Version 12 oder später haben globale Prüfsummen standardmäßig aktiviert, sodass der Datenbankserver bei diesen Datenbanken standardmäßig auf `-wc` gesetzt wird, weil standardmäßig alle Datenbankseiten Prüfsummen haben. Sie können entweder die Option `-wc` oder die `START DATABASE`-Anweisung verwenden, um das Prüfsummenverhalten des Datenbankservers zu ändern, wenn Sie nicht die Standardeinstellungen für Prüfsummen verwenden wollen.

Sie können überprüfen, ob eine Datenbank mit aktivierten globalen Prüfsummen erstellt wurde, indem Sie die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'Checksum' );
```

Sie können überprüfen, ob Schreib-Prüfsummen für I/O-Schreibvorgänge aktiviert sind, indem Sie nur die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'WriteChecksum' );
```

### Siehe auch

- „Erkennung von Beschädigungen mithilfe von Prüfsummen“ auf Seite 1084
- „Datenbankserveroption -wc “ auf Seite 304
- „START DATABASE-Anweisung“ [SQL Anywhere Server - SQL-Referenzhandbuch]

## Datenbankoption -xp

Stellt einem Server Informationen bereit, mit denen er sich mit seinem Partner und dem Arbiter verbinden kann, wenn Datenbankspiegelung oder Scale-Out mit Schreibschutz verwendet wird. Die gesamte Syntax außer **-xp on** wird nicht mehr empfohlen.

### Syntax

```
dbsrv16 [ server-options ] database-file -xp on
```

### Syntax (nicht mehr empfohlen)

```
dbsrv16 [ server-options ] database-file  
-xp { on | mirror-settings }
```

*mirror-settings :*

```
partner=( partner-conn );  
auth=auth-str,  
[ ;arbiter=( arbiter-conn ) ]  
[ ;mode=[ sync | async | page ]  
[ ;autofailover=[ YES | NO ] ]  
[ ;pagetimeout=n ]  
[ ;preferred=[ YES | NO ] ...
```

### Gilt für

- Alle Betriebssysteme, ausgenommen Windows Mobile
- Nur Netzwerkservers

### Bemerkungen

Wenn Sie -xp angeben, müssen Sie auch den Speicherort der Statusinformationsdatei für die Datenbankspiegelung mit der Option -xf angeben. Die Datenbankoption -xp muss nach *database-file* angegeben werden und gilt nur für diese Datenbank.

Wenn die Verbindungsparameter in der Option -xp ungültig sind und mehrere Datenbanken auf dem Server ausgeführt werden, kann die gespiegelte Datenbank nicht starten und versucht nicht, eine neue Verbindung herzustellen. Wenn die gespiegelte Datenbank die einzige laufende Datenbank auf dem Datenbankserver ist, wird der Datenbankserver nicht gestartet.

**on** Sie können nur Datenbankspiegelung und/oder Scale-Out verwenden, wenn Sie beim Starten des Datenbankservers die Option **-xp** angeben, selbst wenn die Informationen zur Spiegelung oder zum Scale-Out in der Datenbank gespeichert sind. Wenn Sie angeben, dass **-xp** aktiviert (on) ist, können Sie keine anderen Spiegelungs- oder Scale-Out-Optionen mit der Option **-xp** angeben. Der Wert **off** wird nicht unterstützt. Datenbankspiegelungs- und Scale-Out-Einstellungen werden in der Datenbank mit folgenden Anweisungen festgelegt:

- CREATE MIRROR SERVER
- SET MIRROR OPTION

Wenn Sie **xp on** angeben, müssen Sie auch den Namen des Datenbankservers im Spiegelungssystem mit der Option **-n** festlegen. Es wird empfohlen, dass Sie auch die Option **-su** angeben, um das Kennwort für die Dienstprogrammdateiabank anzugeben. Dann können Sie über die Dienstprogrammdateiabank den Datenbankserver herunterfahren oder nötigenfalls erzwingen, dass der Spiegelserver zum Primärserver wird.

**partner-conn (nicht mehr empfohlen)** Gibt die Verbindungszeichenfolge für den Partner-Server an. Benutzer-ID und Kennwort sind nicht erforderlich. Es wird empfohlen, dass Sie ein Timeout angeben, um die Failover-Zeit zu verkürzen.

**auth-str (nicht mehr empfohlen)** Gibt die vom Arbiter verwendete Authentifizierungszeichenfolge an

**arbiter-conn (nicht mehr empfohlen)** Gibt die Verbindungszeichenfolge für den Arbiterserver an. Benutzer-ID und Kennwort sind nicht erforderlich. Es wird empfohlen, dass Sie ein Timeout angeben, um die Failover-Zeit zu verkürzen.

**mode (nicht mehr empfohlen)** Gibt den Synchronisationsmodus für die Datenbankspiegelung an: synchronous (sync), asynchronous (async) oder asynfullpage (page).

**autofailover (nicht mehr empfohlen)** Gibt an, ob der Spiegelserver automatisch als Primärserver übernimmt, wenn der ursprüngliche Primärserver ausfällt. Diese Option gilt nicht im synchronous-Modus.

### Hinweis

Es wird empfohlen, dass Sie die Option **-xp autofailover** auf "yes" setzen, wenn Sie den asynchronous- oder asynfullpage-Modus verwenden. Dadurch übernimmt der Spiegelserver automatisch als Primärserver, wenn der ursprüngliche Primärserver ausfällt.

**pagetimeout (nicht mehr empfohlen)** Gibt an, mit welcher Häufigkeit (in Sekunden) Transaktionslog-Seiten an den Spiegelserver gesendet werden, gleichgültig ob sie voll sind oder nicht. Diese Option gilt nur im Asynchron-Ganzseiten-Modus.

**preferred (nicht mehr empfohlen)** Gibt an, ob der Server der bevorzugte Server im Spiegelungssystem ist. Der bevorzugte Server übernimmt wenn möglich die Rolle des Primärservers. Dies ist äquivalent mit der Angabe der bevorzugten Option in der CREATE MIRROR SERVER-Anweisung. Siehe „Bevorzugte Datenbankserver in Datenbankspiegelungssystemen“ auf Seite 1484.

**Vorsicht**

Im asynchronen und im Asynchron-Ganzseiten-Modus ist nicht garantiert, dass festgeschriebene Transaktionen auf dem Spiegelserver aufgezeichnet werden, und es ist möglich, dass Daten verloren gehen. Siehe „Datenbankspiegelungsmodi“ auf Seite 1477.

**Siehe auch**

- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankspiegelungssysteme einrichten“ auf Seite 1480
- „SQL Anywhere-Scale-Out mit Schreibschutz“ auf Seite 1536
- „Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“ auf Seite 1556
- „Praktische Einführung: Datenbankspiegelungssysteme erstellen“ auf Seite 1509
- „Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen“ auf Seite 1516
- „Getrennt lizenzierte Komponenten“ [*SQL Anywhere 16 - Einführung*]
- „Datenbankspiegelungsmodi“ auf Seite 1477
- „Datenbankoption -sn “ auf Seite 332
- „Datenbankserveroption -su “ auf Seite 289
- „Datenbankserveroption -xa “ auf Seite 306
- „Datenbankserveroption -xf “ auf Seite 308
- „Datenbankserveroption -n “ auf Seite 266
- MirrorMode-Datenbankeigenschaft auf Seite 779

**Beispiel**

Der folgende Befehl startet drei Datenbankdateien auf einem Datenbankserver, der zur Beteiligung an einem Spiegelungssystem zur Verfügung steht:

```
dbsrvl6 -n server1 -x tcpip(PORT=6871) -su sql
c:\server1\one.db -xp on c:\server1\two.db -xp on c:\server1\three.db -xp on
```

## Verbindungsparameter

Verbindungsparameter sind in Verbindungszeichenfolgen enthalten. Sie können an den folgenden Stellen eingegeben werden:

- In der Verbindungszeichenfolge einer Anwendung. Siehe „Fehlerbehandlung: Verbindungen einrichten“ auf Seite 81 und Als Verbindungszeichenfolge übergebene Verbindungsparameter auf Seite 31.
- SQLConnect-Umgebungsvariable.
- In einer ODBC-Datenquelle. Siehe „ODBC-Datenquellen“ auf Seite 38.
- Im SQL Anywhere-Fenster **Verbinden**. Siehe „SQL Anywhere-Dienstprogrammverbindungen“ auf Seite 30.

### Hinweis

- Verbindungsparameter berücksichtigen nicht die Groß-/Kleinschreibung, auch wenn ihre Werte dies möglicherweise tun (z.B. Dateinamen unter Unix).
- Boolesche Parameter werden mit YES, Y, ON, TRUE, T oder 1 aktiviert und mit NO, N, OFF, FALSE, F oder 0 deaktiviert. Bei den Parametern wird die Groß-/Kleinschreibung nicht berücksichtigt.
- Die Verwendung der einzelnen Verbindungsparameter bestimmt die Umstände, unter denen der Parameter zu verwenden ist. Zu den allgemein verwendeten Einträgen gehören die Folgenden:
  - **Eingebettete Datenbanken** Der Personal Datenbankserver (dbeng16) wird in der Regel mit eingebetteten Anwendungen verwendet. Wenn die Anwendung die Verbindung von der Datenbank trennt, wird die Datenbank entladen und der Server gestoppt.
  - **Lokale Datenbankserver** Ein lokaler Datenbankserver ist ein Server, der auf Ihrem Computer ausgeführt wird. Sie können entweder den Personal Server (dbeng16) oder den Netzwerkserver (dbsrv16) verwenden.
  - **Netzwerk-Datenbankserver** Ein Netzwerkserver (dbsrv16) kann auf Ihrem Computer oder einem anderen Computer in einem Netzwerk ausgeführt werden. Verwenden Sie den Netzwerkserver, wenn Sie möchten, dass andere Benutzer eine Verbindung mit der Datenbank herstellen können.
- Sie können das dbping-Dienstprogramm verwenden, um Verbindungszeichenfolgen zu testen. Die Option -c wird verwendet, um die Verbindungsparameter anzugeben. Beispiel: Ein Datenbankserver namens demo16 führt die Beispieldatenbank aus (die mit dem Befehl dbsrv16 -n demo16 "%SQLANYAMP16%\demo.db" gestartet werden kann). Der folgende Befehl gibt eine Meldung zurück, die angibt, dass die Verbindung mit der Datenbank erfolgreich war.

```
dbping -d -c "Server=demo16;DBN=demo;UID=DBA;PWD=sql"
```

Der folgende Befehl gibt die Meldung Ping der Datenbank fehlgeschlagen - Datenbankserver läuft nicht zurück, wenn kein Datenbankserver namens "other-server" auf dem lokalen Computer läuft:

```
dbping -c "Server=other-server"
```

### Siehe auch

- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Syntaxregeln für Verbindungsparameter“ auf Seite 36

## Verbindungsparameter AppInfo (APP)

Unterstützt Administratoren dabei, von einem Datenbankserver aus den Ursprung von bestimmten Clientverbindungen zu identifizieren

**Syntax**

{ **AppInfo** | **APP** }=*keyword=value*

**Verwendungszweck**

Überall

**Zulässige Werte**

Clients können ihre eigene Zeichenfolge festlegen, die der generierten Zeichenfolge angefügt wird. Die AppInfo-Eigenschaftszeichenfolge ist eine Sequenz von durch Semikola getrennten **key=Wert**-Paaren. Folgende Schlüssel sind gültig:

- **API** DBLIB, ODBC, OLEDB, ADO.NET, iAnywhereJDBC, PHP, PerlDBD oder DBEXPRESS
- **APPINFO** Wenn Sie AppInfo in der Verbindungszeichenfolge angegeben haben, wird die Zeichenfolge eingegeben.
- **EXE** Der Name der Client-Programmdatei (Windows, Linux und Solaris).
- **HOST** Der Hostname des Clientsystems
- **IP** IP-Adresse des Clientssystems
- **OS** Der Betriebssystemname und die Versionsnummer (zum Beispiel Windows XP).
- **OSUSER** Der Betriebssystem-Benutzername, der dem Clientprozess zugewiesen ist. Wenn der Clientprozess einen anderen Benutzer impersoniert (oder das gesetzte ID-Bit auf Unix gesetzt ist), wird der Name des impersonierten Benutzers zurückgegeben. Für Clients der Version 10.0.1 und früher sowie auch für HTTP- und TDS-Clients wird eine leere Zeichenfolge zurückgegeben.
- **PID** Die Prozesskennung des Clients (nur Windows und Unix)
- **THREAD** Die Thread-ID des Clients (nur Windows und Unix)
- **TIMEZONEADJUSTMENT** Die Anzahl der Minuten, die der Coordinated Universal Time (UTC) hinzugefügt werden muss, damit die Ortszeit für die Verbindung angezeigt wird.
- **VERSION** Die Version der verwendeten Clientbibliothek, mit Haupt- und Nebenversionsnummern sowie einer Erstellungsnummer (zum Beispiel 16.0.0.1403).

**Standardwert**

Leere Zeichenfolge

**Bemerkungen**

Dieser Verbindungsparameter wird von Embedded SQL-, ODBC- oder OLE DB- oder ADO.NET-Clients sowie von Anwendungen zum Datenbankserver gesendet, die den SQL Anywhere JDBC-Treiber verwenden. Von Sybase Open Client- oder jConnect-Anwendungen aus ist er nicht verfügbar.

Er besteht aus einer generierten Zeichenfolge, die Informationen über den Clientprozess wie z.B. die IP-Adresse des Clientcomputers, das Betriebssystem etc. enthält. Die Zeichenfolge ist im Datenbankserver mit der Verbindung verknüpft und Sie können sie mit der folgenden Anweisung abrufen:

```
SELECT CONNECTION_PROPERTY( 'AppInfo' );
```

Wenn Sie in Ihren Clientverbindungsparametern eine Debug-Logdatei definieren, wird die AppInfo-Zeichenfolge der Datei hinzugefügt.

### Siehe auch

- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „request\_timeout-Option“ auf Seite 664
- AppInfo-Verbindungseigenschaft auf Seite 712

### Beispiel

Verbindung mit der Beispieldatenbank von Interactive SQL aus (der SQL Anywhere JDBC-Treiber wird standardmäßig verwendet):

```
dbisql -c "UID=DBA;PWD=sql;DBF=%SQLANYSAMPl6%\demo.db"
```

Anwendungsinformationen anzeigen:

```
SELECT CONNECTION_PROPERTY( 'AppInfo' );
```

Das Ergebnis lautet folgendermaßen (in einer einzigen Zeichenfolge):

```
IP=ip-address;
HOST=computer-name;
OSUSER=user-name;
OS='Windows XP Build 2600 Service Pack 2';
EXE='C:\Program Files\SQL Anywhere 16\Bin32\dbisql.exe';P
ID=0xcac;
THREAD=0xca8;VERSION=16.0.0.1403;
API=iAnywhereJDBC;
TIMEZONEADJUSTMENT=-240
```

Stellen Sie von Interactive SQL aus eine Verbindung mit der Beispieldatenbank her, wobei Sie Ihre eigenen Informationen an die AppInfo-Eigenschaft anfügen:

```
dbisql -c "UID=DBA;PWD=sql;DBF=%SQLANYSAMPl6%\demo.db;APP=Interactive SQL
connection"
```

Anwendungsinformationen anzeigen:

```
SELECT CONNECTION_PROPERTY( 'AppInfo' );
```

Das Ergebnis lautet folgendermaßen (in einer einzigen Zeichenfolge):

```
IP=ip-address;
HOST=computer-name;
OSUSER=user-name;
OS=Windows XP Build 2600 Service Pack 2;
EXE=C:\Program Files\SQL Anywhere 16\Bin32\dbisql.exe;
PID=0xcac;
THREAD=0xba8;
VERSION=16.0.0.1403;
```

```
API=iAnywhereJDBC;  
TIMEZONEADJUSTMENT=-240;  
APPINFO='Interactive SQL connection'
```

## Verbindungsparameter AutoStart (ASTART)

Steuert, ob ein Personal Datenbankserver gestartet wird, wenn keine Verbindung mit einem Datenbankserver hergestellt werden kann.

### Syntax

{ **AutoStart** | **ASTART** }={ YES | NO }

### Verwendungszweck

Überall

### Standardwert

YES

### Bemerkungen

Standardmäßig gilt: Wenn während eines Verbindungsversuches kein Datenbankserver gefunden wird und eine Datenbankdatei, ein Datenbankname oder der START-Verbindungsparameter angegeben wurde, wird ein Personal Datenbankserver auf demselben Computer gestartet. Sie können dieses Verhalten deaktivieren, indem Sie den Verbindungsparameter AutoStart (ASTART) in der Verbindungszeichenfolge auf NO setzen. Der Datenbankserver wird nicht automatisch gestartet, wenn der Host-Verbindungsparameter angegeben ist oder der CommLinks-Parameter (LINKS) den Wert TCPIP enthält.

Um die Abfrageperformance für automatisch gestartete Datenbanken zu erhöhen, starten Sie die Datenbank so bald wie möglich, auch wenn sich noch keine Benutzer damit verbinden. Dadurch kann sich der Cache vorwärmen, bis Abfragen in der Datenbank ausgeführt werden.

#### Hinweis

Der AutoStart-Verbindungsparameter steuert, ob ein Datenbankserver automatisch gestartet wird. Er steuert *nicht*, ob eine Datenbank automatisch gestartet wird. Verwenden Sie den DatabaseName-Verbindungsparameter, um eine Verbindung mit einer bereits gestarteten Datenbank herzustellen. Verwenden Sie den DatabaseFile-Verbindungsparameter, um eine Verbindung mit einer bereits gestarteten Datenbank herzustellen oder ggf. eine Datenbank automatisch zu starten und eine Verbindung mit dieser Datenbank herzustellen.

### Siehe auch

- „Verbindungsparameter DatabaseName (DBN)“ auf Seite 354
- „Verbindungsparameter DatabaseFile (DBF)“ auf Seite 351
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Cachevorwärmung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Fehlerbehandlung: Datenbankserver suchen“ auf Seite 83
- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „Verbindungsparameter Elevate“ auf Seite 358

## Verbindungsparameter AutoStop (ASTOP)

Steuert, ob eine Datenbank gestoppt wird, wenn keine weiteren offenen Nicht-HTTP-Verbindungen mehr bestehen.

### Syntax

{ **AutoStop** | **ASTOP** }={ YES | NO }

### Verwendungszweck

Überall

### Standardwert

YES

### Bemerkungen

Standardmäßig wird jeder von einer Zeichenfolge für die Verbindung gestartete Server gestoppt, wenn keine weiteren Nicht-HTTP-Verbindungen mehr zu ihm bestehen. Ebenso wird jede von einer Zeichenfolge für die Verbindung geladene Datenbank entladen, sobald keine weiteren Nicht-HTTP-Verbindungen mehr zu ihr bestehen. Dieses Verhalten ist gleichbedeutend mit "AutoStop=YES".

Wenn Sie "AutoStop=NO" angeben, laufen alle in dieser Verbindung gestarteten Datenbanken weiter, auch wenn keine Nicht-HTTP-Verbindungen mehr vorhanden sind. Als Folge davon bleibt auch der Datenbankserver betriebsbereit.

Wenn die einzige Verbindung mit einer Datenbank eine HTTP-Verbindung ist und die Datenbank so konfiguriert wurde, dass sie automatisch gestoppt wird, wird bei der Trennung der HTTP-Verbindung die Datenbank nicht automatisch gestoppt. Wenn eine für den automatischen Stopp konfigurierte Datenbank eine HTTP-Verbindung und eine Befehlssequenz oder eine TDS-Verbindung hat und die letzte Befehlssequenz eine Trennung bewirkt oder die TDS-Verbindung getrennt wird, dann wird die Datenbank gestoppt und alle HTTP-Verbindungen werden getrennt.

Der Verbindungsparameter AutoStop (ASTOP) wird nur beim Verbinden mit einer gerade nicht laufenden Datenbank verwendet. Wenn die Datenbank bereits gestartet ist, wird er ignoriert.

Bei NET-Anwendungen sollten Sie mit der Verwendung des Verbindungsparameters AutoStop vorsichtig sein. Das Schließen einer Verbindung schließt diese, was die Anwendung betrifft, aber aktive Verbindungen bleiben geöffnet, wenn Verbindungspooling aktiviert ist. Aus diesem Grund wird der Datenbankserver entgegen den Erwartungen nicht herunterfahren.

### Siehe auch

- „Datenbankserveroption -ga“ auf Seite 238
- „Verbindungsparameter AutoStop (ASTOP)“ auf Seite 342
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungspooling“ [*SQL Anywhere Server - Programmierung*]
- „Datenbanken starten und stoppen“ auf Seite 156
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Verbindungsparameter CharSet (CS)

Legt den Zeichensatz fest, der in dieser Verbindung verwendet werden soll

### Syntax

{ CharSet | CS }={ NONE | *character-set* }

### Verwendungszweck

Überall

### Zulässige Werte

- **NONE** Wenn Sie "CharSet=NONE" angeben, wird angefordert, dass die Verbindung den CHAR-Zeichensatz der Datenbank verwendet.
- **character-set** Geben Sie das zu verwendende Zeichensatzlabel an. Weitere Hinweise über gültige Zeichensatzwerte finden Sie unter [„Empfohlene Zeichensätze und Kollationen“ auf Seite 529](#).

### Standardwert

Der lokale Zeichensatz

### Bemerkungen

Wenn Sie einen Wert für CharSet liefern, wird der angegebene Zeichensatz für die aktuelle Verbindung verwendet.

Wenn Sie Daten entladen, können Sie den Zeichensatz mithilfe des Verbindungsparameters CharSet festlegen.

Um eine verlustreiche Zeichensatzkonvertierung zu vermeiden, wird davon abgeraten, den Verbindungsparameter CharSet einzustellen, wenn Unicode-Client-APIs verwendet werden. Unicode-Client-APIs sind ADO.NET, OLE DB und der SQL Anywhere JDBC-Treiber. ODBC ist ebenfalls eine Unicode-Client-API, wenn die (Unicode) Wide-Funktionen verwendet werden.

### Siehe auch

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Informationen zur Sprachumgebung“ auf Seite 512](#)
- [„SACHARSET-Umgebungsvariable“ auf Seite 472](#)
- [„Zeichensatz der Sprachumgebung“ auf Seite 512](#)

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge gibt an, dass für die Verbindung die Windows-Codepage 1252 verwendet werden soll:

```
CharSet=windows-1252
```

## Verbindungsparameter CommBufferSize (CBSIZE)

Legt die Maximalgröße von Kommunikationspaketen fest

### Syntax

{ **CommBufferSize** | **CBSIZE** }=*size*[ **k** ]

### Verwendungszweck

Überall

### Zulässige Werte

- **size** Diese Ganzzahl legt die Maximalgröße von Kommunikationspaketen fest. Der Standardwert wird in Byte angegeben, Sie können jedoch **k** verwenden, um Einheiten in KByte anzugeben. Der Mindestwert für CommBufferSize ist 500 Byte, der Höchstwert 65535 Byte.

### Standardwert

Wenn kein Wert "CommBufferSize" eingestellt ist, wird "CommBufferSize" von der Einstellung auf dem Server gesteuert, die den Standardwert von 7300 Byte für alle Betriebssysteme außer Windows Mobile hat. Unter Windows Mobile ist der Standardwert 1460 Byte.

### Bemerkungen

Mit dem Protokoll-Stack wird die maximale Größe eines Paketes im Netzwerk festgelegt. Wenn Sie "CommBufferSize" größer als den von Ihrem Netzwerk erlaubten Wert setzen, werden die Kommunikationspakete von der Netzwerksoftware aufgeteilt. Die Standardgröße ist ein Vielfaches der maximalen Standard-Ethernet-TCP/IP-Paketgröße (1460 Byte).

Ein höherer Wert für die Paketgröße kann die Performance für mehrzeilige Datenabrufe und Abrufe von größeren Zeilen verbessern, erhöht aber auch den Speicherbedarf von Client und Server.

Wenn für "CommBufferSize" auf dem Client kein Wert angegeben wurde, benutzt die Verbindung die Puffergröße des Servers. Wenn für "CommBufferSize" auf dem Client ein Wert angegeben wurde, benutzt die Verbindung diesen Wert.

Wenn "CommBufferSize" mit der Datenbankserveroption -p festgelegt wird, verwenden alle Clients, für die kein eigener Wert angegeben wurde, diesen Wert.

### Siehe auch

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Datenbankserveroption -p“ auf Seite 271](#)
- [„Tipp: Paketgröße ändern, um die Performance zu steigern“ \[\*SQL Anywhere Server - SQL-Benutzerhandbuch\*\]](#)

### Beispiel

So wird die Puffergröße auf 1460 Byte eingestellt:

```
...  
CommBufferSize=1460  
...
```

Sie können diesen Parameter auch setzen, indem Sie seinen Wert in das Textfeld **CommBufferSize** auf der Registerkarte **Erweitert** des Fensters **ODBC-Konfiguration für SQL Anywhere** eingeben.

## Verbindungsparameter CommLinks (LINKS)

Gibt clientseitige Netzwerkprotokolloptionen an

### Syntax

```
{ CommLinks | LINKS }={ [ SharedMemory | ShMem ] | ALL | [ TCPIP | TCP ] } [, ... ] string
```

### Verwendungszweck

Der CommLinks-Verbindungsparameter (LINKS) kann für Verbindungen mit einem Netzwerk-Datenbankserver (dbsrv16) verwendet werden und ist für Verbindungen mit einem Personal Datenbankserver (dbeng16) optional.

### Zulässige Werte

Bei den Werten für den Verbindungsparameter CommLinks (LINKS) wird die Groß- und Kleinschreibung berücksichtigt. Sie sind im Folgenden aufgelistet:

- **SharedMemory (ShMem)** Startet das Shared Memory-Protokoll für die Kommunikation auf demselben Computer. Dies ist die Standardeinstellung. SharedMemory wird von dem Client an erster Stelle für den Suchvorgang verwendet, ohne dabei die Stellung dieses Protokolls in der Reihenfolge der Protokolle in der durch den Verbindungsparameter CommLinks(LINKS) festgelegten Liste zu beachten.
- **ALL** Es wird versucht, eine Verbindung zuerst über das Shared Memory-Protokoll und dann über TCP/IP herzustellen.
- **TCPIP (TCP)** Die Verbindung wird über das Kommunikationsprotokoll TCP/IP eingerichtet. TCP/IP wird unter allen Betriebssystemen unterstützt.

Sie können zusätzliche Netzwerkprotokolloptionen für TCP/IP angeben.

### Standardwert

SharedMemory

### Bemerkungen

#### Hinweis

Sie sollten den CommLinks-Verbindungsparameter (LINKS) nur dann verwenden, wenn Sie andere TCP/IP-Protokolloptionen als HOST oder ServerPort (PORT) angeben müssen. Verwenden Sie andernfalls den Host-Verbindungsparameter.

Sie können nicht sowohl CommLinks als auch Host in einer Verbindungszeichenfolge angeben.

Wenn Sie den CommLinks-Verbindungsparameter (LINKS) für eine TCP/IP-Verbindung verwenden, geben Sie mithilfe des ServerName-Verbindungsparameters (Server) einen Servernamen an.

Sie müssen den CommLinks-Verbindungsparameter (LINKS) verwenden, wenn Sie die Verbindung mit einer Datenbank in der Cloud mithilfe einer Clientbibliothek aus Version 10.0.0 bis 12.0.0 herstellen möchten, weil diese Clientbibliotheken keine Verbindungsumleitung unterstützen.

Wenn Sie keinen Verbindungsparameter Host oder CommLinks (LINKS) angeben, sucht der Client nur auf dem aktuellen Computer nach einem Datenbankserver, und das nur unter Verwendung der Shared Memory-Verbindung. Das ist das Standardverhalten und entspricht "CommLinks=ShMem". Das Shared Memory-Protokoll ist die schnellste Kommunikationsverbindung zwischen einem Client und einem Datenbankserver, die auf dem gleichen Computer laufen. Dies ist für Anwendungen typisch, die eine Verbindung mit dem Personal Datenbankserver herstellen.

Hinweise zur Sicherung von Shared Memory-Verbindungen unter Unix finden Sie unter [„Allgemeine Sicherheitstipps“ auf Seite 1406](#).

Wenn Sie TCPIP und SharedMemory oder CommLinks=ALL angeben, wird zuerst eine Shared Memory-Verbindung und dann eine Verbindung über TCP/IP versucht, wenn der Datenbankserver über Shared Memory nicht gefunden werden kann. In der folgenden Verbindungszeichenfolge wird beispielsweise zuerst Shared Memory versucht:

```
"UID=DBA;PWD=sql;Server=demo;DBN=demo;LINKS=TCPIP,SHMEM"
```

Ein Personal Datenbankserver wird nicht automatisch gestartet, wenn der Host-Verbindungsparameter angegeben ist oder der CommLinks-Parameter (LINKS) den Wert TCPIP enthält.

Das Kommunikationsprotokoll TCP/IP wird auf dem Datenbankserver mit der Option -x aktiviert.

### Siehe auch

- [„Host-Verbindungsparameter“ auf Seite 363](#)
- [„Verbindungsparameter ServerName \(Server\)“ auf Seite 383](#)
- [„Netzwerkprotokolloptionen“ auf Seite 388](#)
- [„Kommunikationsprotokolle“ auf Seite 102](#)
- [„Datenbankserveroption -x“ auf Seite 305](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Fehlerbehandlung: Datenbankserver-Adressinformationen für schnellere Verbindungen in sasrv.ini zwischenspeichern“ auf Seite 94](#)
- [CommLink-Verbindungseigenschaft auf Seite 716](#)

### Beispiel

Im folgenden Fragment einer Verbindungszeichenfolge wird versucht, eine Verbindung zum Datenbankserver namens demo herzustellen, der im aktuellen Subnetz läuft:

```
CommLinks=tcPIP;Server=demo;UID=DBA;PWD=sql;
```

Im folgenden Fragment einer Verbindungszeichenfolge wird versucht, eine Verbindung zum Datenbankserver namens demo herzustellen. Zunächst wird versucht, eine Verbindung über Shared Memory herzustellen. Wenn der Datenbankserver über Shared Memory nicht gefunden wird, folgt der Versuch einer Verbindung über TCP/IP.

```
CommLinks=tcPIP,shmem;Server=demo;UID=DBA;PWD=sql
```

In der folgenden Verbindungszeichenfolge wird versucht, eine Verbindung mit dem Server demo herzustellen, der auf dem Host kangaroo läuft.

```
CommLinks=tcPIP(HOST=kangaroo);Server=demo;UID=DBA;PWD=sql
```

Alternativ können Sie den Host-Verbindungsparameter verwenden, um eine Verbindung zum Server demo herzustellen, der auf dem Host kangaroo läuft.

```
Host=kangaroo;Server=demo;UID=DBA;PWD=sql
```

## Verbindungsparameter Compress (COMP)

Schaltet die Komprimierung einer Verbindung ein oder aus.

### Syntax

```
{ Compress | COMP }={ YES | NO }
```

### Verwendungszweck

Überall außer bei TDS-Verbindungen. TDS-Verbindungen (einschließlich jConnect) unterstützen die Verbindungskomprimierung von SQL Anywhere nicht.

### Standardwert

NO

### Bemerkungen

Die zwischen SQL Anywhere-Client und Datenbankserver gesendeten Pakete können durch Angabe des Verbindungsparameters Compress (COMP) komprimiert werden. Unter bestimmten Voraussetzungen kann das Komprimieren einer Verbindung die Performance verbessern. Umfangreiche Datenübertragungen mit stark komprimierbaren Daten erzielen im Allgemeinen die besten Komprimierungswerte.

Wenn kein Wert für den Compress-Kommunikationsparameter gesetzt ist, steuert die Einstellung des Datenbankservers den Komprimierungsstatus, dessen Standardwert "Keine Komprimierung" ist. Wenn die Einstellungen von Client und Datenbankserver unterschiedlich sind, gelten die Clienteinstellungen.

Es wird empfohlen, dass Sie im betreffenden Netzwerk und mit der betreffenden Anwendung eine Performanceanalyse durchführen, bevor Sie die Kommunikationskomprimierung in einer Produktionsumgebung einsetzen.

Wenn Sie die Komprimierung für alle entfernten Verbindungen des Datenbankservers aktivieren möchten, verwenden Sie die Serveroption -pc.

Die Komprimierung wird bei Verbindungen auf demselben System über eine Kommunikationsverbindung nicht aktiviert, auch wenn die Option -pc oder der Parameter COMPRESS=YES verwendet werden.

### Siehe auch

- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Datenbankserveroption -pc“ auf Seite 272
- „Komprimierungseinstellungen für die Kommunikation“ auf Seite 112
- „Tipp: Komprimierung mit Umsicht verwenden“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge aktiviert die Paketkomprimierung:

`Compress=YES`

Das folgende Fragment einer Verbindungszeichenfolge deaktiviert die Paketkomprimierung:

`Compress=NO`

## Verbindungsparameter CompressionThreshold (COMPTH)

Erhöht oder verringert die Größenbegrenzung für die Komprimierung von Paketen.

### Syntax

`{ CompressionThreshold | COMPTH }=size[ k ]`

### Verwendungszweck

Überall außer TDS. Nur für komprimierte Verbindungen

### Zulässige Werte

- **size** Diese Ganzzahl gibt die Größenbegrenzung für die Komprimierung von Paketen an. Der Standardwert wird in Byte angegeben, Sie können jedoch **k** verwenden, um Einheiten in KByte anzugeben. Wenn Client und Datenbankserver unterschiedliche Einstellungen für den Komprimierungsschwellenwert aufweisen, gelten die Clienteneinstellungen. Der unterstützte Mindestwert ist 1 Byte und der unterstützte Höchstwert ist 32767 Byte. Werte unter 80 sind nicht empfehlenswert.

### Standardwert

120

Falls kein Komprimierungswert festgelegt wurde, richtet er sich nach den Servereinstellungen mit einem Standardwert von 120 Byte.

### Bemerkungen

Die Änderung der Komprimierung kann die Performance einer komprimierten Verbindung verbessern, weil Sie festlegen können, dass nur die Pakete komprimiert werden, bei denen die Komprimierung zu einer Erhöhung der Übertragungsgeschwindigkeit der Pakete führt.

Wenn die Komprimierung aktiviert ist, werden einzelne Pakete je nach ihrer Größe komprimiert oder nicht. SQL Anywhere komprimiert beispielsweise keine Pakete, die kleiner sind als der Komprimierungsschwellenwert, auch wenn die Kommunikationskomprimierung aktiviert ist. Kleine Pakete (weniger als 100 Byte) werden im Allgemeinen überhaupt nicht komprimiert. Da CPU-Zeit erforderlich ist, um Pakete zu komprimieren, ist die versuchte Komprimierung kleiner Pakete im Endeffekt möglicherweise sogar ein Nachteil für die Performance.

Das Absenken des Komprimierungsschwellenwerts kann die Performance in sehr langsamen Netzwerken verbessern, während das Erhöhen des Komprimierungsschwellenwerts die Performance dank einer

geringeren CPU-Nutzung verbessern kann. Da allerdings das Absenken des Komprimierungsschwellenwerts die CPU-Nutzung auf dem Client und dem Server erhöht, sollte eine Performanceanalyse erfolgen, um zu ermitteln, ob eine Änderung des Komprimierungsschwellenwerts vorteilhaft ist.

**Siehe auch**

- [„Datenbankserveroption -pt“ auf Seite 273](#)
- [„Komprimierungseinstellungen für die Kommunikation“ auf Seite 112](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)

**Beispiel**

Eine Verbindung mit einem Schwellenwert von 100 Byte herstellen

```
CompressionThreshold=100
```

## Verbindungsparameter ConnectionName (CON)

Benennt eine Verbindung, um das Umschalten auf diese Verbindung in Anwendungen mit mehreren Verbindungen zu erleichtern

**Syntax**

```
{ ConnectionName | CON }=connection-name
```

**Verwendungszweck**

Überall

**Zulässige Werte**

- **connection-name** Diese Zeichenfolge gibt einen Namen für die spezifische Verbindung an, die Sie gerade herstellen.

**Standardwert**

Kein Verbindungsname

**Bemerkungen**

Dieser Verbindungsparameter ist optional. Sie müssen diesen Wert nur angeben, wenn Sie mehr als eine Verbindung herstellen und zwischen ihnen hin- und herschalten.

Der Verbindungsname ist nicht derselbe wie der Name der Datenquelle.

**Siehe auch**

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„SET CONNECTION-Anweisung \[Interactive SQL\] \[ESQL\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [Name-Verbindungseigenschaft auf Seite 727](#)

## Beispiel

Herstellen einer Datenbankverbindung mit dem Namen "first-con":

```
CON=first-con
```

## Verbindungsparameter ConnectionPool (CPOOL)

Steuert das Verhalten des Client-Verbindungspooling.

### Syntax

```
ConnectionPool={ NO | YES [ ( [ Timeout=timeout-sec; ] [ MaxCached=max-cached-conn ] ) ] }
```

### Verwendungszweck

Alle Plattformen mit Ausnahme von Windows Mobile und Unix-Clients ohne Threading.

### Zulässige Werte

- **timeout-sec** Das Inaktivitäts-Timeout des Verbindungspools (in Sekunden). Standardwert ist 60 Sekunden. Im Cache zwischengespeicherte Verbindungen, die nicht innerhalb der durch den Wert von *timeout-sec* angegebenen Zeitspanne wiederverwendet werden, werden getrennt und sind nicht mehr für die Wiederverwendung verfügbar.
- **max-cached-conn** Die maximale Anzahl der im Cache zwischengespeicherten Verbindungen von jeder Anwendung. Der Standardwert beträgt fünf Verbindungen. Eine Verbindung wird im Cache zwischengespeichert, wenn sie getrennt wird und die durch den Wert *max-cached-conn* angegebene maximale Anzahl von Verbindungen noch nicht erreicht ist. Die Verbindung wird erneut initialisiert und die Verbindung im Cache bleibt mit dem Datenbankserver verbunden, selbst wenn die Anwendung diese getrennt hat. Weitere Informationen über die durchgeführten Bereinigungs- und Reinitialisierungsaufgaben finden Sie unter „[Verbindungspooling](#)“ auf Seite 77.

### Standardwert

YES

### Bemerkungen

Verbindungspooling kann die Performance von Anwendungen verbessern, die viele kurze Verbindungen zum Datenbankserver herstellen. Wenn eine Verbindung getrennt wird, wird sie automatisch im Cache abgelegt und kann wiederverwendet werden, wenn die Anwendung erneut eine Verbindung herstellt. Bei einer Verbindung, die im Pool aufgenommen werden soll, kann der Verbindungsname anders lauten, alle anderen Verbindungsparameter müssen jedoch identisch sein.

### Siehe auch

- „[Verbindungspooling](#)“ auf Seite 77
- „[Verbindungsparameter und Verbindungszeichenfolgen](#)“ auf Seite 31
- [ConnPoolCachedCount-Datenbankeigenschaft](#) auf Seite 771
- [ConnPoolHits-Datenbankeigenschaft](#) auf Seite 771
- [ConnPoolMisses-Datenbankeigenschaft](#) auf Seite 771

**Beispiel**

Das folgende Fragment einer Verbindungszeichenfolge deaktiviert Verbindungspooling:

```
ConnectionPool=NO;
```

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird Verbindungspooling mit einem Maximum von 10 Verbindungen im Cache aktiviert.

```
CPOOL=YES(MaxCached=10);
```

## Verbindungsparameter DatabaseFile (DBF)

Gibt an, welche Datenbankdatei Sie laden und mit welcher Datenbankdatei Sie sich verbinden wollen, wenn eine Datenbank gestartet wird, die nicht läuft.

**Syntax**

```
{ DatabaseFile | DBF }=filename
```

**Verwendungszweck**

Lokale Datenbankserver

**Zulässige Werte**

- **filename** Diese Zeichenfolge gibt den Pfad und den Dateinamen einer Datenbank an, die gestartet werden soll.

Wenn der Dateiname keine Erweiterung enthält, suchen SQL Anywhere-Programme nach einer Datei mit der Erweiterung *.db*.

Der Suchpfad der Datei ist relativ zum Arbeitsverzeichnis des Datenbankservers. Wenn Sie den Datenbankserver von einer Eingabeaufforderung aus starten, ist das Arbeitsverzeichnis das Verzeichnis, in dem Sie sich beim Ausführen des Befehls befinden. Wenn Sie den Datenbankserver über ein Symbol oder eine Verknüpfung starten, ist es das vom Symbol oder der Verknüpfung festgelegte Arbeitsverzeichnis. Es wird empfohlen, dass Sie einen kompletten Pfad mit dem Dateinamen angeben.

UNC-Dateinamen werden unterstützt. Weitere Hinweise zur Verwendung von UNC-Dateinamen finden Sie unter „[Syntax des SQL Anywhere-Datenbankservers](#)“ auf Seite 203.

**Standardwert**

Es gibt keine Standardeinstellung.

**Bemerkungen**

Wenn Sie nicht sicher sind, ob die Datenbank läuft, können Sie den DatabaseFile-Verbindungsparameter (DBF) verwenden, um die Datenbank zu starten und eine Verbindung mit ihr herzustellen.

Wenn Sie die Verbindungsparameter DatabaseFile (DBF) und DatabaseName (DBN) angeben, wird versucht, eine Verbindung mit einer laufenden Datenbank mit dem angegebenen Datenbanknamen herzustellen. (Der DatabaseFile-Verbindungsparameter wird ignoriert.) Wenn das fehlschlägt, wird

versucht, die Datenbank unter Verwendung des durch den DatabaseFile-Verbindungsparameter angegebenen Pfads automatisch zu starten und ihr den durch den DatabaseName-Verbindungsparameter angegebenen Namen zuzuordnen.

Wenn Sie den DatabaseFile-Verbindungsparameter (DBF) angeben, jedoch nicht den DatabaseName-Verbindungsparameter (DBN), wird versucht, eine Verbindung mit einer laufenden Datenbank mit demselben Namen wie die angegebene Datei herzustellen (wobei Pfad und Erweiterung entfernt werden). Wenn das fehlschlägt, wird versucht, die Datenbank unter Verwendung des durch den DatabaseFile-Verbindungsparameter angegebenen Pfads automatisch zu starten.

Eine Datenbank kann nicht auf einem Netzwerkservers automatisch gestartet werden, es sei denn, dieses Verhalten wird durch die Datenbankserveroption -gd explizit zugelassen.

Wenn ein laufender Datenbankserver nicht gefunden werden kann, wird standardmäßig ein Personal Datenbankserver automatisch gestartet.

Für bereitgestellte Anwendungen sollten Sie einen Datenbankservernamen mit dem ServerName-Parameter (Server) angeben, wenn Sie versuchen, eine nicht ausgeführte Datenbankdatei automatisch zu starten. Andernfalls stellt die Anwendung möglicherweise eine Verbindung zu einem anderen als dem gewünschten Datenbankserver her. Der Datenbankserver könnte sich z.B. mit einer anderen Version des SQL Anywhere-Servers verbinden, der Teil einer eingebetteten Anwendung ist und bereits ausgeführt wird.

### Vorsicht

Die Datenbankdatei muss sich auf demselben Computer wie der Datenbankserver befinden. Der Start einer Datenbankdatei, die auf einem Netzlaufwerk liegt, kann zu einer Beschädigung der Datei führen.

### Siehe auch

- [DatabaseFile-Verbindungsparameter \(DBF\) verwenden auf Seite 28](#)
- [„Datenbankserveroption -gd“ auf Seite 240](#)
- [„Verbindungsparameter CommLinks \(LINKS\)“ auf Seite 345](#)
- [„Verbindungsparameter DatabaseName \(DBN\)“ auf Seite 354](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Verbindungen mit eingebetteten Datenbanken“ auf Seite 28](#)

### Beispiel

Mit dem Verbindungsparameter DatabaseFile (DBF) im folgenden Beispiel wird die Beispieldatenbank *demo.db* geladen und eine Verbindung zu ihr hergestellt:

```
"DBF=%SQLANYAMP16%\demo.db"
```

Die nachstehenden zwei Beispiele gehen davon aus, dass Sie die Datenbankdatei *cities.db* gestartet und die Datenbank "Kitchener" wie folgt umbenannt haben:

```
dbeng16 cities.db -n Kitchener
```

Um erfolgreich eine Datenbank zu starten, eine Verbindung mit ihr herzustellen und ihr den Namen "Kitchener" zuzuordnen, müssen Sie die folgenden Werte für die Verbindungsparameter DBN und DBF angeben:

```
DBN=Kitchener;DBF=cities.db
```

Durch Angabe von `DBF=cities.db` wird mit der laufenden Datenbank namens "Kitchener" keine Verbindung hergestellt.

## Verbindungsparameter DatabaseKey (DBKEY)

Startet eine verschlüsselte Datenbank mit einer Verbindungsanforderung

### Syntax

```
{ DatabaseKey | DBKEY }=key
```

### Verwendungszweck

Überall

### Zulässige Werte

- **key** Der Chiffrierschlüssel ist eine Zeichenfolge mit einer Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Datenbankschlüssel dürfen keine führenden bzw. nachgestellten Leerzeichen oder Semikola enthalten.

### Standardwert

Keine

### Bemerkungen

Sie müssen diesen Parameter angeben, wenn Sie eine verschlüsselte Datenbank mit einer Verbindungsanforderung starten. Normalerweise brauchen Sie diesen Parameter nicht anzugeben.

Um Kommunikationspakete zwischen Clientanwendungen und dem Datenbankserver zu sichern, verwenden Sie die Serveroption `-ec` und Transportschichtssicherheit.

### Siehe auch

- „Transportschichtssicherheit“ auf Seite 1444
- „Konfigurieren der Clientanwendung für die Verwendung der Transportschichtssicherheit“ auf Seite 1455
- „Datenbankserveroption `-ec`“ auf Seite 230
- „Datenbankoption `-ek`“ auf Seite 326
- „Datenbankserveroption `-ep`“ auf Seite 233
- „Datenbankserveroption `-es`“ auf Seite 234
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359

### Beispiel

Das folgende Fragment veranschaulicht die Verwendung des Verbindungsparameters `DatabaseKey` (`DBKEY`):

```
"UID=DBA;PWD=sql;Server=myeng;DBKEY=V3moj3952B;DBF=%SQLANY16%\demo.db"
```

## Verbindungsparameter DatabaseName (DBN)

Identifiziert eine laufende Datenbank oder ordnet einer Datenbank, die gestartet wird, einen Namen zu.

### Syntax

{ **DatabaseName** | **DBN** }=*database-name*

### Verwendungszweck

Überall

### Zulässige Werte

- **database-name** Diese Zeichenfolge gibt den Namen einer Datenbank an, die bereits auf einem Datenbankserver läuft, oder benennt eine Datenbank, die gestartet wird.

### Standardwert

Es gibt keine Standardeinstellung.

### Bemerkungen

Wenn eine Datenbank auf einem Server gestartet wird, erhält sie einen Datenbanknamen vom Administrator unter Verwendung der Option -n oder vom Datenbankserver unter Verwendung des Dateinamens, wobei Erweiterung und Pfad weggelassen werden.

**Mit einer laufenden Datenbank verbinden** Wenn die Datenbank, mit der Sie sich verbinden möchten, bereits läuft, verwenden Sie den DatabaseName-Verbindungsparameter (DBN). Eine Verbindung wird nur hergestellt, wenn der Name der laufenden Datenbank mit *database-file* übereinstimmt.

Um sich mit der Dienstprogrammdatenbank zu verbinden, verwenden Sie den Datenbanknamen **utility\_db**.

Der DatabaseName-Verbindungsparameter (DBN) wird gegenüber dem DatabaseFile-Verbindungsparameter (DBF) empfohlen, wenn Sie Versuche, die Datenbank zu starten, verhindern möchten, sofern sie nicht bereits läuft.

**Eine nicht laufende Datenbank starten** Wenn Sie die Verbindungsparameter DatabaseName (DBN) und DatabaseFile (DBF) angeben, wird versucht, eine Verbindung mit einer laufenden Datenbank mit dem angegebenen Datenbanknamen herzustellen. (Der DatabaseFile-Verbindungsparameter wird ignoriert.) Wenn das fehlschlägt, wird versucht, die Datenbank unter Verwendung des durch den DatabaseFile-Verbindungsparameter angegebenen Pfads automatisch zu starten und ihr den durch den DatabaseName-Verbindungsparameter angegebenen Namen zuzuordnen.

Es wird empfohlen, zum Benennen von Datenbanken den DatabaseName-Verbindungsparameter (DBN) zu verwenden statt den DatabaseSwitches-Verbindungsparameter (DBS) mit der Option -n oder den START-Verbindungsparameter mit der Option -n.

**Siehe auch**

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„DatabaseName-Protokolloption \(DBN\)“ auf Seite 397](#)
- [„Verbindungsparameter DatabaseSwitches \(DBS\)“ auf Seite 355](#)
- [„Die Dienstprogrammdatenbank“ auf Seite 145](#)
- [„Häufig verwendete Verbindungsszenarien“ auf Seite 32](#)

**Beispiel**

Verwenden Sie die folgende Verbindungszeichenfolge, um die Datenbank *cities.db* zu starten und ihr den Namen "Kitchener" zuzuordnen:

```
"DBF=cities.db;DBN=Kitchener;UID=DBA;PWD=sql"
```

Verwenden Sie die folgende Verbindungszeichenfolge, um eine Verbindung mit einer laufenden Datenbank namens "Kitchener" herzustellen:

```
"DBN=Kitchener;UID=DBA;PWD=sql"
```

## Verbindungsparameter DatabaseSwitches (DBS)

Setzt beim Starten einer Datenbank datenbankspezifische Optionen

**Syntax**

```
{ DatabaseSwitches | DBS }=database-options
```

**Verwendungszweck**

Überall

**Zulässige Werte**

- **database-options** Diese Zeichenfolge gibt Datenbankoptionen an, die sich auf die Datenbankdatei beziehen. Siehe [„Datenbankoptionen \(Datenbank\)“ auf Seite 321](#).

Wenn Sie die Datenbankserveroptionen angeben möchten, verwenden Sie den StartLine-Verbindungsparameter.

**Standardwert**

Keine Optionen

**Bemerkungen**

Verwenden Sie diesen Verbindungsparameter, um eine Verbindung mit einem Datenbankserver herzustellen und auf diesem eine Datenbank zu starten. Wenn der Datenbankserver nicht läuft, startet dieser Verbindungsparameter den Datenbankserver automatisch mit der angegebenen Datenbank und den angegebenen Optionen.

Wenn die Datenbank vor dem Verbindungsversuch bereits läuft, wird der DatabaseSwitches-Verbindungsparameter ignoriert.

Wenn der Datenbankserver die durch DatabaseFile angegebene Datenbank startet, verwendet der Server den angegebenen DatabaseSwitches-Verbindungsparameter, um Startoptionen für die Datenbank zu ermitteln.

### Hinweis

Der Verbindungsparameter DatabaseName (DBN) wird für die Benennung von Datenbanken empfohlen, und nicht der Verbindungsparameter DatabaseSwitches (DBS) mit der Option -n.

### Siehe auch

- „Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungsparameter DatabaseName (DBN)“ auf Seite 354
- „Verbindungsparameter DatabaseKey (DBKEY)“ auf Seite 353
- „Verbindungsparameter StartLine (START)“ auf Seite 385

### Beispiel

Mit dem folgenden Befehl wird eine Verbindung zum Standard-Datenbankserver hergestellt. Die Datenbankdatei *demo.db* (DatabaseFile (DBF)-Verbindungsparameter) wird geladen, in my-db (DatabaseName (DBN)-Verbindungsparameter) umbenannt und schreibgeschützt gestartet (Option -r).

```
dbisql -c "UID=DBA;PWD=sql;DBF=%SQLANYSAMPl6%\demo.db;DBN=my-db;DBS=-r"
```

## Verbindungsparameter DataSourceName (DSN)

Teilt dem ODBC-Treibermanager oder der Embedded SQL-Bibliothek mit, wo sie in der Registrierung oder in der Systeminformationsdatei (standardmäßig *odbc.ini* benannt) nach ODBC-Datenquellen-Informationen suchen soll

### Syntax

{ **DataSourceName** | **DSN** }=*data-source-name*

### Verwendungszweck

Überall

### Zulässige Werte

- **data-source-name** Diese Zeichenfolge gibt den Namen der ODBC-Datenquelle an, die Verbindungsinformationen für Ihre Datenbank enthält.

### Standardwert

Es gibt keinen Standard-Datenquellennamen.

### Bemerkungen

Es ist für ODBC-Anwendungen allgemein üblich, nur einen Datenquellennamen an ODBC zu senden. Der ODBC-Treibermanager und der ODBC-Treiber ermitteln die Position der Datenquelle, die den Rest der Verbindungsparameter enthält.

In SQL Anywhere können Embedded SQL-Anwendungen die ODBC-Datenquellen auch zum Speichern von Verbindungsparametern verwenden.

**Siehe auch**

- „Verbindungsparameter FileDataSourceName (FILEDSN)“ auf Seite 362
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „ODBC-Datenquellen unter Unix“ auf Seite 49
- „ODBC-Datenquellen“ auf Seite 38

**Beispiel**

Der folgende Parameter verwendet einen Datenquellennamen:

```
DSN=My Database
```

## Verbindungsparameter DisableMultiRowFetch (DMRF)

Deaktiviert die Möglichkeit des Abrufs mehrerer Zeilen über das Netzwerk

**Syntax**

```
{ DisableMultiRowFetch | DMRF }={ YES | NO }
```

**Verwendungszweck**

Überall

**Standardwert**

NO

**Bemerkungen**

Wenn der Datenbankserver eine einfache Abrufanforderung erhält, verlangt die Anwendung standardmäßig zusätzliche Zeilen. Sie können dieses Verhalten deaktivieren, indem Sie diesen Parameter auf YES setzen.

Das Setzen des DisableMultiRowFetch-Verbindungsparameters (DMRF) auf YES ist äquivalent mit dem Setzen der prefetch-Datenbankoption auf "Off".

**Siehe auch**

- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Cursor in Prozeduren, Triggern, benutzerdefinierten Funktionen und Batches“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „prefetch-Option“ auf Seite 653
- „Prefetch“ [*SQL Anywhere Server - Programmierung*]

**Beispiel**

Das folgende Verbindungszeichenfolge-Fragment verhindert Prefetch:

```
DMRF=YES
```

## Verbindungsparameter Elevate

Erhöht die Rechte von automatisch gestarteten Datenbankserverprogrammdateien unter Windows Vista oder höher.

### Syntax

**Elevate**={ YES | NO }

### Verwendungszweck

Windows Vista oder höher

### Standardwert

NO

### Bemerkungen

Wenn Sie in Ihrer Verbindungszeichenfolge die Einstellung ELEVATE=YES angeben, können Clientprozesse, deren Rechte nicht erhöht wurden, Server mit erhöhten Rechten automatisch starten. Dies ist unter Windows Vista oder höher möglicherweise notwendig, wenn für den Zugriff auf die Datenbankdatei Administrationsrechte erforderlich sind. Dieser Parameter wird ignoriert, wenn der Datenbankserver nicht automatisch gestartet wird.

### Siehe auch

- [Elevate-Verbindungsparameter verwenden auf Seite 29](#)

### Beispiel

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird ein Datenbankserver automatisch gestartet und die Rechte werden erhöht:

```
"Elevate=YES;START=dbsrv16"
```

## Verbindungsparameter EncryptedPassword (ENP)

Liefert ein Kennwort, das in verschlüsselter Form in einer Datenquelle gespeichert ist.

### Syntax

{ **EncryptedPassword** | **ENP** }=*password*

### Verwendungszweck

Überall

### Zulässige Werte

- **password** Diese Zeichenfolge ist ein verschlüsseltes Kennwort für die Datenbank, mit der die Verbindung hergestellt werden soll.

**Standardwert**

Keine

**Bemerkungen**

Jeder Benutzer einer Datenbank hat ein Kennwort. Das Kennwort muss angegeben werden, damit der Benutzer eine Verbindung mit der Datenbank herstellen kann.

Der Verbindungsparameter EncryptedPassword (ENP) wird zur Angabe eines verschlüsselten Kennworts verwendet. Das verschlüsselte Kennwort einer Anwendung kann in der Verbindungszeichenfolge enthalten sein. Wenn die Verbindungsparameter Password (PWD) und EncryptedPassword (ENP) beide angegeben werden, ist Password (PWD) vorrangig.

**Vorsicht**

Bei der Erstellung einer Datenquelle ist es nicht empfehlenswert, dass das verschlüsselte Kennwort Teil der Definition ist. Auch wenn sowohl das Fenster **ODBC-Konfiguration für SQL Anywhere** im **ODBC-Datenquellen-Administrator** unter Windows als auch das SQL Anywhere-Datenquellen-Dienstprogramm (dbdsn) über diese Funktion verfügen, stellt das Aufnehmen dieser Informationen in die Definition ein Sicherheitsrisiko dar.

Sie können ein in einer ODBC-Datenquelle gespeichertes Kennwort mithilfe des Datenquellen-Dienstprogramms (dbdsn) mit der Option -pe verschlüsseln.

Unter Unix werden diese Datenquelleninformationen in der Systeminformationsdatei (standardmäßig *.odbc.ini* genannt) gespeichert. Weitere Hinweise darüber, wie nach dieser Systeminformationsdatei gesucht wird, finden Sie unter „[ODBC-Datenquellen unter Unix](#)“ auf Seite 49.

**Siehe auch**

- „Datenquellen-Dienstprogramm (dbdsn)“ auf Seite 905
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungsparameter Password (PWD)“ auf Seite 378

## Verbindungsparameter Encryption (ENC)

Verschlüsselt die zwischen der Clientanwendung und dem Datenbankserver gesendeten Pakete, wobei Transportschichtssicherheit oder einfache Verschlüsselung verwendet wird

**Syntax**

```
{ Encryption | ENC }={ NONE
| SIMPLE
| TLS ( [ FIPS={ Y | N }; ]
TRUSTED_CERTIFICATE=public-certificate;
[ CERTIFICATE_COMPANY=organization; ]
[ CERTIFICATE_NAME=common-name; ]
[ CERTIFICATE_UNIT=organization-unit ] )
```

**Verwendungszweck**

TLS: nur für TCP/IP unterstützt

NONE oder SIMPLE: überall

### Zulässige Werte

- **NONE** Akzeptiert nicht verschlüsselte Kommunikationspakete
- **SIMPLE** Hierbei werden Pakete mit einfacher Verschlüsselung angenommen, die auf allen Plattformen und in früheren Versionen von SQL Anywhere unterstützt wird. Die einfache Verschlüsselung verwendet keine Serverauthentifizierung, starke Ellipsenkurven- bzw. RSA-Verschlüsselung oder andere Funktionen der Transportschichtsicherheit.

Wenn der Datenbankserver einfache Verschlüsselung akzeptiert, aber keine unverschlüsselten Verbindungen annimmt, verwendet jede Nicht-TDS-Verbindung, die versucht, keine Verschlüsselung anzuwenden, automatisch einfache Verschlüsselung.

Ein Starten des Datenbankservers mit `-ec SIMPLE` teilt dem Datenbankserver mit, nur Verbindungen zu akzeptieren, die einfache Verschlüsselung verwenden. TLS-Verbindungen (RSA- und RSA FIPS-zertifiziert) schlagen fehl und Verbindungen, die keine Verschlüsselung anfordern, verwenden einfache Verschlüsselung.

- **TLS** Akzeptiert Kommunikationspakete mit RSA-Verschlüsselung. Geben Sie bei FIPS-zertifizierter RSA-Verschlüsselung **FIPS=Y** an. RSA FIPS verwendet eine separate zertifizierte Bibliothek, ist aber mit SQL Anywhere-Servern der Version 9.0.2 oder höher kompatibel, die RSA angeben.

Die Verbindung schlägt fehl, wenn der Algorithmus nicht mit der beim Erstellen Ihrer Zertifikate verwendeten Verschlüsselung übereinstimmt.

Der Client kann die folgenden Argumente verwenden, um die Feldwerte im öffentlichen Zertifikat des Servers zu überprüfen:

- `trusted_certificate`
- `certificate_company`
- `certificate_unit`
- `certificate_name`

Weitere Hinweise zur Verifizierung von Zertifikatsfeldern für die Serverauthentifizierung finden Sie unter [Zertifikatsfelder überprüfen auf Seite 1456](#).

### Standardwert

NONE

### Bemerkungen

Sie können diesen Parameter verwenden, um die Kommunikation zwischen Clientanwendungen und dem Datenbankserver mit Transportschichtsicherheit oder einfacher Verschlüsselung zu sichern.

**Hinweis**

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

Sie können die CONNECTION\_PROPERTY-Systemfunktion verwenden, um die Verschlüsselungseinstellungen für die aktuelle Verbindung abzurufen:

```
SELECT CONNECTION_PROPERTY ( 'Encryption' );
```

Die Funktion gibt einen der folgenden Werte zurück: "None", "Simple", "rsa\_tls" oder "rsa\_tls\_fips", je nach der von der Verbindung verwendeten Art der Verschlüsselung.

Siehe „CONNECTION\_PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

**Siehe auch**

- „Konfigurieren der Clientanwendung für die Verwendung der Transportschichtsicherheit“ auf Seite 1455
- „Datenbankserveroption -ec“ auf Seite 230
- „Datenbankoption -ek“ auf Seite 326
- „Datenbankserveroption -ep“ auf Seite 233
- „Datenbankserveroption -es“ auf Seite 234
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungsparameter DatabaseKey (DBKEY)“ auf Seite 353
- „certificate\_company-Protokolloption“ auf Seite 392
- „certificate\_name-Protokolloption“ auf Seite 393
- „certificate\_unit-Protokolloption“ auf Seite 394
- „trusted\_certificates-Protokolloption“ auf Seite 421
- Encryption-Verbindungseigenschaft auf Seite 719
- „Transportschichtsicherheit“ auf Seite 1444
- „Digitale Zertifikate“ auf Seite 1447

**Beispiel**

Das folgende Fragment einer Verbindungszeichenfolge stellt mithilfe von Transportschichtsicherheit und RSA-Verschlüsselung eine Verbindung zu einem Datenbankserver her:

```
"HOST=myhost;SERVER=myserver;ENCRYPTION=TLS(FIPS=N;TRUSTED_CERTIFICATE=rsaroot.crt)"
```

Das folgende Fragment einer Verbindungszeichenfolge stellt mithilfe einer einfachen Verschlüsselung eine Verbindung zu einem Datenbankserver her:

```
"HOST=myhost;SERVER=myserver;ENCRYPTION=simple"
```

## Verbindungsparameter EngineName (ENG) (veraltet)

Dieser Verbindungsparameter wird nicht mehr empfohlen. Verwenden Sie stattdessen den Verbindungsparameter ServerName (Server).

### Siehe auch

- [„Verbindungsparameter ServerName \(Server\)“ auf Seite 383](#)

## Verbindungsparameter FileDataSourceName (FILEDSN)

Dieser Verbindungsparameter informiert die Clientbibliothek, dass es eine ODBC-Datei-Datenquelle mit Informationen über die Datenbank gibt, mit der eine Verbindung hergestellt werden soll.

### Syntax

{ FileDataSourceName | FILEDSN }=*file-data-source-name*

### Verwendungszweck

Überall

### Zulässige Werte

- **file-data-source-name** Diese Zeichenfolge gibt den Namen der Datei-Datenquelle an, die Verbindungsinformationen für Ihre Datenbank enthält.

### Standardwert

Es gibt keinen Standardnamen.

### Bemerkungen

Datei-Datenquellen beinhalten dieselben Informationen wie in der Registrierung gespeicherte ODBC-Datenquellen. Datei-Datenquellen können einfach an Endbenutzer verteilt werden, sodass die Verbindungsdaten nicht auf jedem System neu aufgebaut werden müssen.

Sowohl ODBC- als auch Embedded SQL-Anwendungen können Datei-Datenquellen verwenden.

### Siehe auch

- [„Dateidatenquellen unter Windows“ auf Seite 46](#)
- [„Verbindungsparameter DataSourceName \(DSN\)“ auf Seite 356](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Dateidatenquellen unter Windows“ auf Seite 46](#)

## Verbindungsparameter ForceStart (FORCE)

Startet einen Datenbankserver, ohne zu überprüfen, ob ein Server läuft.

### Syntax

{ ForceStart | FORCE }={ YES | NO }

**Verwendungszweck**

Nur mit der Funktion `db_start_engine`

**Standardwert**

NO

**Bemerkungen**

Wenn Sie "ForceStart=YES" festlegen, überprüft die `db_start_engine`-Funktion vor dem Starten des Servers nicht, ob ein Server läuft.

**Siehe auch**

- „`db_start_engine`-Funktion“ [*SQL Anywhere Server - Programmierung*]
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31

## Host-Verbindungsparameter

Akzeptiert einen Hostnamen oder eine IP-Adresse und eine optionale Portnummer, die den Client darauf hinweist, wo sich der Datenbankserver befindet.

**Syntax**

**Host**={ *hostname* | *ip-address* }[ *:port-number* ] ...

**Verwendungszweck**

Überall. Der Host-Verbindungsparameter wird für Verbindungen mit einem Netzwerk-Datenbankserver empfohlen und zeigt die Verwendung von TCP/IP an.

**Zulässige Werte**

- **hostname** Der Name des Computers, auf dem der Datenbankserver läuft. Die Liste der Hostwerte ist eine durch Komma getrennte Liste und kann wahlweise auch eine Portnummer enthalten (durch einen Doppelpunkt getrennt). Sie können **localhost** verwenden, um den aktuellen Computer zu identifizieren.
- **ip-address** Die Zeichenfolge muss in Form einer IP-Adresse angegeben werden, und sie kann wahlweise auch eine Portnummer enthalten (durch einen Doppelpunkt getrennt). Die Liste der IP-Adressen ist eine durch Komma getrennte Liste.

Bei IPv6-Adressen, die eine Portnummer enthalten, müssen Sie die Adresse entweder in eckige Klammern oder in Klammern setzen. Zum Beispiel, `Host=[fd77:ab34:2238::3894]:8933`, wobei 8933 die Portnummer ist.

- **port-number** Die vom Datenbankserver verwendete Portnummer. Die Standard-Portnummer ist 2638.

**Standardwert**

Keine

**Bemerkungen**

Der Host-Verbindungsparameter gibt einen oder mehrere Hostnamen (oder IP-Adressen) und optional Portnummern an, wodurch der Client weiß, wo ein Datenbankserver läuft.

Der Host-Verbindungsparameter identifiziert ein oder mehrere Computersysteme, auf denen Datenbankserver laufen. Ein Datenbankserver wird nicht automatisch gestartet, wenn der Host-Verbindungsparameter angegeben wird.

Wenn auf einem Computersystem mehr als ein Datenbankserver läuft und kein Port angegeben wird, muss der ServerName-Verbindungsparameter verwendet werden, um zu kennzeichnen, mit welchem Datenbankserver die Verbindung hergestellt werden soll. Es wird empfohlen, dass Sie immer den ServerName-Parameter verwenden, insbesondere bei eingebetteten Anwendungen.

Option	Beschreibung
Server und Port angeben	<code>host=myhost:1234;</code> <code>servername=myserver</code>  Eine Verbindung wird nur mit einem Datenbankserver hergestellt, der den angegebenen Port abhört und dem angegebenen Servernamen entspricht.
Server, aber nicht Port angeben	<code>host=myhost;</code> <code>servername=myserver</code>  Eine Verbindung wird mit dem Datenbankserver mit dem angegebenen Servernamen hergestellt.
Weder Server noch Port angeben	<code>host=myhost</code>  Es wird versucht, eine Verbindung mit einem Datenbankserver herzustellen, der Port 2638 abhört.

Wenn mehrere Adressen angegeben sind, werden sie in der folgenden Reihenfolge versucht:

1. Die angegebenen Adressen werden mit dem Datenbankserver-Adressencache (*sasrv.ini*) abgeglichen. Wenn eine Übereinstimmung gefunden wird, wird diese Adresse im Datenbankservercache zuerst versucht.
2. Die Adressen werden in der Reihenfolge versucht, in der sie angegeben sind.

Wenn Sie den Host-Parameter verwenden, werden keine UDP-Pakete gesendet, wenn genügend Informationen für die eindeutige Identifikation des Servers angegeben wurden (ein Hostname und eine Portnummer). Wenn weder eine Portnummer noch ein Datenbankservername angegeben ist, wird davon ausgegangen, dass die Portnummer 2638 lautet, und der Client sendet kein Broadcasting aus. Wenn jedoch der Client einen Hostnamen und einen Datenbankservernamen hat, aber keine Portnummer, sendet er ein UDP-Paket an Port 2638 auf dem angegebenen Host, um die Portnummer zu ermitteln. Siehe [„Fehlerbehandlung: Datenbankserver mithilfe des Host-Verbindungsparameters suchen“](#) auf Seite 87.

Sie können die LocalOnly-Protokolloption nicht zusammen mit der HOST-Protokolloption oder dem Host-Verbindungsparameter angeben.

**Hinweis**

Der Host-Verbindungsparameter deaktiviert die Verwendung von Shared Memory. Wenn Sie den Host-Verbindungsparameter verwenden möchten, um eine Verbindung mit einem Personal Datenbankserver herzustellen, müssen Sie das Kommunikationsprotokoll TCP/IP auf dem Datenbankserver mit der Option -x aktivieren. Außerdem müssen Sie den Hostnamen **localhost** verwenden, wenn Sie eine Verbindung mit einem Personal Datenbankserver über TCP/IP herstellen.

Sie sollten den CommLinks-Verbindungsparameter (LINKS) nur dann verwenden, wenn Sie andere TCP/IP-Protokolloptionen als HOST oder ServerPort (PORT) angeben müssen.

Sie können nicht sowohl CommLinks als auch Host in einer Verbindungszeichenfolge angeben.

**Siehe auch**

- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399
- „Häufig verwendete Verbindungsszenarien“ auf Seite 32
- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „Verbindungsparameter ServerName (Server)“ auf Seite 383

**Beispiel**

Wenn Sie wissen, dass ein Datenbankserver mit dem Namen SalesDB auf einem Computer mit dem Namen Elora an der Standard-Portnummer läuft, können Sie die folgende Verbindungszeichenfolge zum Verbinden mit dem Datenbankserver verwenden:

```
UID=DBA;PWD=sql;Server=SalesDB;Host=Elora:2638
```

Wenn Sie die Portnummer, an der der Datenbankserver läuft, nicht kennen, verwenden Sie die folgende Verbindungszeichenfolge für die Verbindung mit dem Datenbankserver SalesDB auf dem Computer mit dem Namen Elora:

```
UID=DBA;PWD=sql;Server=SalesDB;Host=Elora
```

## Verbindungsparameter Idle

Legt den Zeitraum für das Inaktivitäts-Timeout einer Verbindung fest.

**Syntax**

```
Idle=timeout-value
```

**Verwendungszweck**

Überall außer bei TDS-Verbindungen. TDS-Verbindungen (einschließlich jConnect) ignorieren den Idle-Verbindungsparameter von SQL Anywhere.

**Zulässige Werte**

- **timeout-value** Das Inaktivitäts-Timeout der Verbindung (in Minuten). Der Mindestwert für den Verbindungsparameter Idle ist 1 Minute, und der unterstützte Höchstwert ist 32767 Minuten. Wenn Sie 0 angeben, wird die Überprüfung des Inaktivitäts-Timeouts deaktiviert.

### Standardwert

240 Minuten (TCP/IP)

0 (Shared Memory)

### Bemerkungen

Der Idle-Verbindungsparameter betrifft nur die aktuelle Verbindung. Mehrere Verbindungen auf demselben Datenbankserver können auf unterschiedliche Timeoutwerte gesetzt werden.

Wenn der Idle-Verbindungsparameter nicht verwendet wird, hängt der Inaktivitäts-Timeoutwert für TCP/IP-Verbindungen von der Datenbankserveroption -ti ab. Wenn die Datenbankserveroption -ti und der Idle-Verbindungsparameter angegeben werden, hängt der Inaktivitäts-Timeoutwert vom Verbindungsparameter ab.

### Siehe auch

- [„Datenbankserveroption -ti “ auf Seite 291](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Timeoutwerte anpassen“ auf Seite 1114](#)
- [IdleTimeout-Verbindungseigenschaft auf Seite 722](#)

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge setzt den Timeoutwert für diese Verbindung auf 10 Minuten:

```
"Host=myhost;IDLE=10"
```

## Verbindungsparameter Integrated (INT)

Legt fest, ob ein integriertes Login versucht werden kann

### Syntax

{ **Integrated** | **INT** }={ **YES** | **NO** }

### Verwendungszweck

Überall

### Zulässige Werte

- **YES** Ein integriertes Login wird versucht. Wenn der Verbindungsversuch fehlschlägt und die login\_mode-Option auf "Standard,Integrated" gesetzt ist, wird ein Standardlogin versucht.
- **NO** Dies ist die Standardeinstellung. Es wird kein integriertes Login versucht.

### Standardwert

NO

### Bemerkungen

Damit eine Clientanwendung ein integriertes Login verwenden kann, muss der Server mit der Datenbankoption `login_mode` laufen, die auf einen Wert gesetzt ist, der "Integrated" enthält.

### Siehe auch

- „`login_mode`-Option“ auf Seite 623
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Integrierte Windows-Logins“ auf Seite 52

### Beispiel

Das folgende Datenquellen-Fragment verwendet ein integriertes Login:

```
INT=YES
```

## Verbindungsparameter Kerberos (KRB)

Gibt an, ob eine Kerberos-Authentifizierung bei der Verbindung mit dem Datenbankserver verwendet werden kann

### Syntax

```
{ Kerberos | KRB } = { YES | NO | SSPI | GSS-API-library-file }
```

### Verwendungszweck

Alle Plattformen außer Windows Mobile.

### Zulässige Werte

- **YES** Es wird ein Kerberos-authentifiziertes Login versucht.
- **NO** Es wird kein Kerberos-authentifiziertes Login versucht. Dies ist die Standardeinstellung.
- **SSPI** Ein Kerberos-authentifiziertes Login wird versucht, und die integrierte Windows SSPI-Schnittstelle wird anstatt einer GSS-API-Bibliothek verwendet. SSPI kann nur auf Windows-Plattformen verwendet werden, und sie kann mit keinem anderen Key Distribution Center (KDC, Schlüsselverteilungszentrum) als dem Domain Controller Active Directory-KDC verwendet werden. Wenn Ihr Windows-Clientcomputer bereits bei einer Windows-Domäne angemeldet ist, kann SSPI verwendet werden, ohne einen Kerberos-Client installieren oder konfigurieren zu müssen.

#### Hinweis

SSPI kann von SQL Anywhere-Clients nur im Kerberos-Verbindungsparameter verwendet werden. SQL Anywhere-Datenbankserver können SSPI nicht verwenden - sie benötigen einen unterstützten Kerberos-Client, bei dem es sich nicht um SSPI handelt.

- **GSS-API-library-file** Ein Kerberos-authentifiziertes Login wird versucht, und diese Zeichenfolge gibt den Dateinamen der Kerberos GSS-API-Bibliothek (oder ein Shared Object unter Unix) an. Dies ist nur erforderlich, wenn der Kerberos-Client einen anderen als den Standard-Dateinamen für die

Kerberos GSS-API-Bibliothek verwendet, oder wenn mehrere GSS-API-Bibliotheken auf dem Computer installiert sind.

### Standardwert

NO

### Bemerkungen

Die Verbindungsparameter UserID und Password werden ignoriert, wenn ein Kerberos-authentifiziertes Login verwendet wird.

Um die Kerberos-Authentifizierung zu verwenden, muss ein Kerberos-Client bereits installiert und konfiguriert sein (bei SSPI nicht erforderlich), muss sich der Benutzer bereits bei Kerberos angemeldet haben (ein gültiges Ticket-erteilendes Kerberos-Ticket haben) und muss der Datenbankserver für Kerberos-authentifizierte Logins aktiviert und konfiguriert sein.

### Siehe auch

- „Datenbankserveroption -kl “ auf Seite 260
- „Datenbankserveroption -kr (nicht mehr empfohlen)“ auf Seite 262
- „Datenbankserveroption -krb “ auf Seite 263
- „Kerberos-Authentifizierung“ auf Seite 63
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SSPI für Kerberos-Logins unter Windows verwenden“ auf Seite 72

### Beispiel

```
Kerberos=YES  
Kerberos=SSPI  
Kerberos=c:\Program Files\MIT\Kerberos\bin\gssapi32.dll
```

## Verbindungsparameter Language (LANG)

Gibt die Sprache der Verbindung an

### Syntax

{ **Language** | **LANG** }=*language-code*

### Verwendungszweck

Überall

### Zulässige Werte

- **language-code** Die beiden Buchstaben, die für eine Sprache stehen. Mit der Einstellung "LANG=DE" wird die Standardsprache auf Deutsch gesetzt.

Weitere Informationen zu Sprachcodes finden Sie unter „[Sprache der Sprachumgebung](#)“ auf Seite 510.

**Standardwert**

Die Sprache, die (in der Reihenfolge) durch SALANG, das Dienstprogramm dblank oder das Installationsprogramm festgelegt wurde.

**Bemerkungen**

Dieser Verbindungsparameter legt die Sprache für die Verbindung fest. Fehler oder Warnungen vom Server werden in der angegebenen Sprache angezeigt, sofern der Server diese Sprache unterstützt.

Falls keine Sprache angegeben ist, wird die Standardsprache benutzt. Standardsprache ist die Sprache, die (in der Reihenfolge) durch SALANG, das Dienstprogramm dblank oder das Installationsprogramm festgelegt wurde.

Dieser Verbindungsparameter gilt nur für die Verbindung. Meldungen, die von den Tools und Dienstprogrammen von SQL Anywhere zurückgegeben werden, erscheinen in der Standardsprache, die vom Server zurückgegebenen Meldungen hingegen in der Sprache der Verbindung.

**Siehe auch**

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)

## Verbindungsparameter LazyClose (LCLOSE)

Steuert, ob Cursoranforderungen bis zur nächsten Anforderung in die Warteschlange gestellt oder sofort ausgeführt werden sollen. Das in die Warteschlange Stellen von Anforderungen zum Schließen von Cursors erspart einen Roundtrip und verbessert die Performance.

**Syntax**

{ LazyClose | LCLOSE }={ YES | NO | AUTO }

**Verwendungszweck**

Überall

**Zulässige Werte**

- **YES** Das in die Warteschlange Stellen von Anforderungen zum Schließen von Cursors erspart zwar einen Roundtrip, kann aber zu Sperren und anderen Ressourcenbindungen führen, nachdem der Cursor vom Client geschlossen wurde. Der Cursor wird geschlossen, wenn die nächste Anforderung an den Datenbankserver über dieselbe Verbindung gesendet wird. Alle Cursor-Stabilitätssperren der Isolationsstufe 1 gelten weiterhin für den Cursor, während sich die Datenbankanforderung CLOSE cursor-name in der Warteschlange befindet.
- **NO** Den Cursor sofort schließen.
- **AUTO** Die Anforderungen zum Schließen von Cursors in die Warteschlange stellen und einen Roundtrip ersparen, aber nur dann, wenn es nichts daran ändert, wie lange Sperren gehalten oder signifikante Serverressourcen gebunden werden. Wenn der Cursor Cursor-Stabilitätssperren der Isolationsstufe 1 verwendet oder möglicherweise signifikante Serverressourcen bindet, die erst nach dem Schließen des Cursors freigegeben werden, dann wird der Cursor sofort geschlossen. Eine

Abfrage, die eine Arbeitstabelle erfordert, ist ein Beispiel für einen Cursor, der signifikante Serverressourcen bindet.

### Standardwert

AUTO

### Bemerkungen

Wenn dieser Verbindungsparameter auf YES oder AUTO gesetzt ist, werden Cursor bis zur nächsten Datenbankanforderung nicht geschlossen.

Ein Aktivieren dieser Option kann die Performance verbessern, wenn Ihr Netzwerk eine unbefriedigende Verarbeitungszeit hat oder Ihre Anwendung viele Anforderungen zum Öffnen und Schließen von Cursorsn sendet.

### Siehe auch

- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Tipp: Anforderungen zwischen Client und Server reduzieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## LivenessTimeout-Verbindungsparameter (LTO)

Steuert das Herunterfahren von Verbindungen, die nicht mehr intakt sind

### Syntax

{ **LivenessTimeout** | **LTO** }=*timeout-value*

### Verwendungszweck

Nur Netzwerkservers

Alle Plattformen mit Ausnahme von Unix-Anwendungen, die ohne Threading arbeiten

### Zulässige Werte

- **timeout-value** Der Zeitraum für das Verfügbarkeits-Timeout der Verbindung (in Sekunden). Der Mindestwert für den LivenessTimeout-Verbindungsparameter ist 30 Sekunden, und der Höchstwert ist 32767 Sekunden. Wenn Sie 0 angeben, wird die Überprüfung des Verfügbarkeits-Timeouts deaktiviert. Jeder Wert ungleich NULL, der niedriger als der Mindestwert ist, wird auf den Mindestwert zurückgesetzt. Beispiel: Eine Verbindungszeichenfolge, die "LivenessTimeout=5" enthält, verwendet "LivenessTimeout=30". Falls kein LivenessTimeout-Wert gesetzt ist, wird das Verfügbarkeits-Timeout durch die Einstellung auf dem Server gesteuert, die standardmäßig 120 Sekunden beträgt.

### Standardwert

Keine

### Bemerkungen

Ein **Verfügbarkeitspaket** wird regelmäßig über ein Client/Server TCP/IP-Kommunikationsprotokoll gesendet, um zu bestätigen, dass eine Verbindung besteht. Wenn der Client während der LivenessTimeout-Periode läuft ohne eine Verfügbarkeitsanforderung oder ein Antwortpaket zu entdecken, wird die Verbindung beendet.

Verfügbarkeitspakete werden gesendet, wenn eine Verbindung während einem bis zwei Dritteln der LivenessTimeout-Periode keine Pakete übertragen hat.

Wenn mehr als 200 Verbindungen mit einem Server bestehen, berechnet der Server automatisch einen höheren Verfügbarkeitswert auf der Basis des definierten LivenessTimeout-Werts. So kann der Server auch eine große Anzahl von Verbindungen effizient verwalten.

Sie können diesen Parameter auch setzen, indem Sie seinen Wert in das Textfeld **LivenessTimeout** auf der Registerkarte **Erweitert** des Fensters **ODBC-Konfiguration für SQL Anywhere** eingeben.

### Siehe auch

- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Datenbankserveroption -tl“ auf Seite 292](#)
- [LivenessTimeout-Verbindungseigenschaft auf Seite 724](#)

### Beispiel

Mit dem folgenden Fragment einer Verbindungszeichenfolgen-wird ein LivenessTimeout-Wert von 10 Minuten gesetzt:

```
LTO=600
```

## Verbindungsparameter LogFile (LOG)

Sendet Clientfehlermeldungen und Fehlersuchnachrichten an eine Datei

### Syntax

{ **LogFile** | **LOG** }=*filename*

### Verwendungszweck

Überall

### Zulässige Werte

- **filename** Diese Zeichenfolge gibt den Namen der Datei an, in der Clientfehlermeldungen und Fehlersuchnachrichten gespeichert werden. Wenn der Dateiname keinen Suchpfad mit einschließt, ist er relativ zum aktuellen Arbeitsverzeichnis der Clientanwendung.

### Standardwert

Keine Logdatei

### Bemerkungen

Der Verbindungsparameter Logfile (LOG) ist verbindungsspezifisch, sodass Sie von einer einzelnen Anwendung aus verschiedene LogFile-Argumente für verschiedene Verbindungen einstellen können.

Folgende Logdateiinhalte sind üblich:

```
Di Jan 22 2013 10:59:3
10:59:31 Verbindungsversuch mit:
UID=DBA;PWD=*****;DBF='C:\Users\Public\Documents\SQL Anywhere 16\Samples
\demo.db';ServerName=demo16;START='C:\Programme\SQL Anywhere
16\Bin32\dbeng16.exe';CON=SQL_DBC_10b9d400;ASTOP=YES;LOG=c:\logs\test.txt
10:59:31 Verbindungsversuch mit einem laufenden Server...
10:59:31 SharedMemory-Verbindung wird versucht (keine im Cache sasrv.ini
gespeicherte Adresse)
10:59:31 Verbunden mit Server über SharedMemory
10:59:31 Verbunden mit SQL Anywhere Server Version 16.0.0.1403
10:59:31 Hinweise zur Anwendung:
10:59:31 IP=192.138.151.100;HOST=MyComputer1-PC;OSUSER=user1;OS='Windows 7
Build 7601 Service Pack 1';EXE='C:\Program Files\SQL Anywhere
16\bin32\dbisql.exe';PID=0x145c;THREAD=0x508;VERSION=16.0.0.1403;API=iAnywher
eJDBC;TIMEZONEADJUSTMENT=-300
10:59:31 Verbunden mit dem Server, Verbindung mit einer laufenden Datenbank
wird versucht...
10:59:31 [ 205] Verbindung mit der Datenbank erfolgreich eingerichtet
10:59:31 [ 205] Anzahl der abgerufenen Zeilen reduziert auf 16
entsprechend der
10:59:31 [ 205] Abrufpufferbegrenzung. Verbindungsparameter
'PrefetchBuffer' kann Performance verbessern.
```

### Siehe auch

- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „LogFile-Protokoloption (LOG)“ auf Seite 408

### Beispiel

Mit der folgenden Befehlszeile wird Interactive SQL gestartet und eine Verbindung zur Beispieldatenbank mit einem LogFile (LOG)-Verbindungsparameter hergestellt:

```
dbisql -c "DSN=SQL Anywhere 16 Demo;LOG=c:\logs\test.txt"
```

## Verbindungsparameter NewPassword (NEWPWD)

Ermöglicht es Benutzern, Kennwörter ohne Unterstützung des DBA zu ändern, selbst wenn diese abgelaufen sind.

### Syntax

```
{ NewPassword | NEWPWD }={ password-string | * }
```

### Verwendungszweck

Die Clientbibliothek, die zur Eingabe eines neuen Kennworts auffordert, wird nur unter Microsoft Windows unterstützt.

### Zulässige Werte

- **password-string** Wenn der Benutzer ein neues Kennwort liefert, authentifiziert der Datenbankserver die Benutzer-ID und das Kennwort und versucht, das Kennwort zu ändern, bevor die Option `login_procedure` aufgerufen wird. Dieser Prozess ermöglicht es einem Benutzer, ein abgelaufenes Kennwort ohne Beteiligung eines DBA zu ändern. Wenn Sie die Option `verify_password_function` gesetzt haben, wird das neue Kennwort überprüft. Wenn Sie mit einem integrierten oder Kerberos-Login authentifizieren, wird das ursprüngliche Kennwort nicht überprüft und der Datenbankserver ignoriert den neuen Kennwortwert, und das Kennwort wird nicht geändert.
- \* Wenn Sie unter Microsoft Windows den Spezialwert \* verwenden, fordert die Clientbibliothek während eines Verbindungsversuchs nur zur Eingabe eines neuen Kennworts auf, wenn das vorhandene Kennwort abgelaufen ist. Die Benutzer müssen ihr vorhandenes Kennwort und ihr neues Kennwort eingeben sowie ihr neues Kennwort bestätigen. Wenn der Benutzer die Felder ausfüllt und auf **OK** klickt, wird das alte Kennwort authentifiziert und der Datenbankserver versucht, das Kennwort zu ändern. Wenn Sie die Option `verify_password_function` gesetzt haben, wird das neue Kennwort überprüft. Der Prozess der Überprüfung, ob das Kennwort eines Benutzers abgelaufen ist, der Aufforderung zur Eingabe eines Kennworts und der Authentifizierung und Änderung des Kennworts wird mit einem einzigen Verbindungsaufwurf an die Clientbibliothek eingeleitet.

### Standardwert

Das Kennwort wird nicht geändert und die Clientbibliothek fordert nicht zur Eingabe eines neuen Kennworts auf.

### Bemerkungen

Dieser Verbindungsparameter ist sehr effizient, wenn Sie eine Login-Richtlinie unter Verwendung der Optionen `password_life_time` oder `password_expiry_on_next_login` implementieren. Alternativ können Sie eine Kennwortablauf-Richtlinie implementieren, bei der `login_procedure` den Fehler `Kennwort ist abgelaufen` meldet.

Ein Benutzer erhält den Fehler `Kennwort ist abgelaufen`, wenn seine Umgebung die Aufforderung zur Kennworтеingabe nicht unterstützt. In einer Microsoft Windows-Umgebung verhindert das Eingabeaufforderungsfenster möglicherweise nicht korrekt eine Interaktion mit dem Fenster der aufrufenden Anwendung (es ist möglicherweise nicht modal oder hat nicht das korrekte übergeordnete Fenster), wenn die aufrufende Anwendung mehrere Fenster der obersten Ebene hat oder die Anwendungsfenster der obersten Ebene minimiert sind.

Wenn Sie in einer Windows-Umgebung die ODBC-Funktion `SQLDriverConnect` verwenden und das Argument `DriverCompletion` einen anderen Wert als `SQL_DRIVER_NOPROMPT` hat, fordert die Verbindung zur Eingabe eines neuen Kennworts auf, wenn das Kennwort abgelaufen ist. Die Verbindung kann zur Eingabe eines neuen Kennworts in OLE DB auffordern, wenn die Eigenschaft `DBPROP_INIT_PROMPT` einen anderen Wert als `DBPROP_PROMPT_NOPROMPT` hat. Beide Fälle verhalten sich so, als ob der Verbindungsparameter `NewPassword=*` angegeben wurde.

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

### Siehe auch

- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „login\_procedure-Option“ auf Seite 625
- „verify\_password\_function-Option“ auf Seite 704
- „post\_login\_procedure-Option“ auf Seite 651

### Beispiel

Die folgende Verbindungszeichenfolge ändert beim Verbinden das Kennwort des Benutzers Test1.

```
"UID=Test1;PWD=welcome;NEWPWD=hello"
```

Die folgende Verbindungszeichenfolge fordert in einer Windows-Umgebung den Benutzer Test1 zur Eingabe eines neuen Kennworts auf, wenn das bestehende Kennwort abgelaufen ist.

```
"UID=Test1;PWD=welcome;NEWPWD=*" "
```

## Verbindungsparameter MatView (MATVIEW)

Gibt die Zeichenfolge an, die für materialisierte Ansichten zurückgegeben werden soll, wenn die ODBC-Funktion SQLTables aufgerufen wird.

### Syntax

**MATVIEW**=string

### Verwendungszweck

ODBC

### Standardwert

VIEW

### Bemerkungen

Standardmäßig wird beim Ausführen der ODBC-Funktion SQLTables der Wert VIEW in der Spalte TABLE\_TYPE für materialisierte Ansichten zurückgegeben. Verwenden Sie den MatView-Verbindungsparameter für die Angabe eines anderen Rückgabewerts. Die von Ihnen angegebene

Zeichenfolge wird auch zurückgegeben, wenn die Funktion SQLTables mit einem TableType-Filter aufgerufen wird.

### Siehe auch

- „ODBC-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]

### Beispiel

Damit die Funktion SQLTables () materialisierte Ansichten als Typ MATERIALIZED VIEW zurückgibt, verbinden Sie sich wie folgt:

```
UID=DBA;PWD=sql;ServerName=server-name;MATVIEW=MATERIALIZED VIEW
```

## Verbindungsparameter NodeType (NODE)

Steuert die Rolle des Servers, mit dem eine Verbindung letztendlich hergestellt wird. Wird in Hochverfügbarkeitskonfigurationen, Scale-Out-Konfigurationen mit Schreibschutz und Cloud-Konfigurationen verwendet. Je nach Einstellung wird die Verbindung möglicherweise auf einen anderen Server umgeleitet, einschließlich Lastverteilung.

#### Hinweis

Scale-Out mit Schreibschutz und Datenbankspiegelung erfordern jeweils eine getrennte Lizenz. Siehe „[Getrennt lizenzierte Komponenten](#)“ [[SQL Anywhere 16 - Einführung](#)].

### Syntax

```
{ NodeType | NODE }={ DIRECT | PRIMARY | MIRROR | COPY | READONLY}
```

### Verwendungszweck

Nur Netzwerkserver

### Zulässige Werte

- **DIRECT** Dies ist die Standardeinstellung beim Verbinden mit einem Nicht-Cloud-Datenbankserver.

Wenn der NodeType Verbindungsparameter auf DIRECT eingestellt ist, akzeptiert der Datenbankserver die Verbindung, ohne eine Lastverteilung oder Weiterleitung auszuführen.

- **PRIMARY** Dies ist die Standardeinstellung beim Verbinden mit einem Cloud-Server.

Wenn der NodeType-Verbindungsparameter auf PRIMARY eingestellt ist und Sie eine Verbindung zum Primärserver hergestellt haben, wird die Verbindung akzeptiert. Wenn Sie sich mit einem Nicht-Primärserver verbunden haben (z.B. mit einem Spiegelserver, einem Kopieknotten oder einem beliebigen anderen Cloud-Datenbankserver), leitet der Datenbankserver die Verbindung zum Primärserver um.

Geben Sie beim Verbinden mit einem Cloud-Server mit diesem NodeType-Wert nicht den ServerName-Verbindungsparameter an.

- **COPY** Wenn der NodeType-Verbindungsparameter auf COPY eingestellt ist, führt der Datenbankserver die Lastverteilung aus und wählt einen Kopieknoten. In der Cloud wird der Kopieknoten zufällig ausgewählt. In einem nicht Cloud-basierten Scale-Out-System mit Schreibschutz überprüft der Datenbankserver die Kopieknoten in seinem eigenen Zweig (einschließlich seiner selbst, wenn er nicht der Stammknoten ist) und wählt den Kopieknoten mit der geringsten Last. Wenn der Datenbankserver sich nicht selbst auswählt, leitet er den Client zum ausgewählten Datenbankserver um.

Geben Sie beim Verbinden mit einem Cloud-Server mit diesem NodeType-Wert nicht den ServerName-Verbindungsparameter an.

- **MIRROR** Wenn der NodeType-Verbindungsparameter auf MIRROR eingestellt ist und Sie sich mit dem Spiegelserver verbunden haben, wird die Verbindung akzeptiert. Wenn Sie sich mit einem Nicht-Spiegelserver verbunden haben, leitet der Datenbankserver die Verbindung zum Spiegelserver um.

Geben Sie beim Verbinden mit einem Cloud-Server mit diesem NodeType-Wert nicht den ServerName-Verbindungsparameter an.

- **READONLY** Wenn der NodeType-Verbindungsparameter auf READONLY eingestellt, werden Sie mit einem beliebigen schreibgeschützten Server verbunden, entweder mit einem Kopieknoten oder mit dem Spiegelserver. Wenn es keine Kopieknoten gibt, ist dies gleichwertig mit der Einstellung MIRROR. Wenn es Kopieknoten gibt, ist dies gleichwertig mit der Einstellung COPY.

Geben Sie beim Verbinden mit einem Cloud-Server mit diesem NodeType-Wert nicht den ServerName-Verbindungsparameter an.

### Standardwert

DIRECT (Nicht-Cloud-Datenbankserver)

PRIMARY (Cloud-Datenbankserver)

### Bemerkungen

Dieser Verbindungsparameter wird von Clientanwendungen verwendet, um die Rolle des Servers zu steuern, mit dem eine Verbindung hergestellt werden soll, sowie die Lastverteilung zwischen Datenbankservern durchzuführen, die an Scale-Out mit Schreibschutz beteiligt sind. Clients geben diesen Verbindungsparameter als Hinweis darauf an, mit welchem Datenbankservertyp eine Verbindung hergestellt werden soll. Der Datenbankserver, mit dem der Client sich zunächst verbindet, bestimmt, welcher Datenbankserver die Verbindung verwalten soll, und leitet die Verbindung gegebenenfalls zum entsprechenden Datenbankserver um, indem er die Adresse dieses Datenbankservers zurückgibt. Der Client wird automatisch vom ursprünglichen Datenbankserver getrennt und verbindet sich dann mit dem angegebenen Datenbankserver.

**Verwenden von NodeType mit Nicht-Cloud-Datenbankservern** Wenn Sie COPY angeben, findet die Lastverteilung auf dem Zweig statt, der den Datenbankserver enthält, mit dem sich der Client zunächst verbindet. Ein Zweig besteht aus diesem Datenbankserver und allen seinen untergeordneten Objekten. Diese Funktion kann nützlich sein, um eine Lastverteilung zwischen Servern an geografisch getrennten Standorten durchzuführen.

Wenn eine Clientverbindung an einen anderen Datenbankserver umgeleitet wird, stimmen der im Verbindungsparameter `ServerName` (Server) und der in der Datenbankserveigenschaft `Name` angegebene Wert nicht miteinander überein. Siehe [Name-Serveigenschaft auf Seite 755](#).

Wenn `NodeType` angegeben ist, stellt die Anwendung normalerweise eine Verbindung mit dem Stammknoten her, und dieser Datenbankserver entscheidet dann darüber, welcher Kopieknoten am wenigsten stark ausgelastet ist. Die Verbindung wird dann an diesen Kopieknoten umgeleitet. Wenn die Anwendung innerhalb eines kurzen Zeitraums mehrere Verbindungen dieser Art erstellt und löscht, wird die Verbindung gepoolt, und der Stammknoten wird nicht gefragt, welcher Kopieserver verwendet werden soll. Die Verwendung von Verbindungspooling verringert die Auslastung des Stammknotens, hat jedoch möglicherweise nicht das erwartete Verhalten zur Folge. Die Anwendung kann angeben, dass ihre Verbindungen nicht gepoolt werden können, und damit sicherstellen, dass der Stammserver bei jeder Verbindung festlegt, mit welchem Kopieknoten diese erfolgen soll.

Wenn Sie diesen Parameter zum Umleiten von Verbindungen verwenden, die Kerberos-Authentifizierung oder integrierte Logins verwenden, müssen alle Datenbankserver in der Scale-Out-Struktur wie folgt konfiguriert werden:

- **Integrierte Logins** Alle Datenbankserver in der Scale-Out-Struktur müssen ein Teil derselben Windows-Benutzergruppe sein oder so konfiguriert werden, dass dieselben Windows-Benutzer auf sie zugreifen können.
- **Kerberos-Authentifizierung** Bei allen Datenbankservern in der Scale-Out-Struktur muss die Kerberos-Authentifizierung aktiviert sein. Der Kerberos-Serverprinzipal für alle Server in der Scale-Out-Struktur muss denselben Realm haben.

### Siehe auch

- [„Datenbankspiegelung“ auf Seite 1467](#)
- [„SQL Anywhere-Scale-Out mit Schreibschutz“ auf Seite 1536](#)
- [„Verbindungsparameter `ServerName` \(Server\)“ auf Seite 383](#)

### Beispiel

- Der Primär- und der Spiegelserver befinden sich in Waterloo, Ontario. Für in Japan ausgeführte Clients soll beispielsweise eine Gruppe von Kopieknoten in Japan eingerichtet werden, um die Verarbeitungszeit für die Herstellung von Verbindungen zu verringern. Wenn ein Zweig der Kopieknoten in Japan dem Stammknoten direkt untergeordnet wäre, könnten weitere untergeordnete Knoten unterhalb des Kopieknotens in Japan hinzugefügt werden. Clients würden sich mit dem Hub verbinden und Folgendes angeben: `NodeType=COPY`. Die lokalen, schreibgeschützten Verbindungen in Japan würden in diesem Fall eine ausgeglichene Lastverteilung zwischen den lokalen Datenbankservern aufweisen, und kein Client würde jemals eine Verbindung zu einem Datenbankserver an einem Ort außerhalb Japans herstellen. Wenn ein Client Änderungen in der Datenbank durchführen müsste, würde sich die entsprechende Verbindungszeichenfolge wie folgt ändern: `NodeType=PRIMARY`.
- Um sich mit der Lesen-Schreiben-Datenbank "joey" zu verbinden, die in einer Cloud-Datenbankkonfiguration ausgeführt wird, wobei "kangaroo1" und "kangaroo2" zwei Hosts sind, auf denen Cloud-Server laufen, können Sie die folgenden Verbindungsparameter verwenden:

```
UID=rick;PWD=secret;DBN=joey;Host=kangaroo1,kangaroo2
```

- Um sich mit der schreibgeschützten Datenbank "joey" zu verbinden, die in einer Cloud-Datenbankkonfiguration ausgeführt wird, wobei "kangaroo1" und "kangaroo2" zwei Hosts sind, auf denen Cloud-Server laufen, können Sie die folgenden Verbindungsparameter verwenden:

`UID=rick;PWD=secret;DBN=joey;Host=kangaroo1,kangaroo2;NodeType=READONLY`

## Verbindungsparameter Password (PWD)

Liefert ein Kennwort für die Verbindung

### Syntax

`{ Password | PWD }=password-string`

### Verwendungszweck

Überall

### Zulässige Werte

- **password-string** Kennwörter haben eine maximale Länge von 255 Byte und beachten die Groß/Kleinschreibung. Kennwörter dürfen keine führenden bzw. nachgestellten Leerzeichen oder Semikola enthalten.

### Standardwert

Kein Kennwort angegeben

### Bemerkungen

Jeder Benutzer einer Datenbank hat ein Kennwort. Das Kennwort muss angegeben werden, damit für den Benutzer eine Verbindung mit der Datenbank zugelassen wird.

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

Der Verbindungsparameter Password (PWD) ist nicht verschlüsselt. Das Kennwort einer Anwendung kann in der Verbindungszeichenfolge enthalten sein. Wenn die Verbindungsparameter Password (PWD) und EncryptedPassword (ENP) beide angegeben werden, ist Password (PWD) vorrangig.

**Vorsicht**

Bei der Erstellung einer Datenquelle ist es nicht empfehlenswert, dass das Kennwort Teil der Definition ist. Auch wenn sowohl das Fenster **ODBC-Konfiguration für SQL Anywhere** im **ODBC-Datenquellen-Administrator** unter Windows als auch das SQL Anywhere-Datenquellen-Dienstprogramm (dbdsn) über diese Funktion verfügen, stellt das Aufnehmen dieser Informationen in die Definition ein Sicherheitsrisiko dar.

Unter Unix werden diese Datenquelleninformationen in der Systeminformationsdatei (standardmäßig `.odbc.ini` genannt) gespeichert. Weitere Hinweise darüber, wie nach dieser Systeminformationsdatei gesucht wird, finden Sie unter [„ODBC-Datenquellen unter Unix“ auf Seite 49](#).

**Siehe auch**

- [„Verbindungsparameter Userid \(UID\)“ auf Seite 387](#)
- [„Kennwörter“ auf Seite 1367](#)
- [„Hinweise zur Sicherheit: Kennwörter“ auf Seite 1410](#)
- [„Verbindungsparameter EncryptedPassword \(ENP\)“ auf Seite 358](#)
- [„GRANT-Anweisung“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [„Groß-/Kleinschreibung“ \[\*SQL Anywhere Server - SQL-Benutzerhandbuch\*\]](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)

**Beispiel**

Die folgende Zeichenfolge für die Verbindung übergibt die Benutzer-ID DBA und das Kennwort sql.

```
UID=DBA;PWD=sql
```

## Verbindungsparameter PrefetchBuffer (PBUF)

Setzt den größtmöglichen Speicherplatz für Pufferzeilen in Byte fest.

**Syntax**

```
{ PrefetchBuffer | PBUF }=buffer-size[ k | m ]
```

**Verwendungszweck**

Überall

**Zulässige Werte**

- **buffer-size** Der Wert ist in Byte, aber Sie können **k** oder **m** verwenden, um Einheiten in kB bzw. MB anzugeben. Dieser Verbindungsparameter akzeptiert Werte zwischen 64 kB und 8 MB.

Wenn ein niedrigerer Wert als 16384 angegeben ist, wird er aus Gründen der Kompatibilität mit früheren Versionen als kB interpretiert.

Die Verwendung von Kilobyte ohne den Suffix K im Verbindungsparameter PrefetchBuffer ist veraltet.

### Standardwert

512 kB (524288), alle Plattformen außer Windows Mobile

64 kB (65536 Byte) Windows Mobile

### Bemerkungen

Der Verbindungsparameter PrefetchBuffer (PBUF) steuert den auf dem Client für Prefetch-Zeilen pro Verbindung maximal reservierten Speicherplatz.

Unter gewissen Umständen kann eine Erhöhung der Anzahl von Prefetch-Zeilen die Abfrageperformance verbessern. Sie können die Anzahl von Prefetch-Zeilen erhöhen, indem Sie die Verbindungsparameter PrefetchRows (PROWS) und PrefetchBuffer (PBUF) verwenden.

Eine Erhöhung des Verbindungsparameters PrefetchBuffer (PBUF) erweitert das Speichervolumen, das für GET DATA-Anforderungen des Puffers verwendet wird. Dies kann für Anwendungen, die viele GET DATA-Anforderungen (SQLGetData) verarbeiten, Performanceverbesserungen bringen.

### Siehe auch

- „[Verbindungsparameter PrefetchRows \(PROWS\)](#)“ auf Seite 381
- „[Verbindungsparameter und Verbindungszeichenfolgen](#)“ auf Seite 31

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge könnte verwendet werden, um festzustellen, ob die Speichergrenze des Verbindungsparameters PrefetchBuffer die Anzahl der Prefetch-Zeilen reduziert.

```
...PrefetchRows=100;LogFile=c:\client.txt
```

Die folgende Zeichenfolge kann verwendet werden, um das Speicherlimit auf 2 MByte zu erhöhen:

```
...PrefetchRows=100;PrefetchBuffer=2M
```

## Verbindungsparameter PrefetchOnOpen

Wenn dieser Parameter aktiviert ist, wird eine Prefetch-Anforderung mit der Anforderung, den Cursor zu öffnen, gesendet.

### Syntax

PrefetchOnOpen={ YES | NO }

### Verwendungszweck

ODBC

### Standardwert

NO

**Bemerkungen**

Die Aktivierung dieser Option sendet eine Prefetch-Anforderung mit der Anforderung, den Cursor zu öffnen, und auf diese Weise eine Netzwerkanforderung, die bei jedem Öffnen eines Cursors Zeilen abrufen, zu eliminieren. Spalten müssen bereits gebunden sein, damit der Prefetch beim geöffneten Cursor stattfindet. Die erneute Bindung von Spalten zwischen der Cursoröffnung und dem ersten Abruf führt bei der Anwendung von PrefetchOnOpen zu reduzierter Performance.

Der Aufruf von ODBC-SQLExecute oder ODBC-SQLExecDirect bei einer Abfrage oder bei einer gespeicherten Prozedur, die eine Ergebnismenge zurückgibt, führt zur Öffnung eines Cursors.

Die Aktivierung dieser Option kann die Performance verbessern, wenn Folgendes gegeben ist:

- Schlechte Latenzzeit im Netzwerk.
- Die Anwendung sendet zahlreiche Anforderungen zum Öffnen und Schließen von Cursors.

## Verbindungsparameter PrefetchRows (PROWS)

Stellt eine erste, vorgeschlagene Anzahl von Prefetch-Zeilen beim Abfragen der Datenbank bereit.

**Syntax**

{ **PrefetchRows** | **PROWS** }=*number-of-rows*

**Verwendungszweck**

Überall

**Zulässige Werte**

- **number-of-rows** Die Anzahl der Prefetch-Zeilen wird einerseits vom Verbindungsparameter PrefetchRows (PROWS) und andererseits vom Verbindungsparameter PrefetchBuffer (PBUF) beschränkt, der den zur Speicherung von Prefetch-Zeilen verfügbaren Speicherplatz begrenzt.

Die Höchstanzahl von Prefetch-Zeilen ist 10000.

**Standardwert**

10

200 für ADO.NET

**Bemerkungen**

Standardmäßig erhöht die Clientbibliothek die Anzahl der Prefetch-Zeilen dynamisch für Cursor, deren Performance sich durch eine solche Erhöhung verbessert. Aufgrund dieses Verhaltens führt die Erhöhung des PrefetchRow-Standardwerts bei den meisten Anwendungen nicht zu einer signifikanteren Verbesserung der Performance.

Ein Erhöhen des PrefetchRow-Standardwerts verbessert möglicherweise die Performance von ODBC-, OLE DB- und SQL Anywhere JDBC-Anwendungen, die die Cursortypen STATIC oder FORWARD ONLY FOR UPDATE verwenden, jedoch meist nur FETCH NEXT-Vorgänge und nur sehr selten

positionsbasierte Aktualisierungen oder Löschungen vornehmen. Dies gilt insbesondere dann, wenn Client und Datenbankserver über ein langsames Netzwerk oder WAN (Weitbereichsnetzwerk) kommunizieren.

Die Anzahl der Prefetch-Zeilen wird vom Verbindungsparameter PrefetchBuffer (PBUF) beschränkt, der den zur Speicherung von Prefetch-Zeilen verfügbaren Speicherplatz begrenzt.

Die Höchstanzahl von Prefetch-Zeilen ist 10000.

### Siehe auch

- „Verbindungsparameter PrefetchBuffer (PBUF)“ auf Seite 379
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge stellt die Anzahl der Prefetch-Zeilen auf 100:

```
...PrefetchRows=100;...
```

## RetryConnectionTimeout-Verbindungsparameter (RetryConnTO)

Weist die Clientbibliothek (DBLIB, ODBC, ADO etc.) an, den Verbindungsversuch in der angegebenen Zeitspanne zu wiederholen, solange der Server nicht gefunden wird.

### Syntax

{ **RetryConnectionTimeout** | **RetryConnTO** }=*timeout-value*

### Verwendungszweck

Überall

### Zulässige Werte

- **timeout-value** Der durch diesen Verbindungsparameter angegebene Wert ist ein Timeout (in Sekunden). Er ist kein Zähler für die Häufigkeit, mit der der Verbindungsversuch wiederholt werden soll. Der Standardwert "0" gibt an, dass der Verbindungsversuch nur einmal durchgeführt werden soll.

### Standardwert

0

### Bemerkungen

Es gibt eine Verzögerung von einer halben Sekunde zwischen den Versuchen, und die Neuversuche werden nur durchgeführt, wenn der Verbindungsversuch fehlgeschlagen ist, weil der Datenbankserver nicht gefunden wurde. Jeder andere Fehler wird umgehend zurückgegeben. Wenn der Datenbankserver nicht gefunden wird, dauert der Verbindungsversuch mindestens so lang wie die im RetryConnectionTimeout-Verbindungsparameter angegebene Zeitspanne.

Der Standardwert für das TCP-Timeout ist 5 Sekunden. Wenn Ihre Verbindungszeichenfolge einen Wert für RetryConnTO enthält, der kleiner ist als 5 (z.B. Host=host-name;RetryConnTO=3), dauert der Verbindungsversuch dennoch 5 Sekunden.

**Siehe auch**

- „Timeout-Protokolloption (TO)“ auf Seite 420

**Beispiel**

Das folgende Verbindungszeichenfolgen-Fragment teilt der Clientbibliothek mit, den Verbindungsversuch für zumindest 5 Sekunden zu wiederholen:

```
...RetryConnTO=5;...
```

## Verbindungsparameter ServerName (Server)

Gibt den Namen eines laufenden Datenbankservers an, mit dem Sie eine Verbindung herstellen wollen.

**Syntax**

{ **ServerName** | **Server** }=*database-server-name-string*

**Verwendungszweck**

Überall

**Zulässige Werte**

- **database-server-name-string** Wenn Sie einen Datenbankserver automatisch starten, können Sie mit diesem Parameter einen Servernamen angeben.

Der Servername wird entsprechend dem Zeichensatz auf dem Clientcomputer interpretiert. Von der Verwendung von Nicht-ASCII-Zeichen in Servernamen wird abgeraten.

Namen müssen gültige Bezeichner sein. Für Datenbankservernamen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola, Schrägstriche (/) oder Backslashes (\) enthalten.
- Sie dürfen nicht länger sein als 250 Byte.
- Sie dürfen keine Leerstellen enthalten, wenn sie unter Unix laufen.

Lange Datenbankservernamen werden je nach Protokoll auf unterschiedliche Längen gekürzt.

Unter Windows und Unix können sich Clients der Version 9.0.2 und früher nicht mit Datenbankservern der Version 10.0.0 und höher verbinden, die längere Namen als die folgenden Längen haben:

- 40 Byte bei Shared Memory unter Windows
- 31 Byte bei Shared Memory unter Unix
- 40 Byte bei TCP/IP

### Standardwert

Der lokale Standard-Datenbankserver

### Bemerkungen

EngineName und ENG werden aus Gründen der Abwärtskompatibilität akzeptiert, werden jedoch nicht mehr empfohlen.

Wenn ein Datenbankserver startet, versucht er, auf diesem Computer zum Standarddatenbankserver zu werden. Der erste Datenbankserver, der startet, wenn kein Standardserver vorhanden ist, wird zum Standarddatenbankserver. Shared Memory-Verbindungen auf diesem Computer, die nicht ausdrücklich einen Datenbankservernamen angeben, erfolgen mit dem Standardserver.

ServerName wird nicht benötigt, wenn Sie sich mit dem lokalen Standard-Datenbankserver verbinden möchten.

Bei Verwendung des Host-Verbindungsparameters ist ServerName nicht erforderlich, wenn sowohl der Hostname als auch der Port angegeben werden oder wenn auf dem Host nur ein Server am Standardport läuft.

Im Fenster **Verbinden** und im Fenster **ODBC-Konfiguration für SQL Anywhere** ist dies das Feld **Servername**.

#### Hinweis

Es wird empfohlen, dass Sie den ServerName-Parameter in Verbindungszeichenfolgen bei bereitgestellten Anwendungen einbeziehen. Damit wird sichergestellt, dass sich die Anwendung mit dem richtigen Server verbindet, wenn auf einem Computer mehrere SQL Anywhere-Datenbankserver laufen, wodurch Verbindungsfehler durch Zeitablauf verhindert werden können.

Es wird empfohlen, die Option -xd für Datenbankserver anzugeben, die von bereitgestellten Anwendungen verwendet werden, und dafür zu sorgen, dass alle Clients mit dem ServerName-Verbindungsparameter explizit den Namen des Datenbankservers angeben, mit dem sie sich verbinden sollen. Damit wird sichergestellt, dass die Anwendung mit dem richtigen Datenbankserver verbunden wird, wenn auf einem Host mehrere SQL Anywhere-Datenbankserver laufen.

**Siehe auch**

- [ServerName-Verbindungsparameter \(Server\)](#) verwenden auf Seite 28
- „Bezeichner“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -n “ auf Seite 266
- „Datenbankserveroption -xd “ auf Seite 307
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Verbindungen mit eingebetteten Datenbanken“ auf Seite 28

**Beispiel**

Eine Verbindung mit einem Server namens "Guelph" herstellen:

```
Server=Guelph
```

## Verbindungsparameter StartLine (START)

Startet einen lokalen Datenbankserver, der von einer Anwendung verwendet wird

**Syntax**

```
{ StartLine | START }=local-database-server-command
```

**Verwendungszweck**

Lokale Datenbankserver

**Zulässige Werte**

- **local-database-server-command** Standardmäßig versucht SQL Anywhere, eine Verbindung zu einem laufenden Datenbankserver herzustellen. Wenn mit den angegebenen Verbindungsparametern kein Server gefunden werden kann, startet SQL Anywhere mit dem *local-database-server-command* automatisch einen neuen lokalen Datenbankserver. Der Datenbankserver wird nicht automatisch gestartet, wenn der Host-Verbindungsparameter angegeben ist oder der CommLinks-Parameter (LINKS) den Wert TCPIP enthält. Siehe „[Syntax des SQL Anywhere-Datenbankservers](#)“ auf Seite 203.

**Standardwert**

dbeng16 auf allen Plattformen außer Windows Mobile.

dbsrv16 unter Windows Mobile.

**Bemerkungen**

Der Verbindungsparameter StartLine wird nur dann zum Starten eines Datenbankservers verwendet, wenn zum angegebenen Datenbankserver keine Verbindung hergestellt werden kann.

Sie können einen Datenbankserver, der eine Datenbank ausführt, z.B. folgendermaßen starten:

```
dbeng16 c:\mydb.db
```

Stellen Sie eine Verbindung mit einer anderen Datenbank her (ohne Angabe eines Datenbankservernamens mit dem ServerName-Verbindungsparameter):

```
dbisql -c "START=dbsrv16 -x none -c 8M;DBN=seconddb;DBF=c:\myseconddb.db;UID=DBA;PWD=sql"
```

In diesem Fall wird der Datenbankserver `dbsrv16` nicht gestartet. Stattdessen wird der Datenbankserver `dbeng16` verwendet, der zum Starten von `mydb.db` verwendet wurde, um `myseconddb.db` zu starten und eine Verbindung dazu herzustellen.

Wenn allerdings `Server=Servername` angegeben wurde und kein Datenbankserver namens `Servername` läuft, wird der Datenbankserver `dbsrv16` gestartet.

### Hinweis

Zum Angeben von Datenbankname, Datenbankdatei oder Servername wird empfohlen, dass Sie die Verbindungsparameter `DatabaseName` (DBN), `DatabaseFile` (DBF) und `ServerName` (Server) verwenden, statt Datenbankserveroptionen im `StartLine`-Verbindungsparameter festzulegen.

Der folgende Befehl verwendet die empfohlene Syntax:

```
START=dbsrv16 -c 8M;Server=myserver;DBF=c:\sample.db;DBN=mydb
```

Die folgende Syntax ist nicht zu empfehlen:

```
START=dbsrv16 -c 8M -n myserver "c:\sample.db"
```

### Siehe auch

- [StartLine-Verbindungsparameter \[START\] verwenden auf Seite 29](#)
- [„Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31](#)
- [„Verbindungsparameter CommLinks \(LINKS\)“ auf Seite 345](#)
- [„Verbindungen mit eingebetteten Datenbanken“ auf Seite 28](#)

### Beispiel

Das folgende Datenquellen-Fragment startet einen Personal Datenbankserver mit einem Cache von 8 MB.

```
"StartLine=dbeng16 -c 8M;DBF=%SQLANYSAMPl6%\demo.db"
```

## Verbindungsparameter Unconditional (UNC)

Ein Datenbankserver wird mit der Funktion `db_stop_engine` und eine Datenbank wird mit der Funktion `db_stop_database` gestoppt, auch wenn Verbindungen zum Datenbankserver bestehen.

### Syntax

```
{ Unconditional | UNC }={ YES | NO }
```

### Verwendungszweck

Nur für die Funktionen `db_stop_engine` und `db_stop_database`.

### Standardwert

NO

**Bemerkungen**

Die Funktionen `db_stop_engine` und `db_stop_database` fahren einen Datenbankserver bzw. eine Datenbank herunter. Wenn Sie "UNC=YES" in der Zeichenfolge für die Verbindung angeben, wird der Datenbankserver bzw. die Datenbank heruntergefahren, auch wenn aktive Verbindungen bestehen. Wenn "Unconditional" nicht auf YES gesetzt ist, wird der Datenbankserver bzw. die Datenbank nur dann heruntergefahren, wenn keine aktiven Verbindungen bestehen.

**Siehe auch**

- „`db_stop_database`-Funktion“ [[SQL Anywhere Server - Programmierung](#)]
- „`db_stop_engine`-Funktion“ [[SQL Anywhere Server - Programmierung](#)]
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31

## Verbindungsparameter Userid (UID)

Gibt die Benutzer-ID an, die zum Anmelden bei der Datenbank verwendet wird

**Syntax**

`{ Userid | UID }=userid`

**Verwendungszweck**

Überall

**Zulässige Werte**

- **userid** Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.

**Standardwert**

Keine

**Bemerkungen**

Beim Herstellen einer Verbindung mit einer Datenbank muss immer eine Benutzer-ID angegeben werden, außer Sie verwenden ein integriertes Login oder ein Kerberos-Login.

**Siehe auch**

- „Verbindungsparameter Password (PWD)“ auf Seite 378
- „Verbindungsparameter und Verbindungszeichenfolgen“ auf Seite 31
- „Benutzersicherheit (Rollen und Privilegien)“ auf Seite 1271

**Beispiel**

Die folgende Zeichenfolge für die Verbindung übergibt die Benutzer-ID DBA und das Kennwort "sql":

```
UID=DBA;PWD=sql
```

# Netzwerkprotokolloptionen

Netzwerkprotokolloptionen (für den Client und den Server) ermöglichen es Ihnen, die Besonderheiten verschiedener Netzwerkprotokoll-Implementierungen zu umgehen.

Serverseitig	Clientseitig
<p>Für den Datenbankserver geben Sie die Netzwerkprotokolloptionen mithilfe der Option <b>-x tcpip</b> an. Zum Beispiel:</p> <pre>dbsrv16 -x tcpip(PARM1=value1;PARM2=value2;...)</pre>	<p>Für Clientanwendungen geben Sie Netzwerkprotokolloptionen mithilfe des CommLinks-Verbindungsparameters (LINKS) an:</p> <pre>CommLinks=tcpip(PARM1=value1;PARM2=value2;...)</pre> <div><p><b>Hinweise</b></p><p>Es wird empfohlen, dass Sie den Host-Verbindungsparameter verwenden statt den CommLinks-Verbindungsparameter (LINKS). Verwenden Sie den Verbindungsparameter CommLinks (LINKS) nur dann, wenn Sie andere TCP/IP-Optionen als Host oder ServerPort (PORT) angeben müssen.</p><p>Sie können nicht sowohl CommLinks als auch Host in einer Verbindungszeichenfolge angeben.</p><p>Wenn Sie den CommLinks-Verbindungsparameter (LINKS) für eine TCP/IP-Verbindung verwenden, geben Sie mithilfe des ServerName-Verbindungsparameters (Server) einen Servernamen an.</p><p>Wenn Sie eine Verbindung mit einem Datenbankserver herstellen, der auf demselben Computer läuft wie der Client, wird Shared Memory empfohlen.</p></div>

Falls ein Parameter Leerstellen enthält, müssen die Netzwerkprotokolloptionen in Anführungszeichen eingeschlossen werden, damit der System-Befehlsinterpretierer sie syntaktisch richtig analysieren kann:

```
dbsrv16 -x "tcpip(PARM1=value1;PARM2=value2;...)"  
"CommLinks=tcpip(PARM1=value1;PARM2=value2;...)"
```

Die Anführungszeichen sind ebenfalls unter Unix erforderlich, falls mehr als ein Parameter angegeben wird, da Unix die Semikola als Befehlstrennzeichen interpretiert.

Boolesche Parameter werden mit YES, Y, ON, TRUE, T oder 1 aktiviert und mit NO, N, OFF, FALSE, F oder 0 deaktiviert. Bei den Parametern wird die Groß-/Kleinschreibung nicht berücksichtigt.

Sie können auch die Protokolloptionen in eine Konfigurationsdatei einbeziehen und die *@data-*Serveroption zum Aufrufen der Konfigurationsdatei verwenden.

TCP/IP	HTTP	HTTPS	TLS
„Broadcast-Protokolloption (BCAST)“	„DatabaseName-Protokolloption (DBN)“	„certificate_company-Protokolloption“	„certificate_company-Protokolloption“
„BroadcastListener-Protokolloption (BLISTENER) (nur serverseitig)“	„KeepaliveTimeout-Protokolloption (KTO)“	„certificate_name-Protokolloption“	„certificate_name-Protokolloption“
„ClientPort-Protokolloption (CPORT) (nur clientseitig)“	„LocalOnly-Protokolloption (LO)“	„certificate_unit-Protokolloption“	„certificate_unit-Protokolloption“
„DoBroadcast-Protokolloption (DOBROADCAST)“	„LogFile-Protokolloption (LOG)“	„DatabaseName-Protokolloption (DBN)“	„FIPS-Protokolloption“
„Host-Protokolloption (IP) (nur clientseitig)“	„LogFormat-Protokolloption (LF)“	„Identity-Protokolloption“	„LocalOnly-Protokolloption (LO)“
„LDAP-Protokolloption“	„LogMaxSize-Protokolloption (LSIZE)“	„identity_password-Protokolloption“	„trusted_certificates-Protokolloption“
„LocalOnly-Protokolloption (LO)“	„LogOptions-Protokolloption (LOPT)“	„FIPS-Protokolloption“	
„MyIP-Protokolloption (ME)“	„MaxConnections-Protokolloption (MAXCONN)“	„LocalOnly-Protokolloption (LO)“	
„ReceiveBufferSize-Protokolloption (RCVBUFSZ)“	„MaxRequestSize-Protokolloption (MAXSIZE)“	„LogFile-Protokolloption (LOG)“	
„SendBufferSize-Protokolloption (SNDBUFSZ)“	„MaxRequestVars-Protokolloption (MAXVARS)“ auf Seite 413	„LogFormat-Protokolloption (LF)“	
„ServerPort-Protokolloption (PORT)“	„MyIP-Protokolloption (ME)“	„LogMaxSize-Protokolloption (LSIZE)“	
„TDS-Protokolloption (nur serverseitig)“	„ServerPort-Protokolloption (PORT)“	„LogOptions-Protokolloption (LOPT)“	
„Timeout-Protokolloption (TO)“	„Timeout-Protokolloption (TO)“	„MaxConnections-Protokolloption (MAXCONN)“	

TCP/IP	HTTP	HTTPS	TLS
„VerifyServerName-Protokolloption (VERIFY) (nur clientseitig)“		„MaxRequestSize-Protokolloption (MAX-SIZE)“	
		„MaxRequestVars-Protokolloption (MAX-VARS)“ auf Seite 413	
		„MyIP-Protokolloption (ME)“	
		„ServerPort-Protokolloption (PORT)“	
		„Timeout-Protokolloption (TO)“	
		„trusted_certificates-Protokolloption“	
		„KeepaliveTimeout-Protokolloption (KTO)“	

**Siehe auch**

- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „Host-Verbindungsparameter“ auf Seite 363
- „Verbindungsparameter ServerName (Server)“ auf Seite 383
- „Hinweise zum Kommunikationsprotokoll“ auf Seite 103

## Broadcast-Protokolloption (BCAST)

Gibt die IP-Broadcast-Adresse an, die verwendet werden soll, um den Server zu finden.

**Syntax**

{ **Broadcast** | **BCAST** }=*ip-address*

**Verfügbare Protokolle**

TCP/IP

**Zulässige Werte**

- **ip-address** Die Zeichenfolge muss in Form einer IP-Adresse angegeben werden.

**Standardwert**

Broadcast-Rufe an alle Adressen in demselben Subnetz

**Bemerkungen**

Die Standard-Broadcast-Adresse wird unter Verwendung der lokalen IP-Adresse und Subnetzmaske erstellt. Die Subnetzmaske gibt an, welcher Abschnitt der IP-Adresse das Netzwerk und welcher Abschnitt den Host festlegt.

Beispiel: Bei einem Subnetz von 10.24.98.x mit einer Maske von 255.255.255.0 würde die Standard-Broadcast-Maske 10.24.98.255 lauten.

Wenn Sie eine IPv6-Adresse auf einer Windows-Plattform angeben, sollte ein Schnittstellenbezeichner verwendet werden. Unix-Plattformen unterstützen sowohl Schnittstellenbezeichner als auch Schnittstellennamen in IPv6-Adressen. Der Schnittstellenbezeichner ist unter Linux (Kernel 2.6.13 und höher) erforderlich.

**Siehe auch**

- „IPv6-Unterstützung in SQL Anywhere“ auf Seite 106
- „BroadcastListener-Protokolloption (BLISTENER) (nur serverseitig)“ auf Seite 391
- „DoBroadcast-Protokolloption (DOBROAD)“ auf Seite 398
- „Fehlerbehandlung: Datenbankserver mithilfe des Broadcast Repeater-Dienstprogramms suchen“ auf Seite 85

**Beispiel**

Das folgende Beispiel einer Verbindungszeichenfolge teilt dem Client mit, nur auf Schnittstelle Nummer 2 einen Broadcast durchzuführen, wenn "IPv6" verwendet wird:

```
LINKS=tcpip(BROADCAST=ff02::1%2)
```

Das folgende Beispiel einer Verbindungszeichenfolge teilt dem Client mit, ein Broadcast auf alle IP-Adressen im Bereich 10.24.98.0 bis 10.24.98.254 unter Verwendung von IPv zu senden:

```
LINKS=tcpip(BROADCAST=10.24.98.255)
```

## BroadcastListener-Protokolloption (BLISTENER) (nur serverseitig)

Steuert beim angegebenen Port das Abhören von Broadcasts

**Syntax**

```
{ BroadcastListener | BLISTENER }={ YES | NO }
```

**Verfügbare Protokolle**

TCP/IP (nur serverseitig)

**Standardwert**

YES

### Bemerkungen

Mithilfe dieser Option können Sie für diesen Port das Warten auf Broadcasts auf OFF setzen.

Die Verwendung von **-sb 0** ist gleichwertig mit der Angabe von `BroadcastListener=NO` unter TCP/IP.

Wenn das Warten auf Broadcasts deaktiviert ist, reagiert der Datenbankserver nicht auf UDP-Broadcasts. Clients müssen entweder mithilfe der HOST-Protokolloption den Hostnamen des Datenbankservers angeben oder den Datenbankserver bei LDAP registrieren und LDAP auf den Clients zum Suchen nach dem Datenbankserver verwenden. Dies bedeutet auch, dass das Dienstprogramm `dblocate` den Datenbankserver nicht in seine Ausgabe einbezieht.

### Siehe auch

- „Datenbankserveroption -sb “ auf Seite 278
- „Broadcast-Protokolloption (BCAST)“ auf Seite 390
- „DoBroadcast-Protokolloption (DOBROAD)“ auf Seite 398
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- „Host-Verbindungsparameter“ auf Seite 363
- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399

### Beispiel

Starten Sie einen Datenbankserver, der TCP/IP-Verbindungen akzeptiert und erfordert, dass TCP/IP-Verbindungen den Host-Verbindungsparameter oder die HOST-Protokolloption verwenden:

```
dbsrv16 -x tcpip(BroadcastListener=NO) ...
```

Das Folgende ist ein Fragment einer Client-Verbindungszeichenfolge zur Verbindung mit dem Datenbankserver:

```
...LINKS=tcpip(...HOST=myhost;...);...
```

## certificate\_company-Protokolloption

Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Feld "Organisation" auf dem Zertifikat zu diesem Wert passt.

### Syntax

**certificate\_company** = *organization*

### Verfügbare Protokolle

TLS, HTTPS

### Standardwert

Keine

## Bemerkungen

SQL Anywhere-Clients vertrauen allen Zertifikaten der entsprechenden Zertifizierungsstelle, daher akzeptieren sie möglicherweise auch Zertifikate, die diese Zertifizierungsstelle für andere Unternehmen ausgestellt hat. Unbeabsichtigt kann Ihr Client in diesem Fall den Datenbankserver eines anderen Unternehmens für Ihren eigenen halten und vertrauliche Daten an diesen übermitteln. Diese Option legt als weitere Überprüfungsebene fest, dass das Unternehmensfeld im Identitätsabschnitt des Zertifikats auch mit einem von Ihnen angegebenen Wert übereinstimmt.

HTTPS wird nur für Webdienst-Clientprozeduren unterstützt. Siehe „[CREATE PROCEDURE-Anweisung \[Webdienste\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „[Getrennt lizenzierbare Komponenten](#)“ [*SQL Anywhere 16 - Einführung*].

## Siehe auch

- „[certificate\\_name-Protokolloption](#)“ auf Seite 393
- „[certificate\\_unit-Protokolloption](#)“ auf Seite 394
- „[trusted\\_certificates-Protokolloption](#)“ auf Seite 421
- „[Verbindungsparameter Encryption \(ENC\)](#)“ auf Seite 359
- „[Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation](#)“ auf Seite 1454
- „[Dienstprogramm zum Erstellen von Zertifikaten \[createcert\]](#)“ auf Seite 894
- „[Datenbankserveroption -xs](#)“ auf Seite 310

## Beispiel

Mit dem folgenden Befehl wird die SQL Anywhere-Beispieldatenbank unter Verwendung der Transportschichtssicherheit mit Interactive SQL verbunden.

```
dbisql -c
"UID=DBA;PWD=sql;HOST=myhost;Server=demo;ENC=TLS(
FIPS=n;TRUSTED_CERTIFICATES=c:\temp\myident;
CERTIFICATE_UNIT='SA';CERTIFICATE_COMPANY='Sybase iAnywhere';
CERTIFICATE_NAME='Sybase' )"
```

## certificate\_name-Protokolloption

Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Namensfeld ("Common Name") auf dem Zertifikat zu diesem Wert passt.

### Syntax

**certificate\_name**=*common-name*

### Verfügbare Protokolle

TLS, HTTPS

### Standardwert

Keine

### Bemerkungen

SQL Anywhere-Clients vertrauen allen Zertifikaten der entsprechenden Zertifizierungsstelle, daher akzeptieren sie möglicherweise auch Zertifikate, die diese Zertifizierungsstelle für andere Unternehmen ausgestellt hat. Unbeabsichtigt kann Ihr Client in diesem Fall den Datenbankserver eines anderen Unternehmens für Ihren eigenen halten und vertrauliche Daten an diesen übermitteln. Diese Option legt als weitere Überprüfungsebene fest, dass das Namensfeld ("Common Name") im Identitätsabschnitt des Zertifikats auch mit einem von Ihnen angegebenen Wert übereinstimmt.

HTTPS wird nur für Webdienst-Clientprozeduren unterstützt. Siehe „[CREATE PROCEDURE-Anweisung \[Webdienste\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

#### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „[Getrennt lizenzierbare Komponenten](#)“ [[SQL Anywhere 16 - Einführung](#)].

### Siehe auch

- „[certificate\\_company-Protokolloption](#)“ auf Seite 392
- „[certificate\\_unit-Protokolloption](#)“ auf Seite 394
- „[trusted\\_certificates-Protokolloption](#)“ auf Seite 421
- „[Verbindungsparameter Encryption \(ENC\)](#)“ auf Seite 359
- „[Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation](#)“ auf Seite 1454
- „[Dienstprogramm zum Erstellen von Zertifikaten \[createcert\]](#)“ auf Seite 894
- „[Datenbankserveroption -xs](#)“ auf Seite 310

### Beispiel

Mit dem folgenden Befehl wird die SQL Anywhere-Beispieldatenbank unter Verwendung der Transportschichtssicherheit mit Interactive SQL verbunden.

```
dbisql -c
"UID=DBA;PWD=sql;Host=myhost;Server=demo;ENC=TLS(
FIPS=n;trusted_certificates=c:\temp\myident;
certificate_unit='SA';certificate_company='Sybase iAnywhere';
certificate_name='Sybase')"
```

## certificate\_unit-Protokolloption

Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Feld der Organisationseinheit ("Organisation Unit") auf dem Zertifikat zu diesem Wert passt.

### Syntax

**certificate\_unit**=*organization-unit*

**Verfügbare Protokolle**

TLS, HTTPS

**Standardwert**

Keine

**Bemerkungen**

SQL Anywhere-Clients vertrauen allen Zertifikaten der entsprechenden Zertifizierungsstelle, daher akzeptieren sie möglicherweise auch Zertifikate, die diese Zertifizierungsstelle für andere Unternehmen ausgestellt hat. Unbeabsichtigt kann Ihr Client in diesem Fall den Datenbankserver eines anderen Unternehmens für Ihren eigenen halten und vertrauliche Daten an diesen übermitteln. Diese Option legt als weitere Überprüfungsebene fest, dass das Feld der Organisationseinheit im Identitätsabschnitt des Zertifikats auch mit einem von Ihnen angegebenen Wert übereinstimmt.

HTTPS wird nur für Webdienst-Clientprozeduren unterstützt. Siehe „[CREATE PROCEDURE-Anweisung \[Webdienste\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

**Hinweis**

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „[Getrennt lizenzierbare Komponenten](#)“ [*SQL Anywhere 16 - Einführung*].

**Siehe auch**

- „[certificate\\_company-Protokolloption](#)“ auf Seite 392
- „[certificate\\_name-Protokolloption](#)“ auf Seite 393
- „[trusted\\_certificates-Protokolloption](#)“ auf Seite 421
- „[Verbindungsparameter Encryption \(ENC\)](#)“ auf Seite 359
- „[Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation](#)“ auf Seite 1454
- „[Dienstprogramm zum Erstellen von Zertifikaten \[createcert\]](#)“ auf Seite 894
- „[Datenbankserveroption -xs](#)“ auf Seite 310

**Beispiel**

Mit dem folgenden Befehl wird die SQL Anywhere-Beispieldatenbank unter Verwendung der Transportschichtssicherheit mit Interactive SQL verbunden.

```
dbisql -c
"UID=DBA;PWD=sql;Host=myhost;Server=demo;ENC=TLS(
FIPS=n;trusted_certificates=c:\temp\myident;
certificate_unit='SA';certificate_company='Sybase iAnywhere';
certificate_name='Sybase')"
```

**ClientPort-Protokolloption (CPORT) (nur clientseitig)**

Legt die Portnummer fest, über die die Clientanwendung mithilfe von TCP/IP kommuniziert

### Syntax

`{ ClientPort | CPORT }=port-number`

### Verfügbare Protokolle

TCP/IP (nur clientseitig)

### Standardwert

Wird dynamisch pro Verbindung von der Netzwerkimplementierung zugeordnet. Wenn Sie keine Firewall-Einschränkungen haben, wird empfohlen, diese Protokolloption nicht zu verwenden.

### Bemerkungen

Diese Option gilt für Verbindungen durch ein Firewall-Schutzsystem, da die Firewall-Software entsprechend dem TCP/UDP-Port filtert. Sie sollten diese Protokolloption nicht verwenden, außer wenn Sie sie für das Firewall-Schutzsystem benötigen.

Die ClientPort-Option bestimmt die Portnummer, mit der die Clientanwendung über TCP/IP kommuniziert. Sie können eine einzelne Portnummer, eine Kombination einzelner Portnummern oder Bereiche von Portnummern angeben. Zum Beispiel:

- (CPORT=1234)
- (CPORT=1234,1235,1239)
- (CPORT=1234-1238)
- (CPORT=1234-1237,1239,1242)

Es empfiehlt sich, eine Liste oder einen Bereich von Portnummern anzugeben, wenn Sie mehrere Verbindungen unter Verwendung einer bestimmten Datenquelle oder Verbindungszeichenfolge herstellen möchten. Wenn Sie eine einzelne Portnummer angeben, wird Ihre Anwendung nicht in der Lage sein, mehr als eine einzige Verbindung aufrechtzuerhalten. Sogar nach dem Schließen der einen Verbindung gibt es eine Timeoutzeit von mehreren Minuten, währenddessen keine neue Verbindung über den angegebenen Port hergestellt werden kann. Wenn Sie eine Liste bzw. einen Bereich von Portnummern verwenden, sucht die Anwendung solange nach Portnummern, bis sie einen Port gefunden hat, mit dem Sie erfolgreich eine Verbindung herstellen kann.

### Siehe auch

- „Host-Protokolloption (IP) (nur clientseitig)“ auf Seite 399
- „DoBroadcast-Protokolloption (DOBROAD)“ auf Seite 398
- „ServerPort-Protokolloption (PORT)“ auf Seite 416
- „Kommunikationsprotokolle“ auf Seite 102
- „Firewall-Verbindungen“ auf Seite 107

### Beispiel

Mit dem folgenden Fragment einer Zeichenfolge wird eine Verbindung von einer Anwendung, die Port 6000 verwendet, zu einem Datenbankserver namens "my-server" hergestellt, der Port 5000 verwendet.

```
CommLinks=tcip(ClientPort=6000;ServerPort=5000);ServerName=my-server
```

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird eine Verbindung von einer Anwendung, die die angegebenen Ports für die Kommunikation verwenden kann, mit einem Datenbankserver namens my-server über den Standard-Serverport hergestellt:

```
CommLinks=tcip(ClientPort=5040,5050-5060,5070);
ServerName=my-server
```

## DatabaseName-Protokolloption (DBN)

Gibt den Namen der Datenbank an, die benutzt werden soll, wenn Webanforderungen verarbeitet werden, bzw. benutzt die Schlüsselwörter REQUIRED oder AUTO, um festzulegen, ob Datenbanknamen als Teil der URL-Adresse erforderlich sind.

### Syntax

```
{ DatabaseName | DBN }={ AUTO | REQUIRED | database-name }
```

### Verfügbare Protokolle

HTTP, HTTPS

### Standardwert

AUTO

### Bemerkungen

Wenn diese Protokolloption auf REQUIRED gesetzt ist, muss die URL einen Datenbanknamen enthalten.

Wenn diese Protokolloption auf AUTO gesetzt ist, kann die URL einen Datenbanknamen enthalten, muss aber nicht. Wenn die URL keinen Datenbanknamen enthält, wird die Standarddatenbank auf dem Server benutzt, um Webanforderungen zu verarbeiten. Da der Datenbankserver ermitteln muss, ob die URL einen Datenbanknamen enthält, wenn die Option auf AUTO gesetzt ist, sollten Sie jede Zweideutigkeit beim Design der Website vermeiden.

Wenn diese Protokolloption auf den Namen einer Datenbank eingestellt ist, wird diese Datenbank benutzt, um alle Webanforderungen zu verarbeiten. die URL darf keinen Datenbanknamen enthalten.

### Beispiel

Der folgende Befehl startet zwei Datenbanken, gestattet aber den Zugriff über HTTP nur für eine Datenbank.

```
dbsrv16 -xs http(DBN=web) "%SQLANY16%\demo.db" web.db
```

Mit dem folgenden Befehl werden zwei HTTP-Webdienste gestartet, einer für *erste\_Datenbank.db* und einer für *zweite\_Datenbank.db*:

```
dbsrv16 -xs http(PORT=80;DBN=your-first-database),http(PORT=8800;DBN=your-second-database) your-first-database.db your-second-database.db
```

## DoBroadcast-Protokolloption (DOBROAD)

Steuert, wie ein Client nach einem Datenbankserver sucht und ob der Datenbankserver einen Broadcast vornimmt, wenn er gestartet wird

### Syntax (Datenbankserver)

{ DoBroadcast | DOBROAD } = { YES | NO }

### Syntax (Client)

{ DoBroadcast | DOBROAD } = { ALL | NONE | DIRECT }

### Verfügbare Protokolle

TCP/IP

### Zulässige Werte (Datenbankserver)

- **YES** Wenn "DoBroadcast=YES" festgelegt wurde, kann der Datenbankserver bei seinem Start einen Broadcast senden, um andere Datenbankserver mit demselben Namen zu suchen.
- **NO** Das Setzen von "DoBroadcast=NO" verhindert, dass der Datenbankserver einen Broadcast sendet, um beim Start andere Datenbankserver mit demselben Namen zu finden. Dies ist unter besonderen, seltenen Umständen sinnvoll, wird aber allgemein nicht empfohlen.

### Zulässige Werte (Client)

- **ALL** Mit "DoBroadcast=ALL" wird ein Broadcast für die Suche nach einem Datenbankserver ausgeführt. Der Broadcast geht zuerst an das lokale Subnetz. Wenn HOST angegeben wird, werden Broadcast-Pakete auch an jeden Host gesendet. Alle Broadcast-Pakete sind UDP-Pakete.
- **NONE** DoBroadcast=NONE bewirkt, dass keine UDP-Broadcasts verwendet werden und der Datenbankserver-Adressencache (*sasrv.ini*) ignoriert wird. Eine TCP/IP-Verbindung wird direkt mit der HOST/PORT-Angabe durchgeführt, und der Datenbankservername wird geprüft. Wenn Sie DoBroadcast=DIRECT angeben, ist die Protokolloption HOST (IP) erforderlich.
- **DIRECT** Mit "DoBroadcast=DIRECT" wird kein Broadcast für die Suche eines Datenbankservers auf dem lokalen Subnetz ausgeführt. Broadcast-Pakete werden nur zu den Hosts geschickt, die in der Protokolloption HOST (IP) angeführt sind. Wenn Sie "DoBroadcast=DIRECT" angeben, ist die Protokolloption HOST (IP) erforderlich.

### Standardwert

YES (Datenbankserver)

ALL (Client) Wenn die Protokolloption HOST (IP) angegeben wird, ist der Standardwert DIRECT.

### Bemerkungen

**Client-Nutzung** Bei TCP/IP können Sie wählen, den Namen des Datenbankservers nicht zu überprüfen, indem Sie die VerifyServerName-Protokolloption (VERIFY) auf NO setzen. Die Protokolloption HOST (IP) muss angegeben werden, es sei denn, dass LDAP verwendet wird. Die Protokolloption ServerPort (PORT) ist hingegen optional.

Bei DIRECT und NONE müssen Sie den Datenbankserverhost mit der HOST-Option angeben.

### Siehe auch

- „Broadcast-Protokolloption (BCAST)“ auf Seite 390
- „BroadcastListener-Protokolloption (BLISTENER) (nur serverseitig)“ auf Seite 391

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge stellt eine Verbindung zu einem Datenbankserver namens gold her, der auf dem Computer "silver" läuft.

```
Host=silver;ServerName=gold
```

Das folgende Fragment einer Verbindungszeichenfolge verwendet die CommLinks-Protokolloption für die Verbindung zu demselben Datenbankserver.

```
CommLinks=tcPIP(DOBROADCAST=DIRECT;HOST=silver);ServerName=gold
```

## Host-Protokolloption (IP) (nur clientseitig)

Legt die Adresse oder Adressen des Datenbankservers fest.

### Syntax

```
{ Host | IP }=ip-address
```

### Verfügbare Protokolle

TCP/IP (nur clientseitig)

### Zulässige Werte

- **IP\_Adresse** Die Zeichenfolge muss in Form einer IP-Adresse angegeben werden, und sie kann wahlweise auch eine Portnummer enthalten (durch einen Doppelpunkt getrennt). Die Liste der Host-Werte ist eine kommagetrennte Liste. Bei IPv6-Adressen, die eine Portnummer enthalten, müssen Sie die Adresse in entweder eckige oder runde Klammern setzen. Sie können **localhost** verwenden, um den aktuellen Computer zu identifizieren. Zum Beispiel:

```
links=tcPIP(HOST=myhost)
links=tcPIP(HOST=myhost:1234)
links=tcPIP(HOST=10.25.13.5,myotherhost)
links=tcPIP(HOST=myhost:1234,10.25.65.112)
links=tcPIP(HOST=myhost:1234,myotherhost:5678)
```

### Standardwert

Durchsuchen des aktuellen TCP/IP-Subnetzes.

### Bemerkungen

"Host" legt die Adresse oder Adressen des Datenbankservers fest. IP und Host sind Synonyme. Sie können eine durch Semikola getrennte Adressenliste verwenden, wenn nach mehr als einem System gesucht werden soll. Sie können auch eine Portnummer durch einen Doppelpunkt getrennt an eine IP-Adresse anfügen. Alternativ können Sie die Host- und Serverports mit der ServerPort-Protokolloption

explizit angeben, z.B. `HOST=myhost;PORT=5000`. Bei IPv6-Adressen, die eine Portnummer enthalten, müssen Sie die Adresse entweder in eckige Klammern oder in Klammern setzen, z.B. `[fe80::5445:5245:444f]:2638`. Wenn ein Port angegeben wird, wird nur diese Portnummer für TCP/IP-Verbindungen und UDP-Broadcasts verwendet. Wenn keine Portnummer angegeben wird, wird der Port 2638 verwendet.

Wenn Sie eine IPv6-Adresse auf einer Windows-Plattform angeben, sollte ein Schnittstellenbezeichner verwendet werden. Unix-Plattformen unterstützen sowohl Schnittstellenbezeichner als auch Schnittstellennamen in IPv6-Adressen. Der Schnittstellenbezeichner ist unter Linux (Kernel 2.6.13 und höher) erforderlich.

Sie müssen den Hostnamen **localhost** verwenden, wenn Sie eine Verbindung mit einem Personal Datenbankserver über TCP/IP herstellen. Das TCP/IP-Kommunikationsprotokoll müssen Sie auf dem Personal Datenbankserver mit der Option `-x` aktivieren.

Verwenden Sie die Option `-z`, wenn der Datenbankserver während des Starts die Adressinformationen im Meldungsfenster des Datenbankservers ausgeben soll.

Geben Sie den LogFile-Verbindungsparameter an, damit die Clientanwendung Adressierungsinformationen in ihre Logdatei schreibt.

Sie können die LocalOnly-Protokolloption nicht zusammen mit der Host-Protokolloption oder dem Host-Verbindungsparameter angeben.

Die Host-Protokolloption unterscheidet sich vom Host-Verbindungsparameter. Die Host-Protokolloption wird zusammen mit dem CommLinks-Verbindungsparameter verwendet. Sie sollten den Verbindungsparameter CommLinks (LINKS) nur dann verwenden, wenn Sie andere TCP/IP-Optionen als Host oder ServerPort (PORT) angeben müssen. Sie können nicht sowohl CommLinks als auch Host in der Verbindungszeichenfolge angeben. Siehe „[Verbindungsparameter CommLinks \(LINKS\)](#)“ auf Seite 345.

Der CommLinks-Verbindungsparameter erfordert die Angabe eines Hostnamens, jedoch sind die Portnummer und der ServerName-Verbindungsparameter optional. Deshalb gibt es vier mögliche Kombinationen:

Host-Verbindungsparameter	Äquivalente Verbindungszeichenfolge mit CommLinks-Verbindungsparameter (LINKS)
<code>Host=serverhost:1234</code>  Es wird versucht, eine Verbindung mit einem Datenbankserver herzustellen, der auf serverhost an Port 1234 läuft.	<code>LINKS=TCPIP(HOST=serverhost:1234;DoBroadcast=None;VerifyServerName=No)</code>

Host-Verbindungsparameter	Äquivalente Verbindungszeichenfolge mit CommLinks-Verbindungsparameter (LINKS)
<code>Host=serverhost:1234; ServerName=myserver</code>  Es wird versucht, eine Verbindung mit einem Datenbankserver namens myserver herzustellen, der auf serverhost an Port 1234 läuft.	<code>LINKS=TCPIP(HOST=serverhost: 1234;DoBroadcast=None;VerifyServerName=Yes); ServerName=myserver</code>
<code>Host=serverhost</code>  Es wird versucht, eine Verbindung mit einem Datenbankserver herzustellen, der auf serverhost am Standardport 2638 läuft.	<code>LINKS=TCPIP(HOST=serverhost: 2638;DoBroadcast=None;VerifyServerName=No)</code>
<code>Host=serverhost; ServerName=myserver</code>  Es wird versucht, eine Verbindung mit einem Datenbankserver namens myserver herzustellen, der auf serverhost an einem beliebigen Port läuft.	<code>LINKS=TCPIP(HOST=serverhost;DoBroadcast=Direct; VerifyServerName=Yes); ServerName=myserver</code>

### Siehe auch

- „Host-Verbindungsparameter“ auf Seite 363
- „IPv6-Unterstützung in SQL Anywhere“ auf Seite 106
- „Datenbankserveroption -z “ auf Seite 312
- „Verbindungsparameter LogFile (LOG)“ auf Seite 371
- „ClientPort-Protokolloption (CPORT) (nur clientseitig)“ auf Seite 395
- „ServerPort-Protokolloption (PORT)“ auf Seite 416

### Beispiel

Das folgende Fragment einer Verbindungszeichenfolge teilt dem Client mit, auf den Systemen "kangaroo" und "197.75.209.222" (Port 2369) nach einem Datenbankserver zu suchen:

```
LINKS=tcPIP(IP=kangaroo,197.75.209.222:2369)
```

Das folgende Fragment einer Verbindungszeichenfolge weist den Client an, auf den Systemen "my-server" und "kangaroo" nach einem Datenbankserver zu suchen.

```
LINKS=tcPIP(HOST=my-server,kangaroo;PORT=2639)
```

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird der Client angewiesen, nach einem Datenbankserver auf Host1 an Port 1234 und nach einem weiteren Datenbankserver auf Host2 an Port 4567 zu suchen. Der Client sucht weder auf Host1 an Port 4567 noch auf Host2 an Port 1234.

```
LINKS=tcPIP(HOST=host1:1234,host2:4567)
```

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird der Client angewiesen, nach einem Datenbankserver an einer IPv6-Adresse zu suchen:

```
LINKS=tcPIP(HOST=fe80::5445:5245:444f)
```

Mit dem folgenden Fragment einer Verbindungszeichenfolge wird der Client angewiesen, nach einem Datenbankserver an einer IPv6-Adresse am Port 2639 zu suchen:

```
LINKS=tcPIP(HOST=[fe80::5445:5245:444f]:2639)
```

Das folgende Beispiel zeigt die Verwendung von IPv6-Adressen mit der Host-Protokolloption:

```
// Global scope address, unique everywhere, so no interface index is required
// no index required
-c "links=tcPIP(host=fd77:55d:59d9:56a:202:55ff:fe76:df19)"
// all communication is done through interface 2
-c "links=tcPIP(host=fd77:55d:59d9:56a:202:55ff:fe76:df19%2)"
// all communication is done through eth0
-c "links=tcPIP(host=fd77:55d:59d9:56a:202:55ff:fe76:df19%eth0)"

// Link scope address, addresses are unique on each interface
// possibly ambiguous (this host may exist through both eth0 and eth1)
-c "links=tcPIP(host=fe80::202:55ff:fe76:df19)"
// not ambiguous because it must use interface 2
-c "links=tcPIP(host=fe80::202:55ff:fe76:df19%2)"
// not ambiguous because it must use eth0
-c "links=tcPIP(host=fe80::202:55ff:fe76:df19%eth0)"
```

## Identity-Protokolloption

Gibt den Namen einer Identitätsdatei an.

### Syntax

**Identity**=*identity-file*

### Verfügbare Protokolle

HTTPS

### Zulässige Werte

- **identity-file** Diese Zeichenfolge gibt den Namen einer Identitätsdatei an.

### Standardwert

Es gibt keinen Identitätsdatei-Standardnamen.

### Bemerkungen

Wenn Sie die Transportschichtsicherheit verwenden, enthält die Identitätsdatei das öffentliche Zertifikat und seinen privaten Schlüssel. Bei nicht selbstsignierten Zertifikaten enthält die Identitätsdatei auch alle signierenden Zertifikate, u.a. auch das Verschlüsselungszertifikat. Das Kennwort für dieses Zertifikat muss mit dem Parameter `Identity_Password` festgelegt werden.

**Siehe auch**

- „Transportschichtsicherheit einrichten“ auf Seite 1446
- „identity\_password-Protokolloption“ auf Seite 403

**Beispiel**

Einen Datenbankserver starten, dessen Webverbindungen ein bestimmtes Verschlüsselungszertifikat erfordern.

```
dbsrv16 -xs https(Identity=cert.file;Identity_Password=secret) ...
```

**Vorsicht**

Die Beispiel-Identitätsdatei ist nur für Test- und Entwicklungszwecke vorgesehen. Es bietet keinerlei Schutz, da es ein Standardelement von SQL Anywhere ist. Ersetzen Sie es durch Ihr eigenes Zertifikat, bevor Sie das Deployment Ihrer Anwendung vornehmen.

## identity\_password-Protokolloption

Gibt das Kennwort für das Verschlüsselungszertifikat an.

**Syntax**

**Identity\_Password**=*password*

**Verfügbare Protokolle**

HTTPS

**Zulässige Werte**

- **password** Diese Zeichenfolge gibt das Kennwort für ein Verschlüsselungszertifikat an.

**Standardwert**

Es gibt kein Identitätsdatei-Standardkennwort.

**Bemerkungen**

Wenn Sie Transportschichtsicherheit verwenden, gibt diese Option das Kennwort an, das dem Kennwort für das Verschlüsselungszertifikat entspricht, das durch die Identity-Protokolloption festgelegt wurde.

**Siehe auch**

- „Transportschichtsicherheit einrichten“ auf Seite 1446
- „Identity-Protokolloption“ auf Seite 402

**Beispiel**

Einen Datenbankserver starten, dessen Webverbindungen ein bestimmtes Verschlüsselungszertifikat erfordern.

```
dbsrv16 -xs https(Identity=cert.file;Identity_Password=secret) ...
```

## FIPS-Protokolloption

Erlaubt die Verwendung von FIPS-zertifizierten Sicherheitsalgorithmen zum Verschlüsseln von Datenbankdateien, Datenbankclient/Datenbankserver-Kommunikation und Webdiensten.

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

### Syntax

{ FIPS }={ YES | NO }

### Verfügbare Protokolle

TLS, HTTPS

### Zulässige Werte

YES, NO

### Standardwert

NO

### Bemerkungen

FIPS-zertifizierte Verschlüsselung wird nur für RSA-Verschlüsselung unterstützt. Clients, für die die FIPS-Protokolloption nicht aktiviert ist, können Verbindungen mit Servern herstellen, für die die Option - FIPS aktiviert ist, und umgekehrt. Diese Option kann zusammen mit der Ende-zu-Ende-Verschlüsselung verwendet werden.

Wenn FIPS auf YES gesetzt ist, verwenden MobiLink-Clients FIPS 140-2-zertifizierte Implementierungen von RSA und AES.

### Siehe auch

- „certificate\_company-Protokolloption“ auf Seite 392
- „certificate\_name-Protokolloption“ auf Seite 393
- „certificate\_unit-Protokolloption“ auf Seite 394
- „trusted\_certificates-Protokolloption“ auf Seite 421
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation“ auf Seite 1454
- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894
- „Datenbankserveroption -ec “ auf Seite 230
- „Datenbankserveroption -xs “ auf Seite 310

**Beispiel**

Mit der folgenden Befehlszeile werden die Netzwerkprotokolloptionen PORT, FIPS, Identity und Identity\_Password für einen Webserver konfiguriert:

```
dbsrv16 -xs https(PORT=544;FIPS=YES;  
Identity=certificate.id;Identity_Password=password) your-database-name.db
```

## KeepaliveTimeout-Protokolloption (KTO)

Gibt die maximal zulässige Leerlaufzeit in Sekunden zwischen HTTP-Anforderungen an.

**Syntax**

```
{ KeepaliveTimeout | KTO }=timeout-value
```

**Verfügbare Protokolle**

HTTP

HTTPS

**Zulässige Werte**

- **timeout-value** Diese Ganzzahl legt die Zeitspanne in Sekunden fest, die zwischen HTTP-Anforderungen abgewartet wird. Wenn die Verbindung kein Zeitlimit haben soll, geben Sie KTO=0 an. In Produktionsumgebungen wird nicht empfohlen, die Einstellung KTO=0 zu verwenden, weil ein böswilliger Client alle Ressourcen des Datenbankservers belegen und andere Clients an der Verbindungsaufnahme hindern könnte.

**Standardwert**

60

**Bemerkungen**

Diese Protokolloption gilt nur für Keep-Alive-HTTP-Anforderungen. Sie legt die maximal zulässige Leerlaufzeit von dem Zeitpunkt an fest, an dem die letzte HTTP-Anforderung empfangen wurde, bis zu dem Zeitpunkt, an dem erste Daten für die nächste HTTP-Anforderung empfangen werden. Nachdem Daten für eine neue Anforderung empfangen wurden, wird die durch die Timeout-Protokolloption definierte Timeoutzeit wirksam.

**Siehe auch**

- „[Timeout-Protokolloption \(TO\)](#)“ auf Seite 420

**Beispiel**

```
dbsrv16 -n demo1 -xs https(port=443;  
identity=C:\Users\Public\Documents\SQL Anywhere 16\Samples\Certificates  
\rsaserver.id;  
identity_password=test;kto=50 demo.db
```

## LDAP-Protokolloption

Ermöglicht es Clients, Datenbankserver ohne Angabe der IP-Adresse zu finden

### Syntax

**LDAP**={ YES | NO | *filename* }

### Verwendungszweck

TCP/IP

### Zulässige Werte

- **YES** Durch Angeben von "LDAP=YES" wird die Unterstützung des LDAP-Namensservers aktiviert und die Datei *saldap.ini* (Standarddateiname) wird als Konfigurationsdatei verwendet.
- **NO** Durch Angeben von NO wird die Unterstützung des LDAP-Namensservers deaktiviert.
- **Dateiname** Durch Angeben von LDAP=*Dateiname* wird die Unterstützung des LDAP-Namensservers aktiviert und die angegebene Datei wird als Konfigurationsdatei verwendet.

### Standardwert

YES

### Bemerkungen

Wenn sich der Datenbankserver selbst bei einem LDAP-Server registriert, können Clients eine Abfrage beim LDAP-Server durchführen. Clients, die über ein WAN oder eine Firewall laufen, können damit Datenbankserver finden, ohne die IP-Adresse anzugeben. Auch das Dienstprogramm zur Positionsermittlung (dblocate) kann dann solche Server finden.

Wenn in der LDAP-Protokolloption kein kompletter Pfad angegeben wird, muss sich die Datei *saldap.ini* in demselben Verzeichnis befinden wie die SQL Anywhere-Programmdateien (z.B. %SQLANY16%\bin32 unter Windows).

Sie können den Inhalt der Datei *saldap.ini* mithilfe des Dienstprogramms zum Verschleiern von Dateien mit einfacher Verschlüsselung verschleiern.

Die Verwendung von LDAP als Namensserver wird nur für die TCP/IP-Serverkommunikation unterstützt.

### Beispiel

Im folgenden Beispiel wird ein Server mit LDAP gestartet:

```
dbsrv16 -n demo16 -x tcpip(ldap=saldap.ini) demo.db
```

Im folgenden Beispiel wird eine Verbindung mit dem LDAP-Server hergestellt:

```
dbisql -c links=tcpip(ldap=y);servername=demo16;uid=dba;pwd=sql
```

**Siehe auch**

- „Verbindungen mit LDAP als Namensserver“ auf Seite 109
- „Konfigurieren der Datei `saldap.ini`“ auf Seite 109
- „Inhalte von `.ini`-Dateien verbergen“ auf Seite 489

## LocalOnly-Protokolloption (LO)

Ermöglicht es, für einen Client festzulegen, dass nur mit einem Datenbankserver auf dem lokalen Computer eine Verbindung hergestellt wird, falls einer vorhanden ist.

**Syntax**

{ **LocalOnly** | **LO** }={ **YES** | **NO** }

**Verfügbare Protokolle**

TCP/IP, HTTP, HTTPS

**Standardwert**

NO

**Bemerkungen**

Wenn kein Datenbankserver mit dem angegebenen Servernamen auf dem lokalen Computer auffindbar ist, wird kein Datenbankserver automatisch gestartet.

Die LocalOnly-Protokolloption (LO) ist nur sinnvoll, wenn "DoBroadcast=ALL" (Standard) ebenfalls angegeben wird.

Wenn Sie "LocalOnly=YES" setzen, wird der reguläre Broadcast-Mechanismus verwendet und Broadcast-Antworten von Datenbankservern auf anderen Computern werden ignoriert.

Sie können die LocalOnly-Protokolloption (LO) mit dem Datenbankserver verwenden, um Verbindungen auf den lokalen Computer zu beschränken. Verbindungsversuche von entfernten Computern werden diesen Server nicht finden und das Locate-Dienstprogramm (dblocate) kann ihn nicht ermitteln. Wenn ein Datenbankserver ausgeführt wird, für den die LocalOnly-Protokolloption (LO) auf YES gesetzt ist, kann der Netzwerkserver als Personal Server ohne Verbindungs- oder CPU-Einschränkungen laufen.

Wenn diese Option auf YES gesetzt ist, weist ein Netzwerk-Datenbankserver alle Verbindungen von Clients zurück, die nicht auf dem lokalen Computer laufen. Diese Option hat keine Auswirkung auf Personal-Datenbankserver, die von anderen Computern ohne Webdienstanforderungen akzeptieren. Der Standardwert ist NO, was bedeutet, dass Verbindungen von Clients ungeachtet ihrer Herkunft akzeptiert werden.

Sie können die LocalOnly-Protokolloption nicht zusammen mit der HOST-Protokolloption oder dem Host-Verbindungsparameter angeben.

### Siehe auch

- „Broadcast-Protokolloption (BCAST)“ auf Seite 390
- „HTTP-Webserver starten“ [*SQL Anywhere Server - Programmierung*]

## LogFile-Protokolloption (LOG)

Legt den Namen der Datei fest, in die der Datenbankserver Informationen über Webanforderungen schreiben soll

### Syntax

{ **LogFile** | **LOG** }=*filename*

### Verfügbare Protokolle

HTTP, HTTPS

### Standardwert

Keine

### Bemerkungen

Diese Protokolloption legt den Namen der Datei fest, in die der Datenbankserver Informationen über Webanforderungen schreiben soll.

### Siehe auch

- „LogFormat-Protokolloption (LF)“ auf Seite 408
- „LogMaxSize-Protokolloption (LSIZE)“ auf Seite 410
- „LogOptions-Protokolloption (LOPT)“ auf Seite 410

## LogFormat-Protokolloption (LF)

Steuert das Format von Meldungen, die in die Logdatei geschrieben werden, in die der Datenbankserver Informationen über Webanforderungen schreibt, und gibt an, welche Felder in den Meldungen angezeigt werden.

### Syntax

{ **LogFormat** | **LF** }=*format-string*

### Verfügbare Protokolle

HTTP, HTTPS

### Zulässige Werte

- **format-string**    Folgende Codes werden unterstützt:
  - **@@**    Das At-Zeichen

- **@B** Datum und Zeit des Beginns der Anforderungsverarbeitung, außer wenn die Anforderung aufgrund eines Fehlers nicht in die Warteschlange gesetzt werden konnte
- **@C** Datum und Zeit der Verbindungsaufnahme durch den Client
- **@D** Name der mit der Anforderung verbundenen Datenbank
- **@E** Text der Fehlermeldung, wenn ein Fehler aufgetreten ist
- **@F** Datum und Zeit der Beendigung der Anforderungsverarbeitung
- **@I** IP-Adresse des Clients
- **@J** Protokollierung des Client-Ports, der mit der @I-Option angegeben ist.
- **@L** Länge der Antwort in Byte, mitsamt Kopfdaten und Hauptdaten
- **@M** HTTP-Anforderungsmethode
- **@P** Listener-Port, der mit der Anforderung verbunden ist
- **@Q** Datum und Zeit, als die Anforderungsverarbeitung in die Warteschlange zur Verarbeitung gesetzt wurde, außer wenn die Anforderung aufgrund eines Fehlers nicht in die Warteschlange gesetzt werden konnte
- **@R** Statuscode und Beschreibung der HTTP-Antwort
- **@S** HTTP-Statuscode
- **@T** Datum und Zeit des vorliegenden Logeintrags
- **@U** Angeforderter URI
- **@V** Angeforderte HTTP-Version
- **@W** Zeitaufwand für die Verarbeitung der Anforderung (@F - @B); oder 0,000, wenn die Anforderung aufgrund eines Fehlers nicht verarbeitet werden konnte

### Standardwert

**@T - @W - @I:@J - @P - "@M @U @V" - @R - @L - @E**

### Bemerkungen

Diese Protokolloption steuert das Format von Meldungen, die in die Logdatei geschrieben werden, die Informationen über Webanforderungen enthält, und welche Felder in den Meldungen angezeigt werden. Wenn sie in der Zeichenfolge erscheinen, werden beim Schreiben der Meldung die Codes durch die aktuellen Werte ersetzt.

Wenn die Webanforderung fehlschlägt, weil die HTTP-Anforderungsmethode nicht unterstützt wird bzw. weil der URI entweder nicht wohlgeformt ist oder darin ein erforderlicher Datenbankname fehlt, gibt die HTTP-Methode (@M) und die HTTP-Version (@V) die Zeichenfolge ??? zurück und der URI (@U) die angegebene Anforderung mit vorangestelltem >>>.

Beispiel: Wenn das Logformat auf "@M @U @V" gesetzt ist, wird bei einer unbekannten HTTP-Methode für die URL `request/sample/test` HTTP/1.0 Folgendes zurückgegeben:

```
"???>>>request/sample/test HTTP/1.0???"
```

### Siehe auch

- „LogFile-Protokolloption (LOG)“ auf Seite 408
- „LogMaxSize-Protokolloption (LSIZE)“ auf Seite 410
- „LogOptions-Protokolloption (LOPT)“ auf Seite 410

## LogMaxSize-Protokolloption (LSIZE)

Steuert die maximale Größe der Logdatei, in die der Datenbankserver Informationen über Webanforderungen schreibt.

### Syntax

```
{ LogMaxSize | LSIZE }=size[ k | m | g ]
```

### Verfügbare Protokolle

HTTP, HTTPS

### Zulässige Werte

- **size** Diese Ganzzahl gibt die maximale Größe der Datei an, in die Webanforderungsinformationen geschrieben werden. Der Standardwert ist in Byte, aber Sie können **k**, **m** oder **g** verwenden, um Einheiten in KByte, MByte bzw. GByte anzugeben. Wenn LogMaxSize auf Null gesetzt ist, gibt es keine Beschränkung für die Loggröße.

### Standardwert

0

### Bemerkungen

Wenn das Log die angegebene Größe erreicht, wird es umbenannt, und eine neue Logdatei wird erstellt.

### Siehe auch

- „LogFile-Protokolloption (LOG)“ auf Seite 408
- „LogFormat-Protokolloption (LF)“ auf Seite 408
- „LogOptions-Protokolloption (LOPT)“ auf Seite 410

## LogOptions-Protokolloption (LOPT)

Gibt die Typen der Meldungen an, die in der Logdatei aufgezeichnet werden, in die der Datenbankserver Informationen über Webanforderungen schreibt.

**Syntax**

```
{ LogOptions | LOPT } = [ NONE ] [, OK ] [, INFO ] [, ERRORS ] [, ALL ] [, status-codes ] [,
REQHDRS ] [, RESHDRS ] [, HEADERS ]
```

**Verfügbare Protokolle**

HTTP, HTTPS

**Zulässige Werte**

Die nachstehenden Schlüsselwörter steuern, welche Kategorien von Nachrichten protokolliert werden:

- **NONE** Keine Protokollierung
- **OK** Anforderungen protokollieren, die vollständig ausgeführt wurden (20x HTTP-Statuscodes)
- **INFO** Anforderungen protokollieren, die nicht modifizierte Statuscodes zurückgeben (3xx HTTP-Statuscodes)
- **ERRORS** Alle Fehler protokollieren (4xx und 5xx HTTP-Statuscodes)
- **USER** Alle Fehler protokollieren (6xx, 7xx, 8xx und 9xx HTTP-Statuscodes)
- **ALL** Alle Anforderungen.

Die folgenden gängigen HTTP-Statuscodes sind ebenfalls verfügbar. Sie können benutzt werden, um Anforderungen zu protokollieren, die bestimmte Statuscodes zurückgeben:

- **C200** OK
- **C400** Fehlerhafte Anforderung
- **C401** Nicht autorisiert
- **C403** Verboten
- **C404** Nicht gefunden
- **C408** Anforderungs-Timeout
- **C501** Nicht implementiert
- **C503** Dienst nicht verfügbar

Folgende Schlüsselwörter können verwendet werden, um mehr Informationen über die protokollierten Meldungen abzurufen:

- **REQHDRS** Beim Protokollieren von Anforderungen werden auch die Kopfdaten der Anforderungen in die Logdatei geschrieben.
- **RESHDRS** Beim Protokollieren von Anforderungen werden auch die Kopfdaten der Antworten in die Logdatei geschrieben.

- **HEADERS** Beim Protokollieren von Anforderungen werden Kopfdaten der Anforderung und der Antwort in die Logdatei geschrieben (wie REQHDRS, RESHDRS).

#### Standardwert

ALL

#### Bemerkungen

Die verfügbaren Werte enthalten Schlüsselwörter, die bestimmte Nachrichtentypen auswählen, und HTTP-Statuscodes. Mehrere Werte können durch Kommas getrennt eingegeben werden.

#### Siehe auch

- „LogFile-Protokolloption (LOG)“ auf Seite 408
- „LogFormat-Protokolloption (LF)“ auf Seite 408
- „LogMaxSize-Protokolloption (LSIZE)“ auf Seite 410

## MaxConnections-Protokolloption (MAXCONN)

Gibt die Anzahl gleichzeitiger Verbindungen an, die vom Datenbankserver akzeptiert werden

#### Syntax

{ **MaxConnections** | **MAXCONN** }=*size*

#### Verfügbare Protokolle

HTTP, HTTPS

#### Zulässige Werte

- **size** Diese Ganzzahl gibt die Anzahl gleichzeitiger Verbindungen an, die vom Datenbankserver akzeptiert werden. Der Wert "0" zeigt an, dass kein Limit gesetzt wird.

#### Standardwert

5 (Personal Server)

Anzahl der lizenzierten Verbindungen (Netzwerkserver)

#### Siehe auch

- „MaxRequestSize-Protokolloption (MAXSIZE)“ auf Seite 412
- „Dienstprogramm für die Serverlizenzierung (dblic)“ auf Seite 964

## MaxRequestSize-Protokolloption (MAXSIZE)

Gibt die Größe der größten Anforderung an, die der Datenbankserver akzeptieren kann

#### Syntax

{ **MaxRequestSize** | **MAXSIZE** }=*size*[ **k** | **m** | **g** ]

**Verfügbare Protokolle**

HTTP, HTTPS

**Zulässige Werte**

- **size** Diese Ganzzahl gibt die Größe der größten Anforderung an, die der Datenbankserver akzeptieren kann. Der Standardwert ist in Byte, aber Sie können **k**, **m** oder **g** verwenden, um Einheiten in KByte, MByte bzw. GByte anzugeben. Der Wert "0" deaktiviert diese Beschränkung, sollte aber nur mit großer Umsicht verwendet werden. Ohne diese Beschränkung kann ein böswilliger Client den Datenbankserver überladen oder dazu bringen, dass sein Speicher erschöpft wird.

**Standardwert**

100 kB

**Bemerkungen**

Wenn die Größe einer Anforderung dieses Limit überschreitet, wird die Verbindung geschlossen und der Client gibt eine Antwort zurück, die darauf hinweist, dass die Anforderung zu groß ist. Dieser Wert begrenzt nur die Größe der Anforderung, nicht die der Antwort.

**Siehe auch**

- „[MaxConnections-Protokolloption \(MAXCONN\)](#)“ auf Seite 412
- „[MaxRequestVars-Protokolloption \(MAXVARS\)](#)“ auf Seite 413

**Beispiel**

Mit dem folgenden Befehl wird der Datenbankserver angewiesen, Anforderungen einer Größe von bis zu 150000 Byte anzunehmen:

```
dbsrv16 -xs http(MaxRequestSize=150000)
```

**MaxRequestVars-Protokolloption (MAXVARS)**

Legt die maximale Anzahl von HTTP-Eingabevariablen fest, die in Anforderungen an den Datenbankserver zulässig sind.

**Syntax**

```
{ MaxRequestVars | MAXVARS }=number
```

**Verfügbare Protokolle**

HTTP, HTTPS

**Zulässige Werte**

- **number** Diese Ganzzahl gibt die maximale Anzahl von Eingabevariablen an, die in einer Anforderung an den Datenbankserver zulässig sind. Der Wert 0 zeigt an, dass es keine Obergrenze gibt. Die Anzahl der zulässigen Eingabevariablen ist jedoch immer noch durch die Anzahl der zulässigen Bytes in der Anforderung beschränkt. Diese wird durch die MaxRequestSize-Protokolloption bestimmt.

### Standardwert

10000

### Bemerkungen

Wenn die Anzahl der Eingabevariablen diese Grenze überschreitet, wird die Verbindung geschlossen und der Client gibt eine Antwort zurück, die darauf hinweist, dass die Anforderung ungültig ist.

Version 12 und frühere Versionen des Datenbankservers hatten keine Einschränkung bezüglich der Anzahl von Variablen in HTTP- oder HTTPS-Eingabeanforderungen. Sie können die MaxRequestVars-Protokolloption auf 0 setzen und dadurch das frühere Verhalten wiederherstellen, aber dies wird nicht empfohlen.

### Siehe auch

- „MaxConnections-Protokolloption (MAXCONN)“ auf Seite 412
- „MaxRequestSize-Protokolloption (MAXSIZE)“ auf Seite 412

### Beispiel

Dieser Befehl startet einen Datenbankserver, der die Anforderungen mit bis zu 100 Eingabevariablen akzeptiert:

```
dbsrv16 -xs http( MaxRequestVars=100 )
```

## MyIP-Protokolloption (ME)

Gibt die Netzwerk-Schnittstellen an, die der Client für die Suche nach dem Datenbankserver verwenden sollte, wenn er auf dem Client verwendet wird. Gibt die Netzwerk-Schnittstellen an, die der Datenbankserver bei der Verwendung auf dem Datenbankserver auf Verbindungen überwachen soll.

### Syntax

```
{ MyIP | ME }={ ip-address [, ip-address ... ] | NONE }
```

### Verfügbare Protokolle

TCP/IP, HTTP, HTTPS

### Zulässige Werte

- **ip-address** Die Zeichenfolge muss in Form einer IP-Adresse angegeben werden. Mehrere IP-Adressen müssen durch Kommas getrennt werden.
- **NONE** Wenn das Schlüsselwort NONE als IP-Nummer angegeben wurde, wird kein Versuch unternommen, die Adressenangaben zu ermitteln. Das NONE-Schlüsselwort ist für Clients auf Computern gedacht, bei denen dieser Vorgang kostenträchtig ist, wie Computer mit mehreren Netzwerkkarten oder Software für einen Fernzugriff (RAS) und einer Netzwerkkarte. Die Anweisung ist nicht für die Verwendung auf dem Server vorgesehen.

### Bemerkungen

Die Protokolloption MyIP (ME) ist für Systeme mit mehr als einem Netzwerkadapter vorgesehen.

Jeder Adapter hat eine IP-Adresse. Standardmäßig verwendet der Datenbankserver jede Netzwerkschnittstelle, die er findet. Wenn Sie nicht wollen, dass Ihr Datenbankserver alle Netzwerkschnittstellen überwacht, geben Sie in der Protokolloption MyIP (ME) die Adresse der einzelnen Schnittstellen an, die Sie verwenden möchten.

Wenn Sie eine IPv6-Adresse auf einer Windows-Plattform angeben, sollte ein Schnittstellenbezeichner verwendet werden. Unix-Plattformen unterstützen sowohl Schnittstellenbezeichner als auch Schnittstellennamen in IPv6-Adressen. Der Schnittstellenbezeichner ist unter Linux (Kernel 2.6.13 und höher) erforderlich.

### Siehe auch

- „IPv6-Unterstützung in SQL Anywhere“ auf Seite 106
- „TCP/IP-Protokoll“ auf Seite 105

### Beispiel

Die folgende Befehlszeile (in einer einzigen Zeile eingegeben) teilt dem Server mit, zwei Netzwerkkarten zu verwenden.

```
dbsrv16 -x tcpip(MyIP=192.75.209.12,192.75.209.32) "%SQLANY16%\demo.db"
```

Die folgende Befehlszeile (in einer einzigen Zeile eingegeben) teilt dem Datenbankserver mit, eine IPv6-Netzwerkkarte zu verwenden:

```
dbsrv16 -x tcpip(MyIP=fe80::5445:5245:444f) "%SQLANY16%\demo.db"
```

Das folgende Fragment einer Verbindungszeichenfolge teilt dem Client mit, keinen Versuch zu machen, Adressenangaben zu ermitteln.

```
LINKS=tcpip(MyIP=NONE)
```

## ReceiveBufferSize-Protokolloption (RCVBUFSZ)

Legt die Größe eines Puffers fest, der vom TCP/IP-Protokoll-Stack verwendet wird

### Syntax

```
{ ReceiveBufferSize | RCVBUFSZ }=size[ k | m | g ]
```

### Verfügbare Protokolle

TCP/IP

### Zulässige Werte

- **size** Der Wert gibt die Größe des vom TCP/IP-Stack verwendeten Empfangspuffers an. Die maximale Größe, die Sie angeben können, ist 1 MB. Dies ist eine erweiterte Option, die Sie nur verwenden sollten, wenn Sie mit ihren Auswirkungen vertraut sind.

### Standardwert

Computerabhängig

### Bemerkungen

Sie sollten diesen Wert erhöhen, wenn die BLOB-Performance des Netzwerks Priorität hat.

### Siehe auch

- [„TCP/IP-Protokoll“ auf Seite 105](#)

## SendBufferSize-Protokolloption (SNDBUFSZ)

Legt die Größe eines Puffers fest, der vom TCP/IP-Protokoll-Stack verwendet wird

### Syntax

{ **SendBufferSize** | **SNDBUFSZ** }=*size* [ **k** | **m** | **g** ]

### Verfügbare Protokolle

TCP/IP

### Zulässige Werte

- **size** Der Wert gibt die Größe des vom TCP/IP-Stack verwendeten Sendepuffers an. Die maximale Größe, die Sie angeben können, ist 1 MB. Dies ist eine erweiterte Option, die Sie nur verwenden sollten, wenn Sie mit ihren Auswirkungen vertraut sind.

### Standardwert

Computerabhängig

### Bemerkungen

Sie sollten diesen Wert erhöhen, wenn die BLOB-Performance des Netzwerks Priorität hat.

### Siehe auch

- [„TCP/IP-Protokoll“ auf Seite 105](#)

## ServerPort-Protokolloption (PORT)

Gibt den Port an, auf dem der Datenbankserver läuft

### Syntax

{ **ServerPort** | **PORT** }=*port-number*

### Verfügbare Protokolle

TCP/IP, HTTP, HTTPS

### Zulässige Werte

- **port-number** Bei einem Datenbankserver weist die ServerPort-Protokolloption die Portnummer zu, um mithilfe von TCP/IP zu kommunizieren.

Sie können eine einzelne Portnummer, eine Kombination einzelner Portnummern oder Bereiche von Portnummern angeben. Wenn Sie eine Liste und/oder einen Bereich von Portnummern angeben, versucht der Datenbankserver, alle angegebenen Portnummern zu binden. Zum Beispiel:

- (port=1234)
- (port=1234,1235,1239)
- (port=1234-1238)
- (port=1234-1237,1239,1242)

Bei einem Client informiert die ServerPort-Protokolloption (PORT) den Client über den Port, an dem Datenbankserver auf TCP/IP-Kommunikation warten. Der Client sucht an jedem in der ServerPort-Protokolloption (PORT) angegebenen Port nach dem Datenbankserver.

#### Standardwert

- **TCP/IP** 2638
- **HTTP** 80
- **HTTPS** 443

#### Anmerkungen zu TCP/IP

Jede Anwendung, die TCP/IP auf einem Computer verwendet, benutzt einen eigenen **TCP/IP-Port**, sodass Netzwerkpakete in der richtigen Anwendung ankommen. Die IANA (Internet Assigned Numbers Authority) hat dem SQL Anywhere-Datenbankserver die Portnummer 2638 für die TCP/IP-Kommunikation zugeordnet. Es ist anderen Anwendungen jedoch nicht verboten, diesen reservierten Port zu verwenden, und dies könnte eine Adressenkollision zwischen dem Datenbankserver und einer anderen Anwendung verursachen.

- **Auf dem Server** Wenn Sie auf dem Server die ServerPort-Protokolloption (PORT) angeben, wird nur die angegebene Portnummer für TCP/IP-Verbindungen verwendet. UDP-Listener verwenden sowohl die angegebene Portnummer als auch die Standard-Portnummer (2638). Wenn Sie die ServerPort-Protokolloption nicht angeben, wird der Standardport 2638 verwendet.
- **Auf dem Client** Wenn Sie die ServerPort-Protokolloption (PORT) angeben, wird nur die angegebene Portnummer für TCP/IP-Verbindungen und UDP-Broadcasts verwendet. Wenn Sie die ServerPort-Protokolloption nicht angeben, wird Port 2638 verwendet.

Wenn der Server auf einem anderen Port als 2638 läuft, kann die Anwendung normalerweise eine Verbindung mit dem Server aufnehmen, indem Sie den Servernamen, aber keine Portnummer übergibt. Die Portnummer muss angegeben werden, wenn der Datenbankserver auf Mac OS X läuft oder die Serveroption -sb verwendet wird.

### **Tipp**

Mac OS X erlaubt es nicht, dass mehrere Prozesse denselben UDP-Port binden. Wenn ein Datenbankserver auf einer dieser Plattformen läuft, wartet er nur am angegebenen UDP-Port bzw. Port 2638, wenn kein Port angegeben ist.

Clients müssen die TCP/IP-Portnummer angeben, wenn der Datenbankserver nicht den Standardport (2638) verwendet.

Wenn der Datenbankserver zum Beispiel mit dem Befehl `dbsrv16 -n MyServer "samples-dir/demo.db"` gestartet wird, kann ein Client in demselben Subnetz den Server mit den Verbindungsparametern `Server=MyServer;LINKS=tcpip` finden. Wenn ein anderer Datenbankserver auf Mac OS X mit dem Befehl `dbsrv16 -n SecondServer -x tcpip(PORT=7777) samples-dir/demo.db` gestartet wird, kann ein Client in demselben Subnetz den Server mit den Verbindungsparametern `Server=SecondServer;LINKS=tcpip(PORT=7777)` finden. Wenn der Datenbankserver auf einer anderen Plattform als Mac OS X läuft, muss der Client den PORT-Parameter nicht angeben.

Zusätzlich gilt: Wenn auf Mac OS X ein SQL Anywhere-Datenbankserver bereits Port 2638 verwendet und ein zweiter Datenbankserver ohne die PORT-Protokolloption gestartet wird, schlägt das Starten des zweiten Datenbankservers fehl. Daher müssen Benutzer die Portnummer des Servers kennen und sie in Ihren Verbindungsparametern angeben. Personal Server starten erfolgreich, sogar wenn Port 2638 in Verwendung ist, weil zum Verbinden mit Personal Servern gewöhnlich ein gemeinsam genutzter Speicher verwendet wird.

### **Anmerkungen zu HTTP**

Wenn Sie den Datenbankserver als Webserver verwenden, hört er die Standardports für HTTP und HTTPS (80 bzw. 443) ab, sofern nicht anders angegeben.

### **Siehe auch**

- „Datenbankserveroption -x “ auf Seite 305
- „Datenbankserveroption -xs “ auf Seite 310
- „Datenbankserveroption -sb “ auf Seite 278

### **Beispiele**

Die folgenden Beispiele zeigen, wie Sie die PORT-Protokolloption verwenden.

1. Starten eines Netzwerk-Datenbankservers:

```
dbsrv16 -x tcpip -n server1
```

Portnummer 2638 wird nun genommen.

2. Versuch, einen anderen Datenbankserver zu starten:

```
dbsrv16 -x tcpip -n server2
```

Der Standardport ist derzeit zugeordnet, und daher startet der Server auf einem anderen Port. Die Portnummer wird im Meldungsfenster des Servers angezeigt. Unter Mac OS X schlägt dies fehl.

3. Starten Sie einen Datenbankserver auf Port 2629:

```
dbsrv16 -x tcpip(ServerPort=2629) -n server3 c:\mydata.db
```

4. Stellen Sie unter der Annahme, dass server3 auf Host serverhost3 gestartet wurde, eine Verbindung mit server3 her und verwenden Sie dabei den Host-Verbindungsparameter aus dbisql:

```
dbisql -c "UID=DBA;PWD=sql;ServerName=server3;Host=serverhost3:2629"
```

5. Stellen Sie unter der Annahme, dass server3 auf Host serverhost3 gestartet wurde, eine Verbindung mit server3 her und verwenden Sie dabei den CommLinks-Verbindungsparameter aus dbisql:

```
dbisql -c
"UID=DBA;PWD=sql;ServerName=server3;CommLinks=tcpip(HOST=serverhost3;PORT
=2629)"
```

In diesem Beispiel verwendet ein anderer Webserver auf Ihrem Computer bereits Port 80 oder Sie haben nicht die Berechtigung, einen Server auf einer so niedrigen Portnummer zu starten. Starten Sie einen Server, der auf einem anderen Port auf Abfragen wartet, z. B. 8080:

```
dbsrv16 -xs http(PORT=8080) -n server3 web.db
```

## TDS-Protokolloption (nur serverseitig)

Steuert, ob TDS-Verbindungen zu einem Datenbankserver zulässig sind.

### Syntax

TDS={ YES | NO }

### Verfügbare Protokolle

TCP/IP (nur serverseitig)

### Standardwert

YES

### Bemerkungen

Um TDS-Verbindungen zu einem Datenbankserver zu verbieten, setzen Sie TDS auf NO. Wenn Sie sicherstellen möchten, dass nur verschlüsselte Verbindungen mit Ihrem Datenbankserver hergestellt werden, bietet diese Protokolloption die einzige Möglichkeit, keine TDS-Verbindungen zuzulassen.

### Siehe auch

- „Datenbankserveroption -ec“ auf Seite 230

### Beispiel

Mit dem folgenden Befehl wird ein Datenbankserver mit dem TCP/IP-Protokoll gestartet, Verbindungen von Sybase Open Client- oder jConnect-Anwendungen sind hingegen gesperrt.

```
dbsrv16 -x tcpip( TDS=NO ) ...
```

## Timeout-Protokolloption (TO)

- Legt die Zeitspanne, wie lange beim Herstellen von Verbindungen auf eine Antwort gewartet werden soll, in Sekunden fest (TCP/IP).
- Legt die Zeitspanne, wie lange beim Herstellen von Verbindungen auf eine Anforderung (HTTP oder HTTPS) gewartet werden soll, in Sekunden fest.

### Syntax

{ **Timeout** | **TO** }=*timeout-value*

### Verfügbare Protokolle

TCP/IP, HTTP, HTTPS

### Zulässige Werte

- **timeout-value**
  - Bei TCP/IP legt diese Ganzzahl die Zeitspanne in Sekunden fest, wie lange beim Herstellen von Verbindungen auf eine Antwort gewartet werden soll. Die maximale Zeitspanne, die Sie angeben können, ist 3600 Sekunden.
  - Bei HTTP oder HTTPS legt diese Ganzzahl die Zeitspanne in Sekunden fest, wie lange auf den Empfang einer vollständigen Anforderung gewartet werden soll.

### Standardwert

- **TCP/IP** 5
- **HTTP** 30
- **HTTPS** 30

### Bemerkungen

Auf dem Client legt diese Protokolloption fest, wie lange auf folgende Vorgänge gewartet wird:

- Die UDP-Broadcast-Antwort bei der Suche nach dem Server.
- TCP/IP-Verbindungsaufruf, um die Verbindung mit dem Datenbankserver herzustellen.
- Antwort vom Datenbankserver, wenn die Verbindung getrennt wird.

Wenn Sie TCP/IP auf dem Server verwenden, gibt diese Protokolloption an, wie lange auf folgende Vorgänge gewartet wird:

- UDP-Broadcast-Antwort bei der Suche nach Spiegel- oder Diagnoseservern, mit denen eine Verbindung hergestellt werden soll.
- TCP/IP-Verbindungsaufruf, wenn Sie Spiegel- oder Diagnoseverbindungen zu anderen Datenbankservern herstellen.

- Antwort bei der Trennung von Spiegel- oder Diagnoseservern.

Wenn Sie HTTP oder HTTPS auf dem Datenbankserver verwenden, legt diese Protokolloption fest:

- Die maximal zulässige Leerlaufzeit beim Empfang einer Anforderung. Die Timeoutzeit beginnt, wenn die Anforderung gestartet wird, und endet, wenn die Anforderung abgeschlossen ist. Wenn diese Grenze erreicht ist, wird die Verbindung geschlossen und eine Meldung über das Anforderungs-Timeout wird an den Client zurückgegeben.

#### Siehe auch

- „[KeepaliveTimeout-Protokolloption \(KTO\)](#)“ auf Seite 405

#### Beispiel

Mit dem folgenden Fragment einer Verbindungszeichenfolge werden die Clientbibliotheken angewiesen, für die Verbindung mit dem Datenbankserver TCP/IP mit einem Timeout von 20 Sekunden zu verwenden.

```
...
CommLinks=tcPIP(TO=20)
...
```

## trusted\_certificates-Protokolloption

Gibt den Pfad und Dateinamen einer Datei an, die ein oder mehrere vertrauenswürdige Zertifikate enthält.

#### Syntax

**trusted\_certificates**=*public-certificate*

#### Verfügbare Protokolle

TLS, HTTPS

#### Standardwert

Keine

#### Bemerkungen

Mit der trusted\_certificates-Protokolloption geben Clients vertrauenswürdige Zertifikate für Datenbankserver an. Das vertrauenswürdige Zertifikat kann ein selbstsigniertes Zertifikat des Servers, ein öffentliches Unternehmensstammzertifikat oder ein Zertifikat einer kommerziellen Zertifizierungsstelle sein. Wenn Sie FIPS-zertifizierte RSA-Verschlüsselung verwenden, müssen Sie Ihre Zertifikate mit RSA generieren. Wenn der Verbindungsparameter Encryption den Wert TLS enthält, ist diese Protokolloption erforderlich.

#### Hinweis

trusted\_certificate wird ebenfalls akzeptiert.

HTTPS wird nur für Webdienst-Clientprozeduren unterstützt. Siehe „[CREATE PROCEDURE-Anweisung \[Webdienste\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

### Siehe auch

- „certificate\_company-Protokolloption“ auf Seite 392
- „certificate\_name-Protokolloption“ auf Seite 393
- „certificate\_unit-Protokolloption“ auf Seite 394
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation“ auf Seite 1454
- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894
- „Datenbankserveroption -xs “ auf Seite 310

### Beispiel

Mit dem folgenden Befehl wird die SQL Anywhere-Beispieldatenbank unter Verwendung der Transportschichtssicherheit mit Interactive SQL verbunden.

```
dbisql -c
"UID=DBA;PWD=sql;Host=myhost;Server=demo;ENC=TLS(
FIPS=n;trusted_certificates=c:\temp\myident;
certificate_unit='SA';certificate_company='Sybase iAnywhere';
certificate_name='Sybase')"
```

## VerifyServerName-Protokolloption (VERIFY) (nur clientseitig)

Steuert, ob Clients den Datenbankservernamen vor dem Verbinden überprüfen müssen

### Syntax

{ VerifyServerName | VERIFY }={ YES | NO }

### Verfügbare Protokolle

TCP/IP (nur clientseitig)

### Standardwert

YES

### Bemerkungen

Wenn der Client den CommLinks-Verbindungsparameter (LINKS) für eine TCP/IP-Verbindung verwendet und die Verbindung erfolgreich herstellt, überprüft er, ob der gefundene Servername mit demjenigen identisch ist, nach dem er gesucht hat. Wenn kein Servername mit dem ServerName-Verbindungsparameter (Server) angegeben wurde oder wenn die Servernamen nicht übereinstimmen,

schlägt die Verbindung fehl. Durch die Angabe von "VerifyServerName=NO" wird die Prüfung des Servernamens übersprungen. Dadurch können SQL Anywhere-Clients mit einem SQL Anywhere-Server eine Verbindung aufnehmen, auch wenn sie nur eine IP-Adressen- oder Portangabe kennen.

**Hinweis**

Es wird empfohlen, dass Sie den Host-Verbindungsparameter verwenden statt den CommLinks-Verbindungsparameter (LINKS). Wenn der Host-Verbindungsparameter verwendet wird und sowohl der Hostname als auch der Port angegeben werden, ist es nicht erforderlich, dass Sie einen Servernamen angeben. Es wird jedoch empfohlen, immer einen Servernamen anzugeben, um zu gewährleisten, dass eine Verbindung mit dem richtigen Server hergestellt wird.

**Siehe auch**

- „Verbindungsparameter CommLinks (LINKS)“ auf Seite 345
- „Host-Verbindungsparameter“ auf Seite 363
- „Verbindungsparameter ServerName (Server)“ auf Seite 383

## SQL Anywhere für Windows Mobile

SQL Anywhere ermöglicht das Deployment von Client- und Serveranwendungen auf das Windows Mobile-Gerät. Dieses Deployment-Modell gestattet der Datenbankanwendung, autonom zu laufen. SQL Anywhere stellt einen Netzwerk-Datenbankserver zur Verfügung, der auf dem Windows Mobile-Gerät läuft. Der Netzwerk-Datenbankserver unterstützt die Kommunikation über TCP/IP. Da Windows Mobile den Netzwerk-Datenbankserver unterstützt, können Sie Administrationstools auf einem Desktopcomputer ausführen, um Aufgaben in der Windows Mobile-Datenbank durchzuführen. Zum Beispiel:

- Sie können die Datenbank auf Ihrem Desktopcomputer mit Sybase Central verwalten.
- Sie können mit Interactive SQL auf Ihrem Desktopcomputer Daten laden und entladen sowie Abfragen ausführen.

**Siehe auch**

- „Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen“ auf Seite 452
- „Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten“ auf Seite 457

## SQL Anywhere-Funktionsunterstützung unter Windows Mobile

In dieser Tabelle werden die Komponenten und Funktionen von SQL Anywhere aufgelistet, die unter Windows Mobile nicht unterstützt werden bzw. dort eine veränderte Funktion haben. Soweit möglich, werden Alternativen zu nicht unterstützten Funktionen angegeben.

Komponente bzw. Funktion	Hinweise
Anwendungsprofilerstellung	Wenn Sie eine Protokollierungssitzung für eine unter Windows Mobile laufende Datenbank erstellen, müssen Sie die Protokollierung mit dem <b>Assistenten für die Datenbankprotokollierung</b> konfigurieren (Sie können den <b>Assistent für die Anwendungsprofilerstellung</b> nicht verwenden). Weiterhin müssen Sie Daten vom Windows Mobile-Gerät in einer Kopie der Windows Mobile-Datenbank protokollieren, die auf einem Datenbankserver auf einem PC läuft. Sie können weder automatisch eine Protokollierungsdatenbank von einem Windows Mobile-Gerät aus erstellen, noch können Sie ein Protokoll für die lokale Datenbank auf einem Windows Mobile-Gerät erstellen. Siehe „Anwendungsprofilerstellung“ [ <a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a> ].
Datenbankspiegelung	Unter Windows Mobile nicht unterstützt.
Externe gespeicherte Prozeduren	Unter Windows Mobile nicht unterstützt.
SQL Anywhere JDBC-Treiber	Unter Windows Mobile nicht unterstützt. Sie können jConnect unter Windows Mobile verwenden.
Externe Umgebungen	Unter Windows Mobile nicht unterstützt.
jConnect	Sie können den jConnect-Treiber aktivieren, wenn Sie eine Datenbank für Windows Mobile erstellen. Das kann nützlich sein, um die Datenbank auf einen Desktopcomputer zu verschieben, der Java unterstützt. Durch das Aktivieren des jConnect-Treibers wird die Datenbank vergrößert. Noch wichtiger ist jedoch, dass etwa 200 KByte mehr Speicher zum Ausführen der Datenbank erforderlich werden. Dieser zusätzliche Speicherbedarf sollte berücksichtigt werden, wenn die Datenbank in einer Umgebung mit begrenztem Speicher, wie z.B. Windows Mobile, ausgeführt wird. Siehe „jConnect unter Windows Mobile“ auf Seite 440.
Kerberos-Authentifizierung	Unter Windows Mobile nicht unterstützt.
LDAP	Unter Windows Mobile nicht unterstützt.

Komponente bzw. Funktion	Hinweise
ODBC-Clients	Windows Mobile stellt keinen ODBC-Treibermanager oder ODBC-Administrator zur Verfügung, daher verwendet SQL Anywhere in Dateien gespeicherte ODBC-Datenquellen. Siehe „ <a href="#">ODBC-Datenquellen unter Windows Mobile</a> “ auf Seite 48.
Sybase Open Client	Unter Windows Mobile nicht unterstützt.
Parallele Sicherungen	Unter Windows Mobile nicht unterstützt.
Personal Datenbankserver (dbeng16)	Nur der Netzwerk-Datenbankserver ( <i>dbsrv16.exe</i> ) wird unter Windows Mobile unterstützt. Dieses Programm unterstützt lokale Verbindungen und Client/Server-Kommunikation über ein Netzwerk.
Ferndatenzugriff (einschließlich Verzeichniszugriffsserver)	Unter Windows Mobile nicht unterstützt.

### Unterstützung von SQL-Anweisungen unter Windows Mobile

In dieser Tabelle werden die SQL-Anweisungen aufgelistet, die unter Windows Mobile nicht unterstützt werden bzw. dort eine veränderte oder eingeschränkte Funktion haben.

SQL-Anweisung	Hinweise
BACKUP-Anweisung	Nur die BACKUP DATABASE DIRECTORY-Syntax wird unter Windows Mobile unterstützt.
CREATE DATABASE-Anweisung	Mit der CREATE DATABASE-Anweisung können Sie eine Datenbank auf einem PC initialisieren und sie später auf ein Windows Mobile-Gerät kopieren. Siehe „ <a href="#">Erstellen von Datenbanken für Windows Mobile</a> “ auf Seite 441.
CREATE EVENT-Anweisung	DiskSpace-Ereignistypen werden unter Windows Mobile nicht unterstützt. Sie können jedoch mit dieser Anweisung den Ereignistyp GlobalAutoIncrement oder ServerIdle definieren.
CREATE EXISTING TABLE-Anweisung	Unter Windows Mobile nicht unterstützt.
CREATE EXTERNLOGIN-Anweisung	Unter Windows Mobile nicht unterstützt.

SQL-Anweisung	Hinweise
CREATE FUNCTION-Anweisung	Sie können jedoch mit der CREATE FUNCTION-Anweisung unter Windows Mobile benutzerdefinierte SQL-Funktionen für die Verwendung in der Datenbank erstellen. Die Klausel EXTERNAL NAME wird unter Windows Mobile nicht unterstützt.
CREATE SERVER-Anweisung	Unter Windows Mobile nicht unterstützt.
CREATE TABLE-Anweisung	Die Klausel AT der CREATE TABLE-Anweisung zum Erstellen von Proxytabellen wird unter Windows Mobile nicht unterstützt.
DROP DATABASE-Anweisung	Unter Windows Mobile nicht unterstützt.
DROP SERVER-Anweisung	Unter Windows Mobile nicht unterstützt.
INSTALL JAVA-Anweisung	Unter Windows Mobile nicht unterstützt.
REMOVE JAVA-Anweisung	Unter Windows Mobile nicht unterstützt.
REORGANIZE TABLE-Anweisung	Unter Windows Mobile nicht unterstützt.
RESTORE DATABASE-Anweisung	Unter Windows Mobile nicht unterstützt.
START JAVA-Anweisung	Unter Windows Mobile nicht unterstützt.
STOP JAVA-Anweisung	Unter Windows Mobile nicht unterstützt.

### Unter Windows Mobile nicht unterstützte Serveroptionen

In dieser Tabelle werden die Datenbankserveroptionen aufgelistet, die unter Windows Mobile nicht unterstützt werden bzw. dort eine veränderte Funktion haben.

Option	Hinweise
@data-Option	Unter Windows Mobile nicht unterstützt.
Serveroption -?	Unter Windows Mobile nicht unterstützt.
-cm-Serveroption	Unter Windows Mobile nicht unterstützt.

Option	Hinweise
-ec-Serveroption	Die starke Kommunikationsverschlüsselung (TLS) ist unter Windows Mobile nicht verfügbar. Nur die Einstellungen <b>none</b> und <b>simple</b> werden unterstützt. Siehe „Datenbankserveroption -ec “ auf Seite 230.
-gb-Serveroption	Unter Windows Mobile nicht unterstützt.
-ge-Serveroption	Unter Windows Mobile nicht unterstützt.
-gna-Serveroption	Unter Windows Mobile nicht unterstützt.
-gnh-Serveroption	Unter Windows Mobile nicht unterstützt.
-gnl-Serveroption	Unter Windows Mobile nicht unterstützt.
-gns-Serveroption	Unter Windows Mobile nicht unterstützt.
-gt-Serveroption	Unter Windows Mobile nicht unterstützt.
-gtc-Serveroption	Unter Windows Mobile nicht unterstützt.
-qi-Serveroption	Der Netzwerk-Datenbankserver wird auf Ihrem Windows Mobile-Gerät, wenn er ausgeführt wird, unten rechts auf dem Bildschirm "Heute" als Symbol dargestellt. Diese Funktion kann nicht deaktiviert werden.
-s-Serveroption	Unter Windows Mobile nicht unterstützt.
-tmf-Serveroption	Unter Windows Mobile nicht unterstützt.
-tmt-Serveroption	Unter Windows Mobile nicht unterstützt.
-u-Serveroption	Unter Windows Mobile nicht unterstützt.
-ua-Serveroption	Unter Windows Mobile nicht unterstützt.
-uc-Serveroption	Unter Windows Mobile nicht unterstützt.
-ud-Serveroption	Unter Windows Mobile nicht unterstützt.
-uf-Serveroption	Unter Windows Mobile nicht unterstützt.
-ui-Serveroption	Unter Windows Mobile nicht unterstützt.
-ut-Serveroption	Unter Windows Mobile nicht unterstützt.
-ux-Serveroption	Unter Windows Mobile nicht unterstützt.
-xp-Serveroption	Unter Windows Mobile nicht unterstützt.

Option	Hinweise
-ze-Serveroption	Unter Windows Mobile nicht unterstützt.

### Unterstützung für Sybase Central-Assistenten unter Windows Mobile

SQL Anywhere umfasst mehrere Tools für die Administration von Datenbanken. Hierzu gehören Sybase Central, Interactive SQL und Dienstprogramme. Keines dieser Administrationstools kann unter Windows Mobile eingesetzt werden. Stattdessen wird die Datenbankadministration von einem Windows-basierten PC ausgeführt, der mit dem Windows Mobile-Gerät verbunden ist.

Die folgende Tabelle listet die Sybase Central-Assistenten auf, die unter Windows Mobile nicht unterstützt bzw. andere Funktionen haben. Außerdem werden, soweit möglich, Alternativen bereitgestellt.

Assistent	Hinweise
<b>Assistent "Datenbank sichern"</b>	Archivsicherungen werden unter Windows Mobile nicht unterstützt. Der <b>Assistent zum Sichern einer Datenbank</b> wird nicht unterstützt. Siehe <a href="#">„Arten der Datensicherung“ auf Seite 1029</a> .  Als Alternative können Sie unter Windows Mobile den <b>Assistenten für die Erstellung von Sicherungskopien</b> verwenden, mit dem Sie die Datenbank und die Transaktionslogdateien getrennt sichern können. Siehe <a href="#">„Archivsicherungen erstellen (Sybase Central)“ auf Seite 1041</a> .
<b>Assistent "Einstellungen der Logdatei ändern"</b>	Unter Windows Mobile nicht unterstützt.
<b>Assistent zum Erstellen einer Datenbank</b>	Dieser Assistent stellt Optionen für die Erstellung von Datenbanken zur Verwendung auf Windows Mobile zur Verfügung, sofern Windows Mobile-Dienste auf dem PC installiert sind, auf dem Sybase Central ausgeführt wird. Siehe <a href="#">„Erstellen von Datenbanken für Windows Mobile“ auf Seite 441</a> .
<b>Assistent "Wartungsplan erstellen"</b>	Die folgenden Funktionen werden unter Windows Mobile nicht unterstützt: <ul style="list-style-type: none"> <li>• Vollständige Archivsicherung</li> <li>• Auf Band sichern</li> <li>• Den Wartungsplanbericht mit E-Mail senden</li> </ul>
<b>Assistent "Datenbank löschen"</b>	Unter Windows Mobile nicht unterstützt.
<b>Assistent "Datenbank migrieren"</b>	Unter Windows Mobile nicht unterstützt.

Assistent	Hinweise
Assistent "Datenbank wiederherstellen"	Unter Windows Mobile nicht unterstützt.
Assistent zum Erstellen eines Dienstes	Unter Windows Mobile nicht unterstützt.
Assistent zum Übersetzen einer Logdatei	Unter Windows Mobile nicht unterstützt.
Assistent "Datenbank entladen"	Dieser Assistent kann dem Windows Mobile-Verzeichnis, in dem die Datenbankdateien gespeichert sind, nicht zugeordnet werden. Sie können jedoch eine Windows Mobile-Datenbank entladen, indem Sie sie auf Ihren PC kopieren und dort den <b>Assistent zum Entladen einer Datenbank</b> verwenden.
Assistent zum Upgrade einer Datenbank	Dieser Assistent wird unter Windows Mobile nicht unterstützt. Sie können jedoch ein Upgrade einer Windows Mobile-Datenbank ausführen, indem Sie sie auf Ihren PC kopieren und dort diesen Assistenten ausführen, bevor Sie die Datenbank wieder auf Ihr Windows Mobile-Gerät zurückkopieren. Siehe „ <a href="#">SQL Anywhere-Server-Upgrades</a> “ [ <a href="#">SQL Anywhere 16 - Änderungen und Upgrades</a> ].

### Unterstützung von SQL Remote unter Windows Mobile

SQL Remote wird unter Windows Mobile mit den folgenden Ausnahmen unterstützt:

Komponente bzw. Funktion	Hinweise
Extraktionsdienstprogramm (dbxtract)	Dieses Dienstprogramm wird unter Windows Mobile nicht unterstützt. Falls notwendig, kann eine Windows Mobile-Datenbank auf einen PC kopiert werden, sodass dann das Extraktionsdienstprogramm verwendet werden kann.

### Siehe auch

- „SQL-Anweisungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen“ auf Seite 452
- „Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten“ auf Seite 457
- Weitere Informationen zu Komponenten, die unter Windows Mobile unterstützt bzw. nicht unterstützt werden, finden Sie unter <http://www.sybase.com/detail?id=1061806>.

## SQL Anywhere-Installation auf einem Windows Mobile-Gerät

### Anforderungen

- Ein Computer, auf dem ein unterstütztes Windows-Betriebssystem ausgeführt wird
  - Für Windows Vista und höher: Windows Mobile-Gerätecenter 6.1 oder höher
  - Unter Windows XP oder früher: Microsoft ActiveSync 3.5 oder später
- Ein von SQL Anywhere unterstütztes Windows Mobile-Gerät

Eine Liste der von SQL Anywhere unterstützten Windows Mobile-Geräte finden Sie unter <http://www.sybase.com/detail?id=1002288>.

### Windows Mobile-Dateispeicherorte

Auf Windows Mobile-Geräten werden Dateien im Installationsverzeichnis `\Programme\SQLAny16` installiert. Die Beispieldatenbank (demo.db) wird unter `\Eigene Dateien` installiert.

#### Vorsicht

Es wird empfohlen, dass Sie SQL Anywhere nicht auf einer Speicherkarte, wie z.B. einer SD-Karte, installieren.

Wenn das Windows Mobile-Gerät nach dem Ruhezustand wieder aktiv wird, werden alle offenen Dateien, einschließlich Programmdateien und DLLs, die sich auf einem Wechseldatenträger befinden, vom Betriebssystem möglicherweise geschlossen. Das Betriebssystem verliert den Zugriff auf die Programmdateien und DLLs, die von Programmen benutzt wurden, die beim Eintritt des Ruhezustands des Geräts ausgeführt wurden. In diesem Fall kann das Betriebssystem den Prozess (etwa den SQL Anywhere-Datenbankserver) aus dem System ohne weitere Meldung entfernen.

## Hinweise zur Installation: ICU unter Windows Mobile verwenden

Der Unicode-Kollationsalgorithmus (UCA) ist ein Algorithmus zum Sortieren des gesamten Unicode-Zeichensatzes. Er bietet linguistisch korrekte Vergleiche, Sortierungen und Groß-/Kleinschreibungskonvertierungen. Der UCA wurde als Teil des Unicode-Standards entwickelt. SQL Anywhere implementiert den UCA unter Verwendung der Open Source-Bibliothek ICU (International Components for Unicode), die von IBM entwickelt und gepflegt wird.

Unter Windows Mobile benötigen Sie ICU, wenn UCA als NCHAR-Kollation oder CHAR-Kollation verwendet wird. Sie benötigen auch ICU unter Windows Mobile auch, wenn Ihr CHAR-Zeichensatz nicht mit dem Zeichensatz Ihres Betriebssystems übereinstimmt.

Standardmäßig wird die ICU-Bibliothek unter Windows Mobile nicht installiert, weil sie den Umfang der SQL Anywhere-Installation unter Windows Mobile um etwa 1,7 MB erhöht. Sie können jedoch Ihre SQL Anywhere-Installation ändern und die ICU-Bibliothek einbeziehen.

Wenn Sie die ICU-Bibliothek nicht installieren, müssen Sie bei der Erstellung der Datenbank entweder eine Kollation, deren Zeichensatz dem Windows Mobile-Zeichensatz entspricht, oder UTF8BIN als

CHAR-Kollation wählen. Sie müssen bei der Erstellung der Datenbank die UTF8BIN-Kollation als NCHAR-Kollation wählen.

**Hinweis**

Wenn Sie auf dem PC eine Datenbank für das Deployment auf einem Windows Mobile-Gerät erstellen, können Sie die UCA-Kollation nur verwenden, wenn die ICU-Bibliothek auf dem Windows Mobile-Gerät installiert ist. Eine Datenbank, die unter Windows Mobile UCA verwendet, ist unbrauchbar, wenn die ICU-Bibliothek nicht auf dem Gerät installiert ist.

**Siehe auch**

- „Unicode-Kollationsalgorithmus (UCA)“ auf Seite 516
- „Zeichensatzkonvertierung“ auf Seite 502

## Hinweise zur Installation: Das .NET Compact Framework unter Windows Mobile verwenden

Auf einigen Geräten, die SQL Anywhere unterstützt, ist nur ADO.NET 1.x-Unterstützung installiert. Um auf einem Gerät ADO.NET Version 2.0 oder 3.5 zu verwenden, laden Sie die Unterstützung für ADO.NET 2.0 oder 3.5 von Microsoft auf Ihr Gerät herunter und installieren Sie sie.

- **Version 2.0** Informationen zur Entwicklung einer Anwendung mit ADO.NET 2.0 finden Sie unter „SQL Anywhere .NET-Datenprovider“ [[SQL Anywhere Server - Programmierung](#)] und [Namespace \[SQL Anywhere Server - Programmierung\]](#).
- **Version 3.5** Informationen zur Entwicklung einer Anwendung mit ADO.NET 3.5 finden Sie unter „SQL Anywhere .NET-Datenprovider“ [[SQL Anywhere Server - Programmierung](#)] und [Namespace \[SQL Anywhere Server - Programmierung\]](#).

**Siehe auch**

- „Praktische Einführungen zum .NET-Datenprovider“ [[SQL Anywhere Server - Programmierung](#)]

## Hinweise zur Installation: Einschränkungen von Windows Mobile 5 und 6 für Smartphones

Auf Smartphones werden sämtliche Funktionen von SQL Anywhere Server Windows Mobile unterstützt, mit den folgenden Einschränkungen für Windows Mobile 5 und Windows Mobile 6:

- **Das Shared Memory-Protokoll wird nicht unterstützt** TCP/IP wird verwendet, auch wenn Sie kein Kommunikationsprotokoll angeben. Sie müssen immer einen Datenbankservernamen bei der Verbindungsherstellung angeben. Wenn Sie dies nicht tun, schlägt die Verbindung fehl.
- **Das Fenster Server-Startoptionen wird nicht unterstützt.** Das Fenster **Server-Startoptionen** erscheint, wenn Sie den Datenbankserver starten und keine Optionen angeben. Wenn Sie beim Versuch, den Datenbankserver zu starten, einen unvollständigen oder nicht-korrekten Befehl eingeben, wird ein Fehler gemeldet und der Datenbankserver wird nicht gestartet.

- **ODBC-Verbindungen fordern möglicherweise nicht zur Eingabe von Verbindungsinformationen auf** Wenn Sie den ODBC-Parameter DriverCompletion für SQLDriverConnect verwenden, werden Sie möglicherweise zur Eingabe von zusätzlichen Verbindungsinformationen aufgefordert. Diese Eingabeaufforderung erscheint nicht. Wenn SQLDriverConnect fehlschlägt, wird keine Eingabeaufforderung angezeigt und ein Fehler gemeldet.
- **Entladen/Neuladen wird nicht unterstützt** Sie müssen die Windows Mobile-Datenbank auf einer anderen Plattform neu aufbauen und dann die Datenbank auf das Windows Mobile-Gerät kopieren. Dies ist die empfohlene Methode für den Neuaufbau einer Windows Mobile-Datenbank.

Siehe:

- „Neuaufbau von Datenbanken unter Windows Mobile“ auf Seite 447
- „Neuaufbau von Datenbanken“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## SQL Anywhere für Windows Mobile installieren

Sie können SQL Anywhere auf Windows Mobile-Geräten installieren.

### Voraussetzungen

Sie benötigen einen Desktopcomputer, auf dem ein unterstütztes Windows-Betriebssystem läuft. Eine Liste der von SQL Anywhere unterstützten Windows Mobile-Geräte finden Sie unter <http://www.sybase.com/detail?id=1002288>.

### Aufgabe

1. Stellen Sie eine Verbindung zwischen Ihrem Windows Mobile-Gerät und dem Desktopcomputer her.
2. Klicken Sie auf dem Computer auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Deployment auf Windows Mobile**.
3. Befolgen Sie die Anweisungen in **SQL Anywhere für Windows Mobile - Deployment-Assistent**.

### Ergebnisse

SQL Anywhere wird auf Ihrem Windows Mobile-Gerät installiert.

### Nächste Schritte

Sie können die Windows Mobile-Beispielanwendung starten.

### Siehe auch

- „Beispieldatenbank starten (Windows Mobile)“ auf Seite 432
- „SQL Anywhere-Installation auf einem Windows Mobile-Gerät“ auf Seite 430

## Beispieldatenbank starten (Windows Mobile)

Verwenden Sie das SQL Anywhere Server-Symbol, um den Datenbankserver zu starten.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Die von den Beispielanwendungen verwendete Beispieldatenbank heißt *demo.db* und befindet sich auf Windows Mobile-Geräten im Verzeichnis *\Eigene Dateien*. Anders als bei der Beispieldatenbank, die mit der Windows-Version von SQL Anywhere zur Verfügung gestellt wird, sind die Bibliotheken mit den internationalen Komponenten für Unicode (ICU) hier nicht erforderlich. In allen anderen Punkten gleicht die Datenbank der Windows-Version.

## Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16**.
2. Tippen Sie auf **Server**.
3. Im Feld **Datenbank** geben Sie *\My Documents\demo.db* ein oder tippen auf **Durchsuchen** und navigieren zu *demo.db* im Verzeichnis *Eigene Dateien*.
4. Das Feld **Servername** kann leer bleiben.

Der Servername wird auf den Standardwert des Datenbanknamens, *demo*, gesetzt.

5. Das Feld **Cache** kann unverändert bleiben.
6. Das Feld **Optionen** kann leer bleiben.
7. Tippen Sie auf **OK**, um die Beispieldatenbank zu starten.
8. Navigieren Sie auf Ihrem Gerät zum Bildschirm **Heute**.
9. Tippen Sie auf das Datenbanksserversymbol unten rechts auf dem Bildschirm.

## Ergebnisse

Wenn im Meldungsfenster des Datenbanksservers die Meldung **Anforderungen werden jetzt akzeptiert** angezeigt wird, wurde die Windows Mobile-Beispielanwendung gestartet.

## Nächste Schritte

Wenn Sie die Beispieldatenbank nicht mehr verwenden möchten, müssen Sie den Datenbankserver herunterfahren. Tippen Sie zum Herunterfahren des Datenbanksservers unten rechts auf dem Bildschirm "Heute" auf das Netzwerk-Datenbanksserversymbol. Im Menü tippen Sie auf **Menü » Herunterfahren**.

## Mit auf Windows Mobile-Geräten laufenden Datenbanken verbinden

Wenn Sie eine auf einem Desktopcomputer laufende Anwendung mit einer auf einem Windows Mobile-Gerät laufenden Datenbank verbinden möchten, können Sie mithilfe der Windows Mobile-Gerätecenter-Verknüpfung (ActiveSync) eine TCP/IP-Verbindung zwischen dem Desktopcomputer und dem Windows Mobile-Gerät herstellen. So können Sie eine Windows Mobile-Datenbank mit den Administrationstools auf dem PC verwalten.

### Siehe auch

- „Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen“ auf Seite 452
- „Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten“ auf Seite 457

## Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden

Sie können einen Datenbankserver starten und eine Verbindung mit einer Datenbank auf Ihrem Windows Mobile-Gerät herstellen.

### Voraussetzungen

Wenn Sie eine Verbindung zwischen Ihrem Desktopcomputer und einem auf einem Windows Mobile-Gerät laufenden Datenbankserver herstellen möchten, müssen Sie beim Starten des Servers die TCP/IP-Option auswählen.

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16**.
2. Tippen Sie auf **Server**.
3. Im Fenster **Datenbank** geben Sie den Namen der Datenbankdatei ein, die Sie starten wollen, und klicken Sie auf **Durchsuchen**, um nach der Datenbank zu suchen.

Standardmäßig befindet sich die Beispieldatenbank in *\Eigene Dateien\demo.db*.

4. Im Feld **Servername** geben Sie den Datenbankservernamen ein, den Sie verwenden wollen.

Der Standardname für den Server der Beispieldatenbank ist **demo**.

5. Im Feld **Optionen** geben Sie **-x tcpip(port=2639)** ein.

Der Datenbankserver verwendet Port 2639. Vermeiden Sie die Verwendung von Port 2638, weil dies auch der standardmäßige TCP/IP-Port für einen SQL Anywhere-Server ist, der auf Ihrem Desktopsystem läuft.

6. Klicken Sie auf **Über TCP/IP**.

Eine TCP/IP-Verbindung ist notwendig, um eine Verbindung zwischen einem PC und einer Datenbank auf Ihrem Windows Mobile-Gerät herzustellen.

7. Tippen Sie auf **OK**.

### Ergebnisse

Die Beispieldatenbank wird auf dem Datenbankserver gestartet.

### Nächste Schritte

Sie können eine ODBC-Datenquelle erstellen, um eine Verbindung zwischen dem Desktopcomputer und Ihrem Windows Mobile-Gerät herzustellen.

### Siehe auch

- „ODBC-Datenquelle für eine Verbindung mit Ihrem Windows Mobile-Gerät erstellen“ auf Seite 435
- „Datenbankserveroption -x “ auf Seite 305

## ODBC-Datenquelle für eine Verbindung mit Ihrem Windows Mobile-Gerät erstellen

Sie können eine ODBC-Datenquelle erstellen, um eine Verbindung mit einer auf Ihrem Windows Mobile-Gerät laufenden Datenbank herzustellen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Klicken Sie auf dem Windows-Desktopcomputer auf **Start » Programme » SQL Anywhere 16 » Administrationstools » ODBC-Datenquellen-Administrator**.
2. Klicken Sie auf der Registerkarte **Benutzer-DSN** auf **Hinzufügen**.
3. Klicken Sie auf **SQL Anywhere 16** und anschließend auf **Fertig stellen**.
4. Auf der Registerkarte **ODBC** geben Sie im Feld **Datenquellenname** **MobileServer** ein.
5. Klicken Sie auf die Registerkarte **Login** und füllen Sie die Felder folgendermaßen aus:
  - **Authentifizierung** Klicken Sie auf **Datenbank**.
  - **Benutzer-ID** Vergewissern Sie sich, dass dieses Feld leer ist. Jedes Mal, wenn Sie eine Verbindung zu einer Datenbank herstellen, müssen Sie eine Benutzer-ID und ein Kennwort eingeben.
  - **Kennwort** Vergewissern Sie sich, dass dieses Feld leer ist. Löschen Sie das Feld **Kennwort verschlüsseln**.

- **Aktion** Klicken Sie auf **Mit einer laufenden Datenbank auf einem anderen Computer verbinden**.
- **Host** Wenn Sie ein Windows Mobile 5.0- oder 6.0-Gerät über eine USB-Verbindung mit Windows Mobile-Gerätecenter (ActiveSync) verbunden haben, versuchen Sie es mit der IP-Adresse für Windows Mobile-Geräte, **169.254.2.1**.

Vor allem bei einigen älteren Windows Mobile-Geräten können Sie mit dieser Adresse auf Schwierigkeiten stoßen. Ist dies der Fall, versuchen Sie es mit der localhost-IP-Adresse (**127.0.0.1**). In diesem Fall müssen Sie auch einen Proxy-Port eingerichtet haben.

- **Port** Geben Sie die Portnummer an, an der das Windows Mobile-Gerät auf Verbindungen wartet.

Verwenden Sie den Port, der im Datenbankserver auf dem Windows Mobile-Gerät für den Start konfiguriert ist. Es wird empfohlen, Port **2639** zu verwenden. Siehe „[Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden](#)“ auf Seite 434.

- **Servename** Geben Sie den Servernamen an, wenn Sie eine Verbindung mit einem bestimmten Datenbankserver herstellen müssen, der auf dem Windows Mobile-Gerät läuft. Andernfalls vergewissern Sie sich, dass dieses Feld leer ist.
- **Datenbankname** Geben Sie den Datenbanknamen an, wenn Sie eine Verbindung mit einer bestimmten Datenbank herstellen müssen, die auf dem Windows Mobile-Gerät läuft. Andernfalls vergewissern Sie sich, dass dieses Feld leer ist.

6. Klicken Sie auf **OK**.

### Ergebnisse

Jetzt können Sie diese Datenquelle verwenden, um eine Verbindung von einem Windows-PC zu einer auf einem Windows Mobile-Gerät laufenden Datenbank herzustellen.

### Nächste Schritte

Sie können die Verbindung mit dem Dienstprogramm "dbping" testen. Wenn eine Datenbank auf dem Windows Mobile-Gerät gestartet wurde, verwenden Sie einen ähnlichen Befehl wie den folgenden, um die Verbindung zu testen.

```
dbping -c "DSN=MobileServer;UID=DBA;PWD=sql"
```

### Siehe auch

- „[ODBC-Datenquellen](#)“ auf Seite 38
- „[Proxy-Ports für Windows Mobile-Geräte hinzufügen](#)“ auf Seite 437
- „[IP-Adresse Ihres Windows Mobile-Geräts ermitteln](#)“ auf Seite 438
- „[Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen](#)“ auf Seite 452
- „[Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten](#)“ auf Seite 457

## Proxy-Ports für Windows Mobile-Geräte hinzufügen

Sie müssen einen Proxy-Port für das Windows Mobile-Gerätecenter (ActiveSync) hinzufügen, um von einem Desktopcomputer aus eine Verbindung mit einem Datenbankserver auf Ihrem Windows Mobile-Gerät herstellen zu können. Anforderungen an die localhost-IP-Adresse (**127.0.0.1**) werden dann an die auf dem Windows Mobile-Gerät laufende Datenbank weitergegeben.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Sie können auch einen Proxy-Port konfigurieren, indem Sie den folgenden Registrierungsschlüssel setzen: **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows CE Services\ProxyPorts**. Weisen Sie DWORD den Wert **SQL Anywhere** zu und geben Sie den Port an, der für den Windows Mobile-Datenverkehr bestimmt ist (2639 ist eine gute Wahl). Bei 64-Bit-Windows-Versionen, die eine 32-Bit-Version von Windows Mobile-Gerätecenter (ActiveSync) ausführen, befindet sich dieser Registrierungseintrag in der 32-Bit-Registrierungsstruktur.

#### Vorsicht

Änderungen an der Registrierung sind gefährlich und können zu Datenverlust führen. Bevor Sie die Registrierung ändern, sollten Sie eine Sicherungskopie Ihres Systems erstellen.

### Aufgabe

1. Öffnen Sie Interactive SQL auf dem PC. Für die 32-Bit-Version von Windows Mobile-Gerätecenter (ActiveSync) müssen Sie die 32-Bit-Version von Interactive SQL starten.
2. Klicken Sie im unteren Teil des Fensters **Verbinden** auf **Extras** und anschließend auf **Windows Mobile Proxy-Port einrichten**.
3. Klicken Sie auf **Neu**.
4. Im Feld **Name** geben Sie **SQL Anywhere** ein.
5. Im Feld **Port** geben Sie **2639** ein.

Dies ist der empfohlene TCP/IP-Port für einen SQL Anywhere-Datenbankserver, der unter Windows Mobile läuft. Sie können andere Ports verwenden, solange Sie sicherstellen, dass der Datenbankserver auf dem Windows Mobile-Gerät auf die Verwendung desselben Ports konfiguriert ist.

#### Hinweis

Jedes Mal, wenn Sie Ihr Windows Mobile-Gerät in die Dockingstation einsetzen, leitet Windows Mobile-Gerätecenter (ActiveSync) den Datenverkehr über Port 2639 an Ihr Gerät. Wenn Sie auf Ihrem PC einen Datenbankserver starten, während sich Ihr Windows Mobile-Gerät in der Dockingstation befindet, kann Port 2639 nicht verwendet werden. Sollte dies ein Problem darstellen, können Sie einen anderen Port für Windows Mobile angeben.

6. Klicken Sie auf **OK**.

Wenn Sie einen Proxy-Port einrichten oder ändern, kann es notwendig sein, sich abzumelden und sich anschließend bei Ihrem Windows-PC anzumelden, damit die neuen Proxy-Porteinstellungen wirksam werden.

### Ergebnisse

Eine neue Proxy-Port-Einstellung wird konfiguriert.

## IP-Adresse Ihres Windows Mobile-Geräts ermitteln

Sie können die IP-Adresse Ihres Windows Mobile-Geräts ermitteln. Dies kann erforderlich sein, wenn Sie eine Verbindung mit einer Datenbank herstellen möchten, die unter Windows Mobile ausgeführt wird.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16**.
2. Tippen Sie auf **Server**.
3. Im Fenster **Datenbank** geben Sie den Namen der Datenbankdatei ein, die Sie starten wollen, und klicken Sie auf **Durchsuchen**, um nach der Datenbank zu suchen.

Standardmäßig befindet sich die Beispieldatenbank in *\Eigene Dateien\demo.db*.

4. Im Feld **Servername** geben Sie den Datenbankservernamen ein, den Sie verwenden wollen.

Der Standardname für den Server der Beispieldatenbank ist **demo**.

5. Im Feld **Optionen** geben Sie **-z -x tcpip(port=2639)** ein.

Wenn der Parameter -z eingestellt ist, zeigt der Datenbankserver beim Start seine IP-Adresse an. Die Adresse kann sich ändern, wenn Sie Ihr Windows Mobile-Gerät vom Netzwerk trennen und es dann wieder verbinden.

Der Datenbankserver verwendet Port 2639. Es empfiehlt sich, die Verwendung von Port 2638 zu vermeiden. Dies ist auch der standardmäßige TCP/IP-Port für einen SQL Anywhere-Server, der auf Ihrem PC läuft. Weitere Hinweise finden Sie unter „[Datenbankserveroption -x](#)“ auf Seite 305.

6. Klicken Sie auf **Über TCP/IP**.

Eine TCP/IP-Verbindung ist notwendig, um eine Verbindung zwischen einem PC und einer Datenbank auf Ihrem Windows Mobile-Gerät herzustellen.

7. Tippen Sie auf **OK**, um die Beispieldatenbank auf dem Netzwerk-Datenbankserver zu starten.
8. Navigieren Sie auf Ihrem Gerät zum Bildschirm **Heute**.
9. Tippen Sie auf das Datenbankserversymbol unten rechts auf dem Bildschirm.

### Ergebnisse

Die IP-Adresse Ihres Windows Mobile-Geräts wird im Meldungsfenster des Datenbankservers angezeigt. In dieser Liste steht die IP-Adresse in der ersten Meldung namens **UDP Listener wird auf IP-Adresse ... gestartet**.

### Siehe auch

- [„ODBC-Datenquelle für eine Verbindung mit Ihrem Windows Mobile-Gerät erstellen“ auf Seite 435](#)
- [„Datenbankserveroption -z “ auf Seite 312](#)

## Konfigurieren von Datenbanken für Windows Mobile

Die meisten SQL-Funktionen, die in der Vollversion von SQL Anywhere enthalten sind, sind ebenfalls in der Windows Mobile-Version verfügbar. Hierzu gehören Transaktionsverarbeitung, Maßnahmen für die referenzielle Integrität, Prozeduren, Trigger usw. Jedoch stehen die Java-Funktionen und die Fern Datenzugriffsfunktionen unter Windows Mobile nicht zur Verfügung.

Berücksichtigen Sie beim Erstellen einer Datenbank, die auf einem Windows Mobile-Gerät laufen soll, dass bestimmte Funktionen nicht unterstützt werden. Eine vollständige Liste der nicht unterstützten Funktionen finden Sie unter [„SQL Anywhere-Funktionsunterstützung unter Windows Mobile“ auf Seite 423](#).

Die folgenden Einstellungen werden während der Erstellung der Datenbank konfiguriert. Nachdem sie festgelegt wurden, können diese Einstellungen nur durch Neuaufbau der Datenbank geändert werden.

- **Berücksichtigung von Groß-/Kleinschreibung oder nicht** Siehe [„Groß-/Kleinschreibung“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).
- **Behandeln von nachgestellten Leerzeichen in Vergleichen** Standardmäßig werden Datenbanken so erstellt, dass nachgestellte Leerzeichen als zusätzliche Zeichen angesehen werden. "Dirk" ist beispielsweise nicht dasselbe wie "Dirk ". Sie können Datenbanken erstellen, bei denen ein Auffüllen mit Zeichen erfolgt, sodass nachgestellte Leerzeichen ignoriert werden. Siehe [Bei Vergleichen nachgestellte Leerzeichen ignorieren \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).
- **Seitengröße** Siehe [„Tipp: Angemessene Seitengröße verwenden“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).
- **Kollationssequenz und Zeichensatz** Wenn Sie Datenbanken für Windows Mobile erstellen, sollten Sie eine Kollation verwenden, die auf demselben Ein- oder Mehrbyte-Zeichensatz basiert, den Windows für die entsprechende Sprache verwenden würde. Wenn Sie zum Beispiel Englisch, Französisch oder Deutsch verwenden, nehmen Sie die Kollation 1252Latin1. Wenn Sie Japanisch verwenden, nehmen Sie die Kollation 932JPN, bei Koreanisch nehmen Sie 949KOR. Siehe [„Kollationen“ auf Seite 514](#).

**Hinweis**

Geben Sie in der Zeichenfolge für Optionen der Anpassung keine Sprachumgebung oder keinen Sortiertyp an, wenn Sie eine Datenbank zur Verwendung unter Windows Mobile erstellen. Falls Sie dies angeben, ist es wahrscheinlich, dass die Datenbank auf dem Windows Mobile-Gerät nicht startet. Weitere Hinweise zu Optionen der Kollationsanpassung finden Sie unter [„Optionen der Kollationsanpassung“ auf Seite 523](#).

Da die Zeichensatzkonvertierung unter Windows Mobile nicht unterstützt wird, müssen Sie entweder den Zeichensatz des Betriebssystems oder UTF-8 bei Windows Mobile-Datenbanken verwenden.

Sie müssen festlegen, ob Sie die ICU-Bibliothek installieren wollen, wenn Sie Ihre Windows Mobile-Datenbank erstellen. Siehe [„Hinweise zur Installation: ICU unter Windows Mobile verwenden“ auf Seite 430](#).

## Transaktionslog unter Windows Mobile

Im Transaktionslog werden alle Änderungen einer Datenbank in der Reihenfolge der Änderungen gespeichert. Wenn eine Datenbankdatei durch einen Datenträgerfehler in Mitleidenschaft gezogen wird, ist das Transaktionslog ausschlaggebend für die Wiederherstellung der Datenbank. Das Transaktionslog wirkt sich außerdem positiv auf die Produktivität Ihrer Arbeit aus. Standardmäßig wird das Transaktionslog im selben Verzeichnis gespeichert wie die Datenbankdatei. Es wird erstellt, sobald die Datenbank zum ersten Mal auf Ihrem Windows Mobile-Gerät gestartet wird.

Wenn Sie eine vorhandene Datenbank auf Ihr Windows Mobile-Gerät kopieren, können Sie sowohl die Datenbank als auch die Transaktionslogdateien kopieren. Falls Sie die Transaktionslogdateien nicht auf das Gerät kopieren, wird ein neues Transaktionslog erstellt, wenn Sie die Datenbank auf Ihrem Windows Mobile-Gerät starten. Das neue Transaktionslog enthält nicht die Informationen, die im ursprünglichen Transaktionslog enthalten waren. Dieser Umstand kann zu Problemen führen, wenn die Datenbank bei ihrer letzten Verwendung nicht ordnungsgemäß heruntergefahren wurde oder wenn sie an Synchronisationen beteiligt ist. Daher sollten Sie am besten sowohl die Datenbank als auch die Transaktionslogdatei auf das Windows Mobile-Gerät kopieren.

**Siehe auch**

- [„Das Transaktionslog“ auf Seite 135](#)

## jConnect unter Windows Mobile

Sybase jConnect ist ein reiner Java JDBC-Treiber und kann mit SQL Anywhere angewendet werden. Sybase Central und Interactive SQL bieten die Möglichkeit, die Unterstützung für jConnect-Metadaten einzuschließen, sodass Sie mit dem jConnect-JDBC-Treiber auf SQL Anywhere-Datenbanken zugreifen können.

Die jConnect-Metadaten-Unterstützung wird vom **Assistenten zum Erstellen einer Datenbank** standardmäßig nicht bei Datenbanken aktiviert, die für Windows Mobile erstellt werden. Sie können die jConnect-Metadaten-Unterstützung jedoch bei Bedarf aktivieren.

Durch das Bereitstellen der jConnect-Metadaten-Unterstützung für eine Datenbank werden zahlreiche Einträge in die Systemtabellen eingefügt. Dadurch wird die Datenbank vergrößert und es werden rund 200 KByte mehr Speicher zum Ausführen der Datenbank benötigt, auch wenn Sie keine jConnect-Funktionen verwenden.

Wenn Sie jConnect nicht verwenden wollen und eine Umgebung mit begrenzter Speicherkapazität, wie Windows Mobile, haben, wird empfohlen, dass Sie Ihrer Datenbank die jConnect-Metadaten-Unterstützung nicht hinzufügen.

**Siehe auch**

- „jConnect-JDBC-Treiber“ [[SQL Anywhere Server - Programmierung](#)]

## Verschlüsselung unter Windows Mobile

Sie können Ihre Datenbank entweder mit einfacher Verschlüsselung oder mit starker Verschlüsselung chiffrieren. Die Verschlüsselungseinstellung kann nach Initialisierung einer Datenbank nur durch Neuaufbau der gesamten Datenbank geändert werden.

**Siehe auch**

- „Datenbankverschlüsselung und -entschlüsselung“ auf Seite 1424
- „Datenbanksicherheit unter Windows Mobile“ auf Seite 1442

## Erstellen von Datenbanken für Windows Mobile

Sie können eine SQL Anywhere-Datenbank für Ihr Windows Mobile-Gerät folgendermaßen erstellen:

- Mit dem Sybase Central-**Assistenten zum Erstellen einer Datenbank**, um eine Datenbank zu erstellen, die Sie dann direkt auf Ihr Windows Mobile-Gerät kopieren
- Mit dem Dienstprogramm dbinit, um eine Datenbank zu erstellen, die Sie dann manuell auf Ihr Windows Mobile-Gerät kopieren
- Mit der Anweisung CREATE DATABASE in Interactive SQL, um eine Datenbank zu erstellen, die Sie dann manuell auf Ihr Windows Mobile-Gerät kopieren

**Hinweis**

Wenn Sie wollen, dass der **Assistent zum Erstellen einer Datenbank** automatisch eine neue Datenbank auf Ihr Windows Mobile-Gerät kopiert, dann muss Sybase Central denselben Bitwert wie ActiveSync oder Windows Mobile-Gerätecenter (32 Bit oder 64 Bit) aufweisen. Unter Windows XP und früher wird nur 32-Bit-Software unterstützt.

Hinweise zu den Entscheidungen, die Sie treffen müssen, um eine Windows Mobile-Datenbank zu erstellen, finden Sie unter:

- [„Transaktionslog unter Windows Mobile“ auf Seite 440](#)
- [„Hinweise zur Installation: ICU unter Windows Mobile verwenden“ auf Seite 430](#)
- [„Hinweise zur Installation: Das .NET Compact Framework unter Windows Mobile verwenden“ auf Seite 431](#)

### Hinweis

Wenn Sie eine Datenbank unter Windows Mobile ausführen, aktiviert der Datenbankserver automatisch Schreibprüfsummen. Dieses Verhalten erleichtert die Früherkennung, falls die Datenbankdatei beschädigt wird. Siehe [„Erkennung von Beschädigungen mithilfe von Prüfsummen“ auf Seite 1084](#).

## Windows Mobile-Datenbanken erstellen (Sybase Central)

Sybase Central erzwingt die Anforderungen für Windows Mobile-Datenbanken beim Erstellen und gibt Ihnen die Möglichkeit, die Datenbankdatei auf Ihr Windows Mobile-Gerät zu kopieren.

### Voraussetzungen

Wenn Sie wollen, dass der **Assistent zum Erstellen einer Datenbank** automatisch eine neue Datenbank auf Ihr Windows Mobile-Gerät kopiert, dann muss Sybase Central denselben Bitwert wie ActiveSync oder Windows Mobile-Gerätecenter (32 Bit oder 64 Bit) aufweisen. Unter Windows XP und früher wird nur 32-Bit-Software unterstützt.

### Aufgabe

1. Stellen Sie eine Verbindung zwischen Ihrem Windows Mobile-Gerät und einem PC her.
2. Starten Sie Sybase Central auf Ihrem Desktopcomputer. Für die 32-Bit-Version von Windows Mobile-Gerätecenter (ActiveSync) müssen Sie die 32-Bit-Version von Sybase Central starten. Sybase Central überträgt die Datenbank über das Windows Mobile-Gerätecenter (ActiveSync) auf das Windows Mobile-Gerät.
3. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Datenbank erstellen**.
4. Klicken Sie auf **Datenbank auf diesem Computer erstellen**. Klicken Sie auf **Weiter**.
5. Geben Sie einen Dateinamen und ein Verzeichnis an, um die Datenbankdatei auf Ihrem PC zu speichern, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Diese Datenbank für Windows Mobile erstellen** und anschließend auf **Weiter**.
7. Klicken Sie auf **Datenbank auf das Windows Mobile-Gerät kopieren** und anschließend auf **Weiter**.
8. Geben Sie das Windows Mobile-Verzeichnis an, in das Ihre Datenbankdateien kopiert werden sollen. Der Standardstandort ist das Hauptverzeichnis des Geräts.

**Tipp**

Kopieren Sie die Datenbank auf Ihr Windows Mobile-Gerät in das Verzeichnis *Eigene Dateien*, sodass Sie die Datenbank einfacher starten können.

Wenn Sie auf Ihrem Windows Mobile-Gerät eine Datenbank mit dem Fenster **Startoptionen für den Server** starten, können Sie mit **Durchsuchen** nur im Verzeichnis *Eigene Dateien* nach der Datenbank suchen.

Falls die Datenbank nicht im Verzeichnis *Eigene Dateien* gespeichert ist, müssen Sie den Pfad der Datenbank im Fenster **Startoptionen für den Server** im Feld **Datenbank** eingeben.

Sie können aber auch die Option **Datenbank nach dem Kopieren vom Desktop-Computer löschen** wählen.

Wenn Sie die Kopie auf dem PC nicht löschen, wird eine Kopie der Datenbankdatei auf Ihrem PC in dem Verzeichnis gespeichert, das Sie in Schritt 5 angegeben haben. Klicken Sie auf **Weiter**.

9. Geben Sie das Verzeichnis an, in dem die Transaktionslogdatei gespeichert werden soll. Klicken Sie auf **Weiter**.

Auf Ihrem Windows Mobile-Gerät wird die Transaktionslogdatei in demselben Verzeichnis erstellt wie auch die Datenbankdatei, wenn die Datenbank zum ersten Mal auf dem Netzwerkservers gestartet wird.

10. Geben Sie an, ob ein Transaktionslog-Spiegel verwendet werden soll. Klicken Sie auf **Weiter**.

11. Deaktivieren Sie die Option **jConnect Metadaten-Unterstützung installieren** und klicken Sie auf **Weiter**.

12. Legen Sie die Verschlüsselungsstufe für Ihre Datenbank fest, indem Sie die entsprechende Option auswählen, und klicken Sie auf **Weiter**.

Wenn Sie eine starke Verschlüsselung wählen, müssen Sie einen Chiffreschlüssel angeben. Es wird empfohlen, dass Sie einen Wert für Ihren Schlüssel wählen, der mindestens 16 Zeichen umfasst und eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält.

**Vorsicht**

Speichern Sie eine Kopie Ihres Schlüssels an einem sicheren Ort. Sie müssen den Schlüssel jedes Mal angeben, wenn Sie die Datenbank starten oder ändern möchten. Der Verlust eines Schlüssels führt dazu, dass die betreffende Datenbank nicht mehr verfügbar ist und sich nicht wiederherstellen lässt.

13. Wählen Sie eine Seitengröße aus und klicken Sie auf **Weiter**.
14. Klicken Sie auf der Seite **Zusätzliche Einstellungen angeben** auf **Prüfsummen in jede Datenbankseite einbeziehen** und anschließend auf **Weiter**.
15. Befolgen Sie die restlichen Anleitungen des Assistenten und klicken Sie dann auf **Fertig stellen**, um die Datenbank zu erstellen und auf Ihr Gerät zu kopieren.

**Hinweis**

Geben Sie eine Kollationssequenz für NCHAR-Daten an. Wenn keine NCHAR UCA-Sortierung erforderlich ist, sollte die NCHAR-Kollationssequenz UTF8BIN sein. Dadurch benötigt der Datenbankserver nicht die ICU-Bibliotheken (*dbicu16.dll* und *dbicudt16.dat*). Klicken Sie auf **Folgende mitgelieferte Kollation verwenden** und wählen Sie dann **UTF8BIN** aus.

16. Es wird ein Fenster geöffnet, in dem der Fortschritt beim Kopieren der Dateien auf Ihr Windows Mobile-Gerät angezeigt wird. Klicken Sie auf **Schließen**.
17. Nachdem der Assistent die Datenbank auf Ihr Windows Mobile-Gerät kopiert hat, überprüfen Sie den Speicherort der Dateien:

Tippen Sie auf **Start » Programme » Datei-Explorer** und navigieren Sie zu dem Windows Mobile-Verzeichnis, in das Sie die Datenbank kopiert haben.

**Ergebnisse**

Die Datenbankdatei ist dort aufgelistet. Die Transaktionslogdatei wird erst in der Liste aufgeführt, nachdem Sie die Datenbank zum ersten Mal auf Ihrem Windows Mobile-Gerät gestartet haben.

**Nächste Schritte**

Sie können die Windows Mobile-Datenbank auf dem Gerät starten.

**Siehe auch**

- „Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden“ auf Seite 434
- „Erstellen von Datenbanken für Windows Mobile“ auf Seite 441

**Windows Mobile-Datenbanken erstellen (Dienstprogramm dbinit)**

Verwenden Sie das Dienstprogramm dbinit auf Ihrem Desktopcomputer, um eine Datenbank zu erstellen, die unter Windows Mobile verwendet werden kann.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Aufgabe**

1. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in dem Sie die Datenbank erstellen wollen. Zum Beispiel:

```
cd temp
```

2. Erstellen Sie eine Datenbank mit der DBA-Benutzer-ID "DBA" und dem Kennwort "sql", indem Sie folgenden Befehl ausführen (wobei *Datenbankname* der Name der neuen Datenbank ist):

```
dbinit -s -dba DBA,sql database-name.db
```

Die Option -s aktiviert Prüfsummen für die Datenbank.

3. Kopieren Sie die Datenbank auf Ihr Windows Mobile-Gerät.

## Ergebnisse

Eine Datenbank wird erstellt und auf Ihr Windows Mobile-Gerät kopiert.

## Nächste Schritte

Sie können die Datenbank starten.

## Siehe auch

- „Eine Datenbank auf Ihr Windows Mobile-Gerät kopieren“ auf Seite 446
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden“ auf Seite 434
- „Erstellen von Datenbanken für Windows Mobile“ auf Seite 441

## Windows Mobile-Datenbanken erstellen (SQL)

Erstellen Sie eine Datenbank auf Ihrem Desktopcomputer und kopieren Sie die Datei dann auf Ihr Windows Mobile-Gerät.

## Voraussetzungen

Ob Sie die CREATE DATABASE-Anweisung ausführen können, hängt von der Einstellung der Option -gu ab und davon, ob Sie das SERVER OPERATOR-Systemprivileg haben.

## Aufgabe

1. Stellen Sie in Interactive SQL eine Verbindung mit einer Datenbank her. Sie müssen mit einer Datenbank verbunden sein, um eine andere Datenbank erstellen zu können, z.B. mit der Dienstprogrammdatenbank.
2. Geben Sie die folgende Anweisung in den Fensterausschnitt **SQL-Anweisungen** von Interactive SQL ein (wobei *Datenbankname* der Name der neuen Datenbank ist):

```
CREATE DATABASE 'c:\\temp\\database-name.db'  
DBA USER 'DBA' DBA PASSWORD 'sql'  
TRANSACTION LOG ON  
CHECKSUM ON;
```

3. Klicken Sie im Menü **SQL** auf **Ausführen**.

Im Verzeichnis *c:\\temp* Ihres Computers werden eine Datenbank und ein Transaktionslog erstellt.

4. Kopieren Sie die Datenbank auf Ihr Windows Mobile-Gerät.

## Ergebnisse

Eine Datenbank wird erstellt und auf Ihr Windows Mobile-Gerät kopiert.

## Nächste Schritte

Sie können die Datenbank starten.

## Siehe auch

- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Eine Datenbank auf Ihr Windows Mobile-Gerät kopieren“ auf Seite 446
- „Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden“ auf Seite 434

## Eine Datenbank auf Ihr Windows Mobile-Gerät kopieren

Sie können SQL Anywhere Datenbanken auf Ihr Windows Mobile-Gerät kopieren.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Stellen Sie eine Verbindung zwischen dem Windows Mobile-Gerät und Ihrem Computer her.
2. Öffnen Sie Windows Explorer auf Ihrem PC.
3. Navigieren Sie auf Ihrem PC zu dem Verzeichnis, das die zu kopierende Datenbank enthält.
4. Rechtsklicken Sie auf die Datenbankdatei und klicken Sie auf **Kopieren**.
5. Navigieren Sie auf Ihrem Windows Mobile-Gerät zu dem Verzeichnis, in dem Sie die Datenbankdatei speichern wollen.

#### Tipp

Wenn Sie auf Ihrem Windows Mobile-Gerät eine Datenbank mit dem Fenster **Startoptionen für den Server** starten, können Sie mit **Durchsuchen** nur im Verzeichnis *Eigene Dateien* und dessen Unterverzeichnissen nach der Datenbankdatei suchen.

Falls die Datenbank nicht im Verzeichnis *Eigene Dateien* gespeichert ist, müssen Sie den Pfad der Datenbank im Fenster **Startoptionen für den Server** im Feld **Datenbank** eingeben.

6. Rechtsklicken Sie im Windows Explorer-Fenster Ihres Windows Mobile-Geräts auf einen leeren Bereich und klicken Sie dann auf **Einfügen**.

## Ergebnisse

Die Datei wird auf das Windows Mobile-Gerät kopiert.

## Nächste Schritte

Sie können Ihre Datenbank starten.

### Hinweis

Unter Windows Mobile nicht unterstützte Datenbankfunktionen funktionieren nicht, wenn Sie die Datenbank auf Ihr Windows Mobile-Gerät kopieren.

## Siehe auch

- „SQL Anywhere-Funktionsunterstützung unter Windows Mobile“ auf Seite 423
- „Datenbankserver starten und Datenbanken auf Ihrem Windows Mobile-Gerät verbinden“ auf Seite 434

## Neuaufbau von Datenbanken unter Windows Mobile

Wenn Sie eine Datenbank unter Windows Mobile neu aufbauen, haben Sie die folgenden Optionen:

- Die Windows Mobile-Datenbank auf einer anderen Plattform neu aufbauen und dann die Datenbank auf das Windows Mobile-Gerät kopieren. Dies ist die empfohlene Methode.
- Eine leere Datenbank mit "dbmlsync" neu füllen
- Eine leere Datenbank mit "dbremote" neu füllen
- "dbunload" auf dem Windows Mobile-Gerät verwenden Diese Option ist auf Smartphones nicht verfügbar.

Die ersten drei Optionen sind bei einem Upgrade der Windows Mobile-Datenbank zu empfehlen. Wenn diese Optionen Ihnen nicht zur Verfügung stehen, können Sie jedoch das Dienstprogramm zum Entladen (dbunload) unter Windows Mobile verwenden. Da das Ausführen von dbunload auf einem Windows Mobile-Gerät mehr Ressourcen erfordern kann, als auf manchen Geräten verfügbar sind, sollten Sie Upgrades der Datenbank nach Möglichkeit auf einer anderen Plattform durchführen.

## Datenbanken unter Windows Mobile neu aufbauen

Wenn Sie eine Datenbank unter Windows Mobile neu aufbauen möchten, können Sie das Dienstprogramm zum Entladen (dbunload) und das Dienstprogramm für die Skriptausführung (dbrunsql) verwenden. Diese Neuaufbauoption ist auf Smartphones nicht verfügbar. Diese Option wird nicht empfohlen, weil sie mehr Ressourcen erfordern kann, als auf manchen Geräten verfügbar sind. Es wird empfohlen, dass Sie die Datenbank auf einer anderen Plattform neu aufbauen und anschließend wieder auf das Windows Mobile-Gerät kopieren.

### Voraussetzungen

Vergewissern Sie sich, dass die Datenbank nicht läuft. Vergewissern Sie sich, dass keine Datenbankserver auf dem Gerät ausgeführt werden.

Sie müssen die Systemprivilegien SELECT ANY TABLE und SERVER OPERATOR haben.

### Hinweis

Wenn Sie dbunload auf einem Windows Mobile-Gerät ausführen möchten, müssen Sie die Option **Unterstützung für Entladen/Neuladen im Assistenten für das Deployment von SQL Anywhere 16 für Windows Mobile** wählen. Sie können Ihre SQL Anywhere-Installation ändern, um diese Unterstützung hinzuzufügen, falls Sie diese Option nicht beim erstmaligen Installieren von SQL Anywhere für Windows Mobile ausgewählt haben.

### Kontext und Bemerkungen

Bevor Sie sich entscheiden, "dbunload" unter Windows Mobile zu verwenden, sollten Sie die folgenden Implikationen bedenken:

- Die Größe der temporären Datei des Datenbankservers (Entladen und Neuladen können bewirken, dass diese Datei um mehrere MB wächst)
- Der zusätzliche Speicherplatz, der für "dbunload" und dazugehörige Komponenten erforderlich ist
- Die Zusatzkosten, mehrere Kopien einer Datenbank auf dem Windows Mobile-Gerät zu haben

### Aufgabe

1. Stellen Sie Folgendes sicher, wenn Sie dbunload auf einem Windows Mobile-Gerät verwenden möchten:
  - Die folgenden Dateien werden in Ihrem SQL Anywhere-Installationsverzeichnis (standardmäßig `\Program Files\SQLAny16`) bereitgestellt:
    - `dbsrv16.exe`
    - `dbsrv16.lic`
    - `dbunlspt.exe`
    - `dbunload.exe`
    - `dbrunsql.exe`
  - Die folgenden Dateien werden im Verzeichnis `\Windows` bereitgestellt, wenn Sie beabsichtigen, alte Datenbanken (Version 9 oder früher) zu entladen, und Sie die Datei `dbunlspt.exe` einbeziehen.
    - `Scripts\optdeflt.sql`
    - `Scripts\opttemp.sql`
    - `Scripts\unloadold.sql`
  - Die folgenden Dateien werden im Verzeichnis `\Windows` bereitgestellt:
    - `dblggen16.dll`
    - `dblib16.dll`
    - `dbscript16.dll`
    - `dbtool16.dll`
    - `dbusen.dll`
2. Vergewissern Sie sich, dass der Zeichenfolgenwert für **Location** (REG\_SZ) im folgenden Registrierungsschlüssel auf das SQL Anywhere-Softwareverzeichnis gesetzt ist:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Sybase\SQL Anywhere\ 16.0\`.

3. Erstellen Sie auf einer anderen Plattform als Windows Mobile eine neue, leere SQL Anywhere 16-Datenbank.

Die CHAR-Kollationssequenz muss mit derjenigen der vorhandenen Datenbank übereinstimmen. Wenn keine NCHAR UCA-Sortierung erforderlich ist, sollte die NCHAR-Kollationssequenz UTF8BIN sein. Dadurch benötigt der Datenbankserver nicht die ICU-Bibliotheken (*dbicu16.dll*, *dbicudt16.dat*).

4. Kopieren Sie die SQL Anywhere 16-Software und die leere SQL Anywhere-Datenbankdatei auf das Windows Mobile-Gerät.
5. Führen Sie den folgenden Befehl aus, um die Datenbank zu entladen:

```
dbunload-path\dbunload -c "UID=DBA;PWD=DBA-  
password;CHARSET=none;DBF=existing-database" unload-directory
```

6. Wenn dbunload abgeschlossen ist, schließen Sie das dbunload-Fenster.
7. Führen Sie den folgenden Befehl aus, um die Skriptdatei *reload.sql* für die leere SQL Anywhere-Datenbankdatei auszuführen:

```
dbrunsql-path\dbrunsql -c "UID=DBA;PWD=sql;CHARSET=none;DBF=new-empty-  
SQLAnywhere16database-file" -g- \reload.sql
```

8. Wenn dbrunsql abgeschlossen ist, schließen Sie das dbrunsql-Fenster.
9. Sie können die Datei *reload.sql* und das *unload-Verzeichnis* vom Windows Mobile-Gerät entfernen.

## Ergebnisse

Die Datenbank wird neu aufgebaut.

## Nächste Schritte

Die Befehle für dbunload und dbrunsql können in Windows Mobile-Anwendungen von Drittherstellern verwendet werden, um den Prozess für den Endbenutzer zu automatisieren. Wenn Sie dies vorhaben, sollten Sie erwägen, die dbunload- und dbrunsql-Optionen -qc bzw. -q zu verwenden oder die DBUnload-Funktion in *dbtool16.dll* aufzurufen.

## Siehe auch

- „Dienstprogramm zum Entladen (dbunload)“ auf Seite 1000
- „Skriptausführungs-Dienstprogramm (dbrunsql)“ auf Seite 959

## Sichern von Datenbanken unter Windows Mobile

Die Sicherung und Wiederherstellung von Daten ist unerlässlich, um im Falle von Datenbeschädigung oder Datenträgerfehlern einen Datenverlust zu verhindern. Am besten sichern Sie Ihre Windows Mobile-Datenbank auf einem physisch separaten Speicherort, um sie vor Datenverlust durch Diebstahl oder Verlust des Geräts bzw. Datenträgerfehlern auf dem Gerät zu schützen.

Die meisten Dienstprogramme zum Sichern und Wiederherstellen von Daten sind auch unter Windows Mobile verfügbar. Diese Dienstprogramme sind jedoch nicht von Nutzen, da Sie mit ihnen keine Windows Mobile-Sicherungen an einem physisch separaten Speicherort ablegen können (Ausnahme: Sicherung von Hauptspeicher-Datenbanken auf austauschbaren SD-Karten). Stattdessen können Daten durch Kopieren der gesamten Datenbankdatei auf einen PC gesichert werden. Sie können auch durch Synchronisation eine aktuelle Kopie Ihrer Windows Mobile-Datenbank auf einem PC aufbewahren.

### Siehe auch

- „MobiLink-Synchronisation“ [[MobiLink - Erste Orientierung](#)]

## Windows Mobile-Datenbanken über die Benutzeroberfläche des Geräts löschen

Löschen Sie Datenbanken über die Benutzeroberfläche des Geräts von Ihrem Windows Mobile-Gerät.

### Voraussetzungen

Die Datenbank darf nicht laufen.

### Kontext und Bemerkungen

SQL Anywhere für Windows Mobile unterstützt weder den **Assistenten zum Löschen einer Datenbank** noch die DROP DATABASE-Anweisung oder das Löschen-Dienstprogramm (dberase).

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » Datei-Explorer** und navigieren Sie zu dem Verzeichnis, das die zu löschende Datenbank enthält.
2. Tippen Sie und halten den Stift auf die Datenbankdatei.
3. Tippen Sie auf **Löschen**.
4. Tippen Sie auf **Ja**, um den Löschvorgang zu bestätigen.
5. Löschen Sie die Transaktionslogdatei (falls vorhanden).

### Ergebnisse

Die Datenbank wird gelöscht.

## Windows Mobile-Datenbanken mit dem Windows-Explorer löschen

Löschen Sie Datenbanken mit dem Windows-Explorer von Ihrem Windows Mobile-Gerät.

### Voraussetzungen

Die Datenbank darf nicht laufen.

## Kontext und Bemerkungen

SQL Anywhere für Windows Mobile unterstützt weder den **Assistenten zum Löschen einer Datenbank** noch die DROP DATABASE-Anweisung oder das Löschen-Dienstprogramm (dberase).

## Aufgabe

1. Setzen Sie Ihr Windows Mobile-Gerät in die Dockingstation ein und stellen Sie sicher, dass über das Windows Mobile-Gerätecenter (ActiveSync) eine Verbindung zum PC aufgebaut wird.
2. Öffnen Sie Windows Explorer auf Ihrem PC.
3. Navigieren Sie zum Windows Mobile-Verzeichnis, in dem die Datenbankdatei gespeichert ist.
4. Rechtsklicken Sie auf die Datenbankdatei und klicken Sie auf **Löschen**.
5. Klicken Sie auf **Ja**.
6. Löschen Sie die Transaktionslogdatei (falls vorhanden).

## Ergebnisse

Die Datenbank wird gelöscht.

# Datenbankserver unter Windows Mobile

Der Windows Mobile-Datenbankserver startet die TCP/IP-Netzwerkverbindung erst, wenn dies explizit angefordert wird.

Wenn Sie unter Windows Mobile versuchen, einen zweiten SQL Anywhere-Datenbankserver zu starten, während der erste noch läuft, wird der erste Server in den Vordergrund gebracht. Dies ist Standardverhalten bei Windows Mobile-Anwendungen. Aufgrund dieses Verhaltens können Sie auf einem Windows Mobile-Gerät nicht zwei Datenbankserver gleichzeitig ausführen. SQL Anywhere hingegen unterstützt das Ausführen mehrerer Datenbanken auf einem einzelnen Datenbankserver.

## Siehe auch

- [„Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen“ auf Seite 452](#)

# Serveroptionen unter Windows Mobile

Sie haben die Möglichkeit, beim Start des Datenbankservers Server- und Datenbankoptionen anzugeben, um das Verhalten und die Performance von SQL Anywhere zu optimieren. Sie können unter zahlreichen Optionen wählen, um beispielsweise festzulegen, wie viel Speicher der Cache belegen darf, welches Privileg erforderlich ist, um eine Datenbank auf dem Datenbankserver zu starten, und welche Netzwerkprotokolle verwendet werden sollen.

Unter Windows Mobile werden Optionen im Fenster **Server-Startoptionen** festgelegt. Hier besteht ein Unterschied zu anderen Windows-Betriebssystemen, bei denen die Datenbankserveroptionen in der Befehlszeile eingestellt werden können. Die meisten Serveroptionen sind für Windows Mobile verfügbar.

### Siehe auch

- [„Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203](#)
- [Unter Windows Mobile nicht unterstützte Serveroptionen auf Seite 426](#)

## Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen

Bei Sybase Central handelt es sich um ein Datenbankverwaltungstool, das eine grafische Benutzeroberfläche für die Verwaltung von SQL Anywhere zur Verfügung stellt. Sybase Central kann auch für die Verwaltung anderer Produkte, wie etwa MobiLink-Synchronisation, eingesetzt werden.

In dieser praktischen Einführung wird kurz vorgestellt, wie Sie mit Sybase Central von einem Desktopcomputer aus Datenbanken auf Ihrem Windows Mobile-Gerät verwalten, einschließlich Starten und Stoppen des Servers, Ausführen einzelner oder mehrerer Datenbanken auf einem Datenbankserver und Herstellen von Verbindungen mit Datenbanken.

### Privilegien

In dieser praktischen Einführung wird der **Assistent zum Erstellen einer Datenbank** verwendet, um eine neue Datenbank automatisch auf Ihr Windows Mobile-Gerät zu kopieren. Daher muss Sybase Central denselben Bitwert aufweisen wie ActiveSync oder das Windows Mobile-Gerätecenter (32 Bit oder 64 Bit). Unter Windows XP und früher wird nur 32-Bit-Software unterstützt.

### Siehe auch

- [„SQL Anywhere 16-Plug-In“ auf Seite 808](#)
- [„Tabellen, Ansichten und Indizes“ \[\*SQL Anywhere Server - SQL-Benutzerhandbuch\*\]](#)

## Lektion 1: Windows Mobile-Datenbanken erstellen

Sie müssen für diese praktische Einführung zwei Windows Mobile-Datenbanken erstellen.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Windows Mobile-Datenbanken über Sybase Central ausführen“](#).

### Aufgabe

1. Stellen Sie eine Verbindung zwischen Ihrem Windows Mobile-Gerät und dem Desktopcomputer her.
2. Starten Sie Sybase Central auf Ihrem Desktopcomputer.

3. Starten Sie den **Assistenten zum Erstellen einer Datenbank**. Klicken Sie auf **Extras » SQL Anywhere 16 » Datenbank erstellen**.
  - a. Klicken Sie auf der Seite **Eine Datenbankdatei angeben** auf **Durchsuchen** und wählen Sie einen Speicherort für die Datenbankdatei aus. Nennen Sie die Datenbankdatei *Alpha*. Klicken Sie auf **Speichern**.
  - b. Klicken Sie auf der Seite **Für Windows Mobile erstellen** auf **Diese Datenbank für Windows Mobile erstellen** und anschließend auf **Weiter**.

Der Assistent testet die Verbindung zu Ihrem Windows Mobile-Gerät.
  - c. Klicken Sie auf der Seite **Festlegen, ob Datenbank kopiert wird** auf **Datenbank auf das Windows Mobile-Gerät kopieren**.
  - d. Im Feld **Windows Mobile-Dateiname** geben Sie *\Eigene Dateien\Alpha.db* ein.
  - e. Klicken Sie auf **Datenbank nach dem Kopieren vom Desktopcomputer löschen** und anschließend auf **Weiter**.
  - f. Klicken Sie auf der Seite **Eine Kollationssequenz für NCHAR-Daten angeben** auf **Folgende mitgelieferte Kollation verwenden** und anschließend auf **UTF8BIN**.

Weitere Hinweise finden Sie unter „[Hinweise zur Installation: ICU unter Windows Mobile verwenden](#)“ auf Seite 430.
  - g. Klicken Sie auf **Fertig stellen** und anschließend auf **Schließen**.
4. Wiederholen Sie die vorherigen Schritte, um die Datenbank *\Eigene Dateien\Beta.db* zu erstellen.

## Ergebnisse

Sie haben zwei Windows Mobile-Datenbanken erstellt, *Alpha.db* und *Beta.db*.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 2: Datenbankserver starten](#)“ auf Seite 453.

# Lektion 2: Datenbankserver starten

Starten Sie den Datenbankserver auf Ihrem Windows Mobile-Gerät und stellen Sie eine Verbindung mit der Datenbank *Alpha.db* her.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Windows Mobile-Datenbanken erstellen](#)“ auf Seite 452.

## Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16**.
2. Tippen Sie auf **Server**.

- a. Im Feld **Datenbank** geben Sie *Alpha.db* ein.
- b. Im Feld **Servername** geben Sie **MobileServer** ein.
- c. Geben Sie in das Feld **Optionen -gd all -x tcpip(port=2639)** ein.

Die Option -gd stellt die Berechtigungen so ein, dass jeder Benutzer zusätzliche Datenbanken auf dem Netzwerk-Datenbankserver starten kann. Dies ist in einer späteren Lektion erforderlich. Siehe „Datenbankserveroption -gd“ auf Seite 240.

Der Datenbankserver verwendet Port 2639. Es empfiehlt sich, die Verwendung von Port 2638 zu vermeiden, weil dies der standardmäßige TCP/IP-Port für einen SQL Anywhere-Server ist, der auf Ihrem Desktopsystem läuft. Weitere Hinweise finden Sie unter „Datenbankserveroption -x“ auf Seite 305.

- d. Klicken Sie auf **Über TCP/IP**.  
Eine TCP/IP-Verbindung ist notwendig, um eine Verbindung zwischen einem PC und einer Datenbank auf Ihrem Windows Mobile-Gerät herzustellen.
- e. Tippen Sie auf **OK**, um die Beispieldatenbank auf dem Netzwerk-Datenbankserver zu starten.

3. Navigieren Sie auf Ihrem Gerät zum Bildschirm **Heute**.
4. Tippen Sie auf das Datenbankserversymbol unten rechts auf dem Bildschirm.

### Ergebnisse

Ein Datenbankserver wird gestartet und die Datenbank "Alpha" wird ausgeführt.

### Nächste Schritte

Wenn im Meldungsfenster des Datenbankservers die Meldung **Anforderungen werden jetzt akzeptiert** angezeigt wird, können Sie mit „Lektion 3: Verbindungen mit Windows Mobile-Datenbanken über Sybase Central herstellen“ auf Seite 454 fortfahren .

## Lektion 3: Verbindungen mit Windows Mobile-Datenbanken über Sybase Central herstellen

Starten Sie Sybase Central, um eine Verbindung mit der Datenbank "Alpha" herzustellen, die auf Ihrem Windows Mobile-Gerät ausgeführt wird.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „Lektion 1: Windows Mobile-Datenbanken erstellen“ auf Seite 452.

### Aufgabe

1. Starten Sie Sybase Central. Klicken Sie auf dem Desktopcomputer auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.

2. Klicken Sie auf **Verbindungen** » **Verbinden mit SQL Anywhere 16**.
3. Füllen Sie im Fenster **Verbinden** die folgenden Felder aus:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - c. Im Feld **Kennwort** geben Sie **sql** ein.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf einem anderen Computer verbinden**.
  - e. Im Feld **Host** geben Sie **169.254.2.1** ein.
  - f. Im Feld **Port** geben Sie **2639** ein.
  - g. Im Feld **Servername** geben Sie **MobileServer** ein.
  - h. Im Feld **Datenbankname** geben Sie **Alpha** ein.
4. Klicken Sie auf **Verbinden**, um eine Verbindung zur Datenbank *Alpha.db* herzustellen, die auf Ihrem Windows Mobile-Gerät ausgeführt wird.

## Ergebnisse

Wenn Sie die Verbindung mit einer Datenbank über Sybase Central herstellen, können Sie Daten zu den Tabellen in Ihrer Datenbank hinzufügen, Datenbankobjekte hinzufügen und bearbeiten sowie andere Administrationsaufgaben ausführen.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 4: Mehrere Datenbanken starten“ auf Seite 455](#).

# Lektion 4: Mehrere Datenbanken starten

Nachdem Sie jetzt den Datenbankserver gestartet und die Verbindung mit der Datenbank "Alpha" hergestellt haben, können Sie weitere Datenbanken auf Ihrem Windows Mobile-Gerät starten.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Windows Mobile-Datenbanken erstellen“ auf Seite 452](#).

## Kontext und Bemerkungen

Wenn Sie versuchen, einen zweiten SQL Anywhere-Datenbankserver auf einem Windows Mobile-Gerät zu starten, besteht das Standardverhalten für Windows Mobile-Anwendungen darin, den ersten Datenbankserver in den Vordergrund zu bringen. Aufgrund dieses Verhaltens können auf einem Windows Mobile-Gerät nicht zwei Datenbankserver gleichzeitig laufen. Als Alternative zum Ausführen mehrerer Datenbankserver kann ein Datenbankserver mehrere Datenbanken ausführen.

## Aufgabe

1. Rechtsklicken Sie im linken Fensterausschnitt von Sybase Central auf **MobileServer** und klicken Sie auf **Datenbank starten**.
  - a. Geben Sie im Feld **Datenbankdatei** Folgendes ein: **\My Documents\Beta.db**.
  - b. Klicken Sie auf **OK**, um die Datenbank auf dem Netzwerk-Datenbankserver zu starten.

Die Datenbank wird auf dem Netzwerk-Datenbankserver gestartet. Nun müssen Sie von Ihrem Desktopcomputer aus eine Verbindung initiieren.

2. Rechtsklicken Sie im linken Fensterausschnitt von Sybase Central auf **Beta** und klicken Sie dann auf **Verbinden**.
3. Füllen Sie im Fenster **Verbinden** die folgenden Felder aus:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - c. Im Feld **Kennwort** geben Sie **sql** ein.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf einem anderen Computer verbinden**.
  - e. Im Feld **Host** geben Sie **169.254.2.1** ein.
  - f. Im Feld **Port** geben Sie **2639** ein.
  - g. Im Feld **Servername** geben Sie **MobileServer** ein.
  - h. Im Feld **Datenbankname** geben Sie **Beta** ein.
4. Klicken Sie auf **Verbinden**, um eine Verbindung mit *Beta.db* herzustellen.

## Ergebnisse

Nun können Sie mithilfe von Sybase Central die Daten in den Datenbanken "Alpha" und "Beta" anzeigen und bearbeiten.

Wenn Sie die Verbindung mit einer Datenbank über Sybase Central herstellen, können Sie Daten zu den Tabellen in Ihrer Datenbank hinzufügen, Datenbankobjekte hinzufügen und bearbeiten sowie andere Administrationsaufgaben ausführen.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 5: Datenbankserver unter Windows Mobile herunterfahren](#)“ auf Seite 456.

## Lektion 5: Datenbankserver unter Windows Mobile herunterfahren

Bevor Sie den Netzwerk-Datenbankserver auf Ihrem Windows Mobile-Gerät herunterfahren können, müssen Sie die Verbindungen von Ihrem Desktopcomputer aus trennen.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Windows Mobile-Datenbanken erstellen](#)“ auf Seite 452.

## Aufgabe

1. Klicken Sie in Sybase Central auf **Verbindungen » Trennen**.
2. Wählen Sie die Verbindung, die zur Datenbank "Alpha" gehört.
3. Klicken Sie auf **OK**.

Die Verbindung mit der Datenbank "Alpha" wird getrennt.

4. Wiederholen Sie die vorherigen Schritte, um die Verbindung mit der Datenbank "Beta" zu trennen.
5. Nachdem Sie die Verbindungen mit den Windows Mobile-Datenbanken in Sybase Central getrennt haben, können Sie nun den Netzwerk-Datenbankserver herunterfahren.

Auf dem Windows Mobile-Gerät tippen Sie auf das Datenbankserver-Symbol unten rechts auf dem Bildschirm **Heute**.

6. Tippen Sie auf **Menü » Herunterfahren**.

## Ergebnisse

Die Windows Mobile-Datenbanken werden von Sybase Central getrennt und der Datenbankserver wird heruntergefahren.

# Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten

Interactive SQL ist eine Anwendung, mit deren Hilfe Sie Daten in Ihrer Datenbank abfragen und ändern sowie die Struktur der Datenbank ändern können. Interactive SQL bietet einen Fensterausschnitt, in dem Sie SQL-Anweisungen ausführen können, und Fensterausschnitte, in denen Informationen zur Verarbeitung der jeweiligen Abfrage sowie die Ergebnismenge angezeigt werden.

In dieser praktischen Einführung wird kurz vorgestellt, wie Sie mit Interactive SQL von einem Desktopcomputer aus Datenbanken auf Ihrem Windows Mobile-Gerät verwalten, einschließlich Herstellen der Verbindung mit der Beispieldatenbank auf Ihrem Windows Mobile-Gerät über Interactive SQL. Nachdem die Verbindung hergestellt wurde, können Sie SQL-Anweisungen mithilfe von Interactive SQL ausführen.

## Privilegien

Wenn Sie Daten in den Tabellen auswählen möchten, benötigen Sie die entsprechenden SELECT-Privilegien für die Objekte, die in der SELECT-Anweisung referenziert werden.

## Lektion 1: Beispieldatenbank starten

Starten Sie die Beispieldatenbank auf Ihrem Windows Mobile-Gerät, damit Sie über Interactive SQL eine Verbindung mit ihr herstellen können.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten“](#).

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16**.
2. Tippen Sie auf **Server**.
  - a. Geben Sie im Feld **Datenbank** den Pfad der Beispieldatenbank ein. Der Standardspeicherort ist `\Eigene Dateien\demo.db`. Alternativ dazu suchen Sie mithilfe von **Durchsuchen** nach der Datei `demo.db`.
  - b. Im Feld **Servername** geben Sie **MobileServer** ein.
  - c. Geben Sie in das Feld **Cache 5M** ein.

Die Standard-Cachegröße unter Windows Mobile beträgt 600 kB. Eine größere Cachegröße kann jedoch die Performance verbessern.
  - d. Im Feld **Optionen** geben Sie **-x tcpip(port=2639)** ein.

Der Datenbankserver verwendet Port 2639. Es empfiehlt sich, die Verwendung von Port 2638 zu vermeiden, weil dies der standardmäßige TCP/IP-Port für einen SQL Anywhere-Server ist, der auf Ihrem Desktopsystem läuft. Weitere Hinweise finden Sie unter [„Datenbankserveroption - x“](#) auf Seite 305.
  - e. Klicken Sie auf **Über TCP/IP**.

Eine TCP/IP-Verbindung ist notwendig, um eine Verbindung zwischen einem PC und einer Datenbank auf Ihrem Windows Mobile-Gerät herzustellen.
  - f. Tippen Sie auf **OK**, um die Beispieldatenbank auf dem Netzwerk-Datenbankserver zu starten.
3. Navigieren Sie auf Ihrem Gerät zum Bildschirm **Heute**.
4. Tippen Sie auf das Datenbankserversymbol unten rechts auf dem Bildschirm.

### Ergebnisse

Die Beispieldatenbank wird auf Ihrem Windows Mobile-Gerät gestartet.

### Nächste Schritte

Wenn im Meldungsfenster des Datenbankservers die Meldung **Anforderungen werden jetzt akzeptiert** angezeigt wird, können Sie mit [„Lektion 2: Interactive SQL starten und Verbindung herstellen“](#) auf Seite 459 fortfahren.

## Lektion 2: Interactive SQL starten und Verbindung herstellen

Wenn die Beispieldatenbank auf Ihrem Windows Mobile-Gerät ausgeführt wird, stellen Sie zu ihr mit Interactive SQL eine Verbindung her, um die Datenbank von Ihrem PC aus anzuzeigen und zu verwalten.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beispieldatenbank starten](#)“ auf Seite 458.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten](#)“.

### Aufgabe

1. Starten Sie Interactive SQL. Klicken Sie auf dem Desktopcomputer auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Interactive SQL**.
2. Füllen Sie im Fenster **Verbinden** die folgenden Felder aus:
  - a. Klicken Sie in der Dropdown-Liste **Authentifizierung** auf **Datenbank**.
  - b. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - c. Im Feld **Kennwort** geben Sie **sql** ein.
  - d. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf einem anderen Computer verbinden**.
  - e. Im Feld **Host** geben Sie **169.254.2.1** ein.
  - f. Im Feld **Port** geben Sie **2639** ein.
  - g. Im Feld **Servename** geben Sie **MobileServer** ein.
  - h. Im Feld **Datenbankname** geben Sie **Demo** ein.
3. Klicken Sie auf **Verbinden**, um eine Verbindung mit der Beispieldatenbank herzustellen, die auf Ihrem Windows Mobile-Gerät ausgeführt wird.

### Ergebnisse

Interactive SQL wird auf Ihrem Desktopcomputer gestartet und eine Verbindung mit der Beispieldatenbank auf Ihrem Windows Mobile-Gerät wird hergestellt.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: Abfragen in einer Windows Mobile-Datenbank ausführen](#)“ auf Seite 460.

## Lektion 3: Abfragen in einer Windows Mobile-Datenbank ausführen

Verwenden Sie Interactive SQL, um in Ihrer Windows Mobile-Datenbank die Daten anzuzeigen und zu bearbeiten sowie Datenbankobjekte hinzuzufügen und zu ändern.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beispieldatenbank starten](#)“ auf Seite 458.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Windows Mobile-Datenbanken mit Interactive SQL verwalten](#)“.

### Kontext und Bemerkungen

In erster Linie wird Interactive SQL dazu verwendet, Tabellendaten zu durchsuchen. Interactive SQL ruft Daten ab, indem es eine Anforderung an einen Datenbankserver sendet. Der Datenbankserver sucht die Daten und gibt sie an Interactive SQL zurück.

### Aufgabe

1. Führen Sie in Interactive SQL die folgende Anweisung aus:

```
SELECT * FROM Employees;
```

2. Klicken Sie im Menü **SQL** auf **Ausführen**, um die Anweisung auszuführen.

Alle Daten aus der Tabelle "Employees" werden jetzt im Fensterausschnitt **Ergebnisse** angezeigt.

3. Klicken Sie im Menü **SQL** auf **Trennen**, um Interactive SQL von der Windows Mobile-Datenbank zu trennen.

### Ergebnisse

Sie haben eine Abfrage ausgeführt, um Tabellendaten zu durchsuchen, und die Verbindung mit Ihrer Windows Mobile-Datenbank über Interactive SQL getrennt.

### Nächste Schritte

(Optional) Fahren Sie den Datenbankserver auf Ihrem Windows Mobile-Gerät herunter.

### Siehe auch

- „Interactive SQL“ auf Seite 814
- „Abfragen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Abfrageergebnisse zusammenfassen, gruppieren und sortieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Joins: Daten aus mehreren Tabellen abrufen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SQL-Anweisungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Praktische Einführung: Windows Mobile-Beispielanwendungen verwenden

Die folgenden Beispielanwendungen sind bei der Installation von SQL Anywhere für Windows Mobile enthalten:

- ADO.NET Sample
- ESQL Sample
- ODBC Sample

Mit diesen Anwendungen können Sie auf die Beispieldatenbank zugreifen und die Funktionen von SQL Anywhere für Windows Mobile testen.

### Siehe auch

- „Hinweise zur Installation: ICU unter Windows Mobile verwenden“ auf Seite 430
- „Lektion 2: ADO.NET-Beispiel für Windows Mobile verwenden“ auf Seite 461
- „Lektion 3: ESQL-Beispiel für Windows Mobile verwenden“ auf Seite 463
- „Lektion 4: ODBC-Beispiel für Windows Mobile verwenden“ auf Seite 464

## Lektion 2: ADO.NET-Beispiel für Windows Mobile verwenden

ADO.NET Sample zeigt eine einfache Anwendung, die die ADO.NET-Programmierschnittstelle verwendet. Mit dieser Anwendung können Sie die Beispieldatenbank auf dem Netzwerk-Datenbankserver starten und über SQL-Anweisungen darauf zugreifen und Daten ändern.

### Voraussetzungen

Um das ADO.NET Sample verwenden zu können, muss auf Ihrem Gerät das Microsoft .NET Compact Framework, Version 2.0 oder 3.0, installiert sein. Das Microsoft .NET Compact Framework Version 2.0 ist auf Windows Mobile 6-Geräten, aber nicht auf Windows Mobile 5-Geräten enthalten. Das ADO.NET Sample unterstützt nur Windows Mobile Classic- und Professional-Geräte mit Touch-Screens.

Wenn Sie Daten in den Tabellen auswählen möchten, benötigen Sie die entsprechenden SELECT-Privilegien für die Objekte, die in der SELECT-Anweisung referenziert werden.

Wenn Sie die Daten in den Tabellen aktualisieren möchten, müssen Sie der Eigentümer der zu aktualisierenden Tabelle sein bzw. das UPDATE-Privileg für die zu ändernden Spalten oder das UPDATE ANY TABLE-Systemprivileg haben.

### Kontext und Bemerkungen

Der Quellcode für diese Beispielanwendung befindet sich in `%SQLANY%SAMP16%\SQLAnywhere\ce\ado_net_sample`.

Sie können dieses Projekt in Microsoft Visual Studio aus dem `%SQLANY%SAMP16%\SQLAnywhere\ce\ado_net_sample\ado_net_sample.sln` laden.

Um diese Komponente vom Microsoft Download Center herunterzuladen, gehen Sie zu <http://www.microsoft.com/downloads/search.aspx?displaylang=en>.

### Hinweis

Auf der Benutzeroberfläche von ADO.NET Sample müssen SQL-Anweisungen in einer einzigen Zeile eingegeben werden.

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16 » ADO.NET-Beispiel**.

2. Tippen Sie auf **Connect** (Verbinden).

Wenn der SQL Anywhere-Datenbankserver nicht bereits gestartet wurde, dann tippen Sie auf **Connect** (Verbinden), um dies nachzuholen.

3. Tippen Sie auf **Exec SQL**, um die Standard-SQL-Anweisung **SELECT \* FROM Employees** auszuführen.

Daten aus der Tabelle "Employees" werden im Datenfenster angezeigt.

4. Navigieren Sie mit den Bildlaufleisten an der Seite und unten im Datenfenster durch die Daten in der Tabelle "Employees".

5. Geben Sie die folgende Abfrage ein, um auf einen spezifischeren Datenbereich zuzugreifen:

```
SELECT EmployeeID, Surname FROM Employees;
```

6. Tippen Sie auf **Exec SQL**, um die SQL-Anweisung auszuführen.

Der spezifische Datenbereich ersetzt die Daten, die zuvor im Datenfensterausschnitt angezeigt wurden.

7. Geben Sie **SELECT \* FROM Employees ORDER BY EmployeeID** ein und tippen Sie auf **Exec SQL**.

Beachten Sie den Mitarbeiter Matthew Cobb mit der EmployeeID 105.

8. Geben Sie **UPDATE Employees SET Surname = 'Jones' WHERE Surname = 'Cobb'** ein und tippen Sie anschließend auf **Exec SQL**, um die SQL-Anweisung auszuführen.

9. Geben Sie **SELECT \* FROM Employees ORDER BY EmployeeID** ein und tippen Sie auf **Exec SQL**.

Beachten Sie, dass Matthews Nachname von Cobb auf Jones geändert wird.

10. Geben Sie **UPDATE Employees SET Surname = 'Cobb' WHERE Surname = 'Jones'** ein und tippen Sie anschließend auf **Exec SQL**, um die Änderungen zurückzusetzen, die Sie in der Beispieldatenbank durchgeführt haben.

11. Überprüfen Sie, dass die Änderungen zurückgesetzt wurden, indem Sie **SELECT \* FROM Employees ORDER BY EmployeeID** eingeben und anschließend auf **Exec SQL** tippen.

Beachten Sie, dass Matthews Nachname wieder auf Cobb geändert wird.

12. Greifen Sie auf Daten in einer anderen Tabelle zu, indem Sie **SELECT \* FROM Customers** eingeben und dann auf **Exec SQL** tippen.

Alle Daten der Tabelle "Customers" werden im Datenfenster angezeigt und ersetzen die Daten der Tabelle "Employees".

13. Trennen Sie die Verbindung zum Datenbankserver, indem Sie auf **Disconnect** (Trennen) tippen.

ADO.NET Sample wird getrennt. Der Datenbankserver wird nicht automatisch heruntergefahren, weil die Verbindung gepoolt ist.

14. Schließen Sie ADO.NET Sample, indem Sie auf das kleine Kreuz × rechts oben im Fenster tippen.

### Ergebnisse

Sie haben die Beispieldatenbank gestartet sowie mithilfe von SQL-Anweisungen auf Daten zugegriffen und sie geändert.

## Lektion 3: ESQL-Beispiel für Windows Mobile verwenden

ESQL Sample zeigt eine einfache Anwendung, die die Embedded SQL-Programmierschnittstelle verwendet. Mit dieser Anwendung können Sie die Beispieldatenbank auf dem Netzwerk-Datenbankserver starten und über SQL-Anweisungen darauf zugreifen.

### Voraussetzungen

Wenn Sie Daten in den Tabellen auswählen möchten, benötigen Sie die entsprechenden SELECT-Privilegien für die Objekte, die in der SELECT-Anweisung referenziert werden.

### Kontext und Bemerkungen

Der Quellcode für diese Beispielanwendung befindet sich in *%SQLANYAMP16%\SQLAnywhere\ce\esql\_sample*.

Sie können diese Projektdatei in Visual Studio 2005 von folgendem Ort aus laden: *%SQLANYAMP16%\SQLAnywhere\ce\esql\_sample\esql\_sample.sln*.

#### Hinweis

Auf der Benutzeroberfläche von ESQL Sample müssen SQL-Anweisungen in einer einzigen Zeile eingegeben werden.

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16 » ESQL-Beispiel**.
2. Tippen Sie auf **Connect**, um unter Verwendung der Standardverbindungszeichenfolge eine Verbindung zur Beispieldatenbank herzustellen.

3. Tippen Sie auf **ExecSQL**, um die Standard-SQL-Anweisung **SELECT \* FROM Employees** auszuführen.

Daten aus der Tabelle "Employees" werden im Datenfenster angezeigt.

4. Verwenden Sie die Abrollleisten, um Mitarbeiter-Tabellendaten anzuzeigen.
5. Um auf die Tabelle "Customers" zuzugreifen, geben Sie **SELECT \* FROM Customers** ein und tippen auf **ExecSQL**.

Kundendaten ersetzen Mitarbeiterdaten im Datenfenster.

6. Tippen Sie auf **Menü » Disconnect** (Trennen), um den Netzwerk-Datenbankserver herunterzufahren.  
ESQL Sample trennt die Verbindung und der Netzwerk-Datenbankserver wird heruntergefahren.
7. Schließen Sie ESQL Sample, indem Sie auf das kleine Kreuz × rechts oben im Fenster tippen.

### Ergebnisse

Sie haben die Beispieldatenbank gestartet und mithilfe von SQL-Anweisungen auf Daten zugegriffen.

## Lektion 4: ODBC-Beispiel für Windows Mobile verwenden

ODBC Sample zeigt eine einfache Anwendung, die die ODBC-Programmierschnittstelle verwendet. Mit dieser Anwendung können Sie die Beispieldatenbank auf dem Netzwerk-Datenbankserver starten und über grundlegende SQL-Anweisungen darauf zugreifen.

### Voraussetzungen

Wenn Sie Daten in den Tabellen auswählen möchten, benötigen Sie die entsprechenden SELECT-Privilegien für die Objekte, die in der SELECT-Anweisung referenziert werden.

### Kontext und Bemerkungen

Der Quellcode für diese Beispielanwendung befindet sich in `%SQLANYAMP16%\SQLAnywhere\ce\odbc_sample`.

Sie können diese Projektdatei in Visual Studio 2005 von folgendem Ort aus laden: `%SQLANYAMP16%\SQLAnywhere\ce\odbc_sample\odbc_sample.sln`.

#### Hinweis

Auf der Benutzeroberfläche von ODBC Sample müssen SQL-Anweisungen in einer einzigen Zeile eingegeben werden.

### Aufgabe

1. Tippen Sie auf Ihrem Windows Mobile-Gerät auf **Start » Programme » SQLAny16 » ODBC-Beispiel**.

2. Tippen Sie auf **Connect** (Verbinden).
3. Tippen Sie auf **ExecSQL**, um die Standard-SQL-Anweisung **SELECT \* FROM Employees** auszuführen.

Daten aus der Tabelle "Employees" werden im Datenfenster angezeigt.

4. Verwenden Sie die Abrollleisten, um Employee-Tabellendaten anzuzeigen.
5. Um auf die Tabelle "Customers" zuzugreifen, geben Sie **SELECT \* FROM Customers** ein und tippen auf **ExecSQL**.

Kundendaten ersetzen Mitarbeiterdaten im Datenfenster.

6. Tippen Sie auf **Menü » Disconnect** (Trennen), um den Netzwerk-Datenbankserver herunterzufahren.

ODBC Sample trennt die Verbindung und der Netzwerk-Datenbankserver wird heruntergefahren.

7. Schließen Sie ODBC Sample.

### **Ergebnisse**

Sie haben die Beispieldatenbank gestartet und mithilfe von SQL-Anweisungen auf Daten zugegriffen.



---

# Datenbankkonfiguration

Dieser Abschnitt beschreibt die Dateien, die von SQL Anywhere genutzt werden, Einschränkungen der Datenbanken und wie Sie Datenbankeigenschaften und Optionen konfigurieren. In diesem Kapitel wird beschrieben, wie SQL Anywhere für die Verwendung anderer Sprachen als Englisch konfiguriert wird.

## SQL Anywhere-Umgebungsvariablen

SQL Anywhere benutzt Umgebungsvariablen, um bestimmte Informationen zu speichern. Nicht alle Umgebungsvariablen müssen unter allen Umständen gesetzt werden.

Beim SQL Anywhere-Server können Sie die für einen bestimmten Server gesetzten Umgebungsvariablen anzeigen, indem Sie den Server mit der Option `-ze` starten. Nach dem Starten des Servers können Sie Umgebungsvariablen mit der `xp_getenv`-Systemprozedur anzeigen.

### Umgebungsvariablen unter Windows setzen

Das SQL Anywhere-Installationsprogramm erstellt oder ändert die folgenden Umgebungsvariablen in den Eigenschaften Ihres Computers: `PATH` und `SQLANY16`.

Andere Umgebungsvariablen können gesetzt werden, indem Sie die Eigenschaften für Ihren Computer ändern bzw. indem Sie innerhalb von Eingabeaufforderungen oder Batchdateien den `SET`-Befehl verwenden.

### Siehe auch

- „Datenbankserveroption `-z`“ auf Seite 312
- „`xp_getenv`-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Unix- und Mac OS X-Umgebungsvariablen

Nach der Installation von SQL Anywhere muss jeder Benutzer Umgebungsvariablen setzen, damit das System SQL Anywhere-Anwendungen finden und ausführen kann. Zu diesem Zweck erstellt das SQL Anywhere-Installationsprogramm die beiden Dateien `sa_config.sh` und `sa_config.csh`. Diese Dateien befinden sich in `SQLANY16/bin32` und `SQLANY16/bin64`. Jede Datei richtet alle erforderlichen Umgebungsvariablen ein.

Wie aus den Namen ersichtlich wird, ist eine Datei für die Bourne-Shell (`sh`) und davon abgeleitete Shells (`ksh` oder `bash`) vorgesehen. Die andere Datei läuft unter der C-Shell (`csh`) und davon abgeleiteten Shells (z.B. `tcsh`).

In diesen Batchdateien sind einige Anweisungen auskommentiert. Der Systemadministrator kann diese Dateien je nach Systemkonfiguration bearbeiten und Kommentare entfernen.

Um eine SQL Anywhere-Anwendung auszuführen, gibt es mehrere Optionen:

1. Wenn Sie Umgebungsvariable aus den *sa\_config*-Dateien Ihrer Systemumgebung hinzufügen, können Sie Anwendungen ausführen, indem Sie sie von einer GUI, wie z.B. X Window-Server, starten oder den Anwendungsnamen in ein Terminalfenster eingeben.
2. Wenn Sie eine der *sa\_config*-Dateien als Source nehmen wollen, können Sie die Anwendung ausführen, indem Sie ihren Namen in ein Terminalfenster eintippen. Siehe „[sa\\_config.sh und sample\\_config32.sh/sample\\_config64.sh sourcen \[Unix und Mac OS X\]](#)“ auf Seite 468.
3. *\$SQLANY16/bin32s* und *\$SQLANY16/bin64s* enthalten Skripten mit demselben Namen wie SQL Anywhere-Anwendungen. Diese Skripten setzen die entsprechenden Umgebungsvariablen, bevor die Anwendung gestartet wird. Sie können die Anwendung ausführen, indem Sie das entsprechende Skript ausführen. Sie müssen keine *sa\_config*-Datei als Source nehmen, um diese Skripten auszuführen.

### Umgebungsvariablen für den Finder in Mac OS X setzen

Das SQL Anywhere-Installationsprogramm richtet folgende Umgebungsvariablen ein: DYLD\_LIBRARY\_PATH, ODBCINI, PATH und SQLANY16. Ein Neustart ist nicht erforderlich.

Terminalsitzungen übernehmen keine Umgebungsvariablen vom Finder. Weitere Hinweise zur Einstellung der Umgebungsvariablen für Terminalsitzungen finden Sie unter „[sa\\_config.sh und sample\\_config32.sh/sample\\_config64.sh sourcen \[Unix und Mac OS X\]](#)“ auf Seite 468.

## ***sa\_config.sh und sample\_config32.sh/sample\_config64.sh sourcen [Unix und Mac OS X]***

Eine Datei **sourcen** bedeutet, die in einer Textdatei enthaltenen Befehle in der aktuellen Instanz der Shell auszuführen. Dies erfolgt mit einem für diese Shell gültigen Befehl.

Unter der Bourne-Shell und ihren Derivaten lautet dieser Befehl `.` (ein einzelner Punkt). Beispiel: Wenn SQL Anywhere in */opt/sqlanywhere16* installiert ist, legt die folgende Anweisung *sa\_config.sh* als Source fest:

```
. /opt/sqlanywhere16/bin32/sa_config.sh
```

Auf einem Mac können Sie beispielsweise den folgenden Befehl ausführen, um *sa\_config.sh* zu sourcen:

```
. Applications/SQLAnywhere16/System/bin32/sa_config.sh
```

Unter der C-Shell und ihren Derivaten lautet dieser Befehl `source`. Beispiel: Wenn SQL Anywhere in */opt/sqlanywhere16* installiert ist, bewirkt die folgende Anweisung das Sourcen von *sa\_config.csh*:

```
source /opt/sqlanywhere16/bin32/sa_config.csh
```

### Konfiguration der Beispiele

Führen Sie vor der Verwendung der Beispiele für SQL Anywhere 16 das Konfigurationsskript aus, das dem zu verwendenden Bitwert von SQL Anywhere entspricht. Zum Konfigurieren der Beispiele für 32-Bit-Software geben Sie z.B. Folgendes an:

```
. /opt/sqlanywhere16/samples/sample_config32.sh
```

Auf einem Mac führen Sie zum Konfigurieren der Beispiele für die Verwendung mit einer 32-Bit-Software folgende Anweisung aus:

```
. Applications/SQLAnywhere16/samples/sample_config32.sh
```

## DYLD\_LIBRARY\_PATH-Umgebungsvariable [Mac OS X]

Gibt die Verzeichnisse an, in denen zur Zeit der Ausführung nach den Bibliotheken gesucht wird, die für SQL Anywhere-Anwendungen unter Mac OS X erforderlich sind.

### Syntax

**DYLD\_LIBRARY\_PATH**=*path-list*

### Standardwert

*/Applications/SQLAnywhere16/System/lib32*

### Bemerkungen

Die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, sind Skripten, die diese oder andere Umgebungsvariablen erstellen oder ändern.

### Siehe auch

- „LD\_LIBRARY\_PATH-Umgebungsvariable [Linux und Solaris]“ auf Seite 469
- „LIBPATH-Umgebungsvariable [IBM AIX]“ auf Seite 470
- „SHLIB\_PATH-Umgebungsvariable [HP-UX]“ auf Seite 477
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## LD\_LIBRARY\_PATH-Umgebungsvariable [Linux und Solaris]

Gibt die Verzeichnisse an, in denen zur Zeit der Ausführung nach den Bibliotheken gesucht wird, die für SQL Anywhere-Anwendungen unter Linux und Solaris erforderlich sind.

### Syntax

**LD\_LIBRARY\_PATH**=*path-list*

### Standardwert

- **Linux und Solaris (32-Bit)**

```
$SQLANY16/lib32:  
$SQLANY16/lib64:  
$SQLANY16/bin32/jre170/lib/i386/client:  
$SQLANY16/bin32/jre170/lib/i386/server:  
$SQLANY16/bin32/jre170/lib/i386:  
$SQLANY16/bin32/jre170/lib/i386/native_threads
```

- **Linux und Solaris (64-Bit)**

```
$SQLANY16/lib32:  
$SQLANY16/lib64:  
$SQLANY16/bin64/jre170/lib/amd64/client:  
$SQLANY16/bin64/jre170/lib/amd64/server:  
$SQLANY16/bin64/jre170/lib/amd64:  
$SQLANY16/bin64/jre170/lib/amd64/native_threads
```

### Bemerkungen

Die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, sind Skripten, die diese oder andere Umgebungsvariablen erstellen oder ändern.

### Siehe auch

- „DYLD\_LIBRARY\_PATH-Umgebungsvariable [Mac OS X]“ auf Seite 469
- „LIBPATH-Umgebungsvariable [IBM AIX]“ auf Seite 470
- „SHLIB\_PATH-Umgebungsvariable [HP-UX]“ auf Seite 477
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## LIBPATH-Umgebungsvariable [IBM AIX]

Gibt die Verzeichnisse an, in denen zur Zeit der Ausführung nach den Bibliotheken gesucht wird, die für SQL Anywhere-Anwendungen unter IBM AIX erforderlich sind.

### Syntax

**LIBPATH**=*path-list*

### Standardwert

- */usr/lpp/sqlanywhere16/lib32* (32-Bit-Plattformen)
- */usr/lpp/sqlanywhere16/lib64* (64-Bit-Plattformen)

### Bemerkungen

Die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, sind Skripten, die diese oder andere Umgebungsvariable erstellen oder ändern.

### Siehe auch

- „DYLD\_LIBRARY\_PATH-Umgebungsvariable [Mac OS X]“ auf Seite 469
- „LD\_LIBRARY\_PATH-Umgebungsvariable [Linux und Solaris]“ auf Seite 469
- „SHLIB\_PATH-Umgebungsvariable [HP-UX]“ auf Seite 477
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## ODBCHOME-Umgebungsvariable [Unix]

Gibt den Speicherort der *.odbc.ini*-Datei an.

### Syntax

**ODBCHOME**=*odbc-ini-directory*

**Bemerkungen**

Die Datei *.odbc.ini* ist die Systeminformationsdatei, die die ODBC-Datenquellen enthält. Wenn der Dateiname ein anderer als *.odbc.ini* ist, müssen Sie die ODBCINI- oder ODBC\_INI-Umgebungsvariablen verwenden, um den Speicherort anzugeben.

Hinweise über den Algorithmus zum Auffinden von ODBC-Datenquellen finden Sie unter [„ODBC-Datenquellen unter Unix“ auf Seite 49](#).

**Siehe auch**

- [„ODBCINI- und ODBC\\_INI-Umgebungsvariable \[Unix\]“ auf Seite 471](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## ODBCINI- und ODBC\_INI-Umgebungsvariable [Unix]

Gibt den Pfad und den Namen der Systeminformationsdatei an, die ODBC-Datenquellen enthält.

**Syntax**

**ODBCINI**=*odbc-ini-file*

**ODBC\_INI**=*odbc-ini-file*

**Bemerkungen**

Der Dateiname muss nicht *.odbc.ini* sein, wenn er mit einer dieser Umgebungsvariablen angegeben wird. Beide Umgebungsvariablen werden aus Gründen der Kompatibilität mit anderen Produkten bereitgestellt.

Hinweise über den Algorithmus zum Auffinden von ODBC-Datenquellen finden Sie unter [„ODBC-Datenquellen unter Unix“ auf Seite 49](#).

**Siehe auch**

- [„ODBCHOME-Umgebungsvariable \[Unix\]“ auf Seite 470](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## PATH-Umgebungsvariable

Gibt die Speicherorte von Verzeichnissen an, die ausführbare Dateien von SQL Anywhere enthalten.

**Syntax**

**PATH**=*path-list*

**Standardwert**

Die folgenden Pfade werden nur hinzugefügt, wenn die entsprechende Komponente installiert ist.

Betriebssystem	Standardspeicherort
Windows (32-Bit)	<i>C:\Program Files\SQL Anywhere 16\bin32</i>

Betriebssystem	Standardspeicherort
Windows (64-Bit)	<i>C:\Program Files\SQL Anywhere 16\bin64</i>
Mac OS X (32-Bit)	<i>/Applications/SQLAnywhere16/System/bin32</i>
Mac OS X (64-Bit)	<i>/Applications/SQLAnywhere16/System/bin64</i>
IBM AIX (32-Bit)	<i>/usr/lpp/sqlanywhere16/bin32</i>
IBM AIX (64-Bit)	<i>/usr/lpp/sqlanywhere16/bin64</i>
Solaris Sparc (32-Bit und 64-Bit)	<i>/opt/sqlanywhere16/sun/jre160/bin</i>
Linux (32-Bit)	<i>/opt/sqlanywhere16/bin32:/opt/sqlanywhere16/bin32/jre170/</i>
Linux (64-Bit)	<i>/opt/sqlanywhere16/bin32:/opt/sqlanywhere16/bin64/jre170</i>
Andere Unix-Betriebssysteme (32-Bit)	<i>/opt/sqlanywhere16/bin32</i>
Andere Unix-Betriebssysteme (64-Bit)	<i>/opt/sqlanywhere16/bin64</i>

### Bemerkungen

Unter Windows wird die Umgebungsvariable PATH vom Installationsprogramm verändert, um die Verzeichnisse einzubeziehen, in denen Programmdateien von SQL Anywhere untergebracht sind.

Unter Unix sind die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, Skripten, die diese oder andere Umgebungsvariablen erstellen oder ändern.

### Siehe auch

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)
- [„sa\\_config.sh und sample\\_config32.sh/sample\\_config64.sh sourcen \[Unix und Mac OS X\]“ auf Seite 468](#)

## SACHARSET-Umgebungsvariable

Gibt den von SQL Anywhere verwendeten Zeichensatz an.

### Syntax

**SACHARSET**=*charset-label*

### Bemerkungen

*charset-label* steht für ein Zeichensatzlabel.

Weitere Hinweise zu den empfohlenen Zeichensatzlabels für Windows- und Unix-Betriebssysteme finden Sie unter [„Empfohlene Zeichensätze und Kollationen“ auf Seite 529](#).

Mit der dbinit-Option `-le` können Sie eine Liste aller verfügbaren Zeichensatzlabels für eine SQL Anywhere-Datenbank abrufen. Die dbinit-Option `-l` gibt die für eine SQL Anywhere-Datenbank verfügbaren Kollationen zurück. Siehe „[Dienstprogramm Initialisierung \(dbinit\)](#)“ auf Seite 927.

Wenn SACHARSET nicht angegeben ist, kommt der Zeichensatz vom Betriebssystem.

**Siehe auch**

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## SADIAGDIR-Umgebungsvariable

Gibt den Speicherort des SQL Anywhere-Diagnoseverzeichnisses an.

**Syntax**

**SADIAGDIR**=*diagnostic-information-directory*

**Standardwert**

Diese Umgebungsvariable ist nicht standardmäßig gesetzt.

**Bemerkungen**

Diese Umgebungsvariable setzt den Standardspeicherort des SQL Anywhere-Diagnoseverzeichnisses außer Kraft. SQL Anywhere-Programme verwenden dieses Verzeichnis zum Speichern von Berichten, wenn in der Software ein schwerwiegender Fehler auftritt.

Informationen zu Absturzberichten und Funktionsstatistiken werden von SQL Anywhere im Diagnoseverzeichnis gespeichert. Die SADIAGDIR-Umgebungsvariable wird verwendet, um den Speicherort des Diagnoseverzeichnisses anzugeben, in das SQL Anywhere Crash-Berichte schreibt.

Falls das von dieser Umgebungsvariablen angegebene Verzeichnis nicht existiert, verhält sich der Datenbankserver so, als ob die Umgebungsvariable nicht gesetzt wurde.

**Siehe auch**

- [Speicherort des Diagnoseverzeichnisses auf Seite 995](#)
- [„Dienstprogramm für Supportanfragen \(dbsupport\)“ auf Seite 987](#)
- [„Fehlerbehandlung: Fehler in SQL Anywhere melden“ auf Seite 1108](#)
- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## SALANG-Umgebungsvariable

Gibt den Sprachcode für SQL Anywhere an.

**Syntax**

**SALANG**=*language-code*

## Bemerkungen

*language-code* besteht aus zwei Buchstaben und steht für eine Sprache. Mit der Einstellung **SALANG=DE** wird die Standardsprache auf Deutsch gesetzt.

Weitere Informationen zu unterstützten Sprachcodes finden Sie unter [„Sprache der Sprachumgebung“ auf Seite 510](#).

Die erste der folgenden Methoden, die einen Wert zurückgibt, legt die Standardsprache fest:

1. Überprüfen der SALANG-Umgebungsvariable
2. (Windows) Überprüfung der Registrierung während der Installation oder von *dblang.exe* gesetzt. Siehe [„Dienstprogramm für die Sprachauswahl \(dblang\)“ auf Seite 946](#).
3. Abfragen des Betriebssystems nach Sprachinformationen
4. Wenn keine Sprachinformationen definiert sind, wird Englisch als Standardwert verwendet.

## Siehe auch

- [„Dienstprogramm für die Sprachauswahl \(dblang\)“ auf Seite 946](#)
- [„Registrierungseinstellungen bei der Installation“ auf Seite 490](#)
- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

# SALOGDIR-Umgebungsvariable

Gibt den Speicherort der Datei *backup.syb* an.

## Syntax

**SALOGDIR**=*directory-name*

## Bemerkungen

Wenn die SALOGDIR-Umgebungsvariable gesetzt ist, wird angenommen, dass sie den Pfad für das Verzeichnis enthält, in das die Sicherungsverlaufsdatei, *backup.syb*, geschrieben werden kann. Die Datei wird jedes Mal aktualisiert, wenn Sie eine BACKUP- oder RESTORE-Anweisung ausführen.

Unter Windows wird die Datei *backup.syb* auf dem ersten beschreibbaren Speicherort der folgenden Liste erstellt:

1. In der SALOGDIR-Umgebungsvariablen.
2. *%ALLUSERSPROFILE%\SQL Anywhere 16*.
3. In das Stammverzeichnis des aktuellen Laufwerks.
4. In das aktuelle Verzeichnis.

Unter Windows CE wird die Datei *backup.syb* auf dem ersten beschreibbaren Speicherort der folgenden Liste erstellt:

1. In der SALOGDIR-Umgebungsvariablen.
2. In das Verzeichnis, in dem der Datenbankserver gestartet wurde.
3. In das Stammverzeichnis.
4. In das aktuelle Verzeichnis.

Unter Unix wird die Datei *backup.syb* auf dem ersten beschreibbaren Speicherort der folgenden Liste erstellt:

1. In der SALOGDIR-Umgebungsvariablen.
2. *\$HOME/.sqlanywhere16*.
3. In das aktuelle Verzeichnis.

#### Siehe auch

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## SATMP-Umgebungsvariable

Gibt den Speicherort von temporären Dateien an, die vom Datenbankserver und den SQL Anywhere-Befehlszeilen-Dienstprogrammen, die ein Verzeichnis für temporäre Dateien erfordern, verwendet werden.

#### Syntax

**SATMP**=*directory-name*

#### Bemerkungen

SQL Anywhere erstellt zwei Arten von temporären Dateien: dem Datenbankserver zugeordnete temporäre Dateien (auf allen Plattformen erstellt) und der Kommunikation zugeordnete temporäre Dateien (nur unter Unix für den Client und den Server erstellt).

Die SATMP-Umgebungsvariable gibt den Speicherort von temporären Dateien an, die vom Datenbankserver verwendet werden und von den SQL Anywhere-Befehlszeilen-Dienstprogrammen, die ein Verzeichnis für temporäre Dateien erfordern. Sie ist nützlich, wenn der Datenbankserver als Dienst ausgeführt wird, weil Sie mit ihrer Hilfe die temporäre Datei in einem Verzeichnis speichern können, auf das nicht von anderen Programmen zugegriffen werden kann.

Wenn der Speicherort der temporären Datei nicht beim Starten des Datenbankservers mit der Option -dt angegeben wird, überprüft der Datenbankserver den Wert der SATMP-Umgebungsvariable, um zu ermitteln, wo die temporäre Datei abgelegt werden soll. Wenn die SATMP-Umgebungsvariable nicht vorhanden ist, wird die erste vorhandene der Umgebungsvariablen TMP, TMPDIR und TEMP verwendet. Unter Windows wird das aktuelle Verzeichnis verwendet, wenn keine dieser Umgebungsvariablen existiert. Unter Unix wird */tmp* verwendet, wenn keine dieser Umgebungsvariablen existiert.

Unter Windows Mobile können Sie in der Registrierung angeben, welches Verzeichnis als temporäres Serververzeichnis verwendet werden soll. Hinweise zum Speicherort von temporären Dateien unter Windows Mobile finden Sie unter [„Registrierungseinstellungen unter Windows Mobile“ auf Seite 491](#).

Unter Unix müssen der Client und der Datenbankserver SATMP auf denselben Wert setzen, wenn sie sich über Shared Memory verbinden.

**Hinweis**

In SQL Anywhere Version 9 und früher ist die Umgebungsvariable ASTMP mit SATMP äquivalent. Wenn Sie Shared Memory zum Verbinden von Software der Versionen 9 und 10 verwenden, müssen Sie die Umgebungsvariablen SATMP und ASTMP so setzen, dass sie den(selben) Speicherort des temporären Verzeichnisses angeben.

Wenn Sie die Berechtigungen für temporäre Dateien einschränken möchten, die vom Datenbankserver oder Client unter Unix erstellt werden, müssen Sie diese Umgebungsvariable auf ein Verzeichnis setzen, das nicht in der folgenden Liste enthalten ist:

- `/tmp`
- `/tmp/.SQLAnywhere`
- Der Wert der TMP-Umgebungsvariable, falls gesetzt
- Der Wert der TMPDIR-Umgebungsvariable, falls gesetzt
- Der Wert der TEMP-Umgebungsvariable, falls gesetzt
- Eine Symbolverknüpfung, die auf eine der obenstehenden Verzeichnisse zeigt

Wenn SATMP auf ein nicht in der Liste oben aufgeführtes Verzeichnis gesetzt ist, durchsucht der Datenbankserver den angegebenen Verzeichnispfad aufwärts nach Verzeichnissen, die dem aktuellen Benutzer mit auf 770, 707 oder 700 gesetzten Berechtigungen gehören. Wenn die Berechtigungen nicht auf einen dieser Werte gesetzt sind, werden Dateien mit Berechtigungen erstellt, die auf 777 gesetzt sind. Bei jedem gefundenen Verzeichnis entfernt der Datenbankserver die entsprechenden Berechtigungen (other, group bzw. other+group) aus der Berechtigungsmaske, die zum Erstellen von temporären Dateien verwendet wird.

**Vorsicht**

Das Setzen von SATMP auf ein nicht in der Liste oben aufgeführtes Verzeichnis wirkt sich möglicherweise auf die Fähigkeit von Benutzern aus, verschiedene Unix-Konten zu verwenden, um Shared Memory-Verbindungen mit dem Datenbankserver herzustellen.

Hinweise zur Sicherung von Shared Memory-Verbindungen unter Unix finden Sie unter [Setzen Sie die SATMP-Umgebungsvariable auf ein eindeutiges Verzeichnis \(Unix\) auf Seite 1407](#).

**Siehe auch**

- „Datenbankserveroption -dt“ auf Seite 228
- „Umgebungsvariablen TMP, TMPDIR und TEMP“ auf Seite 481
- Umgebungsvariablen unter Windows setzen auf Seite 467
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467
- „Tipp: Verschiedene Dateien auf verschiedene Geräte platzieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Sicherstellen von genügend Festplattenspeicher für die temporäre Datei“ auf Seite 1110
- „sa\_disk\_free\_space-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## SHLIB\_PATH-Umgebungsvariable [HP-UX]

Gibt die Verzeichnisse an, in denen zur Zeit der Ausführung nach den Bibliotheken gesucht wird, die für SQL Anywhere-Anwendungen unter HP-UX erforderlich sind.

**Syntax**

**SHLIB\_PATH**=*path-list*

**Standardwert**

- */opt/sqlanywhere16/lib32* (32-Bit-Plattformen)
- */opt/sqlanywhere16/lib64* (64-Bit-Plattformen)

**Bemerkungen**

Die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, sind Skripten, die diese oder andere Umgebungsvariable erstellen oder ändern.

**Siehe auch**

- „DYLD\_LIBRARY\_PATH-Umgebungsvariable [Mac OS X]“ auf Seite 469
- „LD\_LIBRARY\_PATH-Umgebungsvariable [Linux und Solaris]“ auf Seite 469
- „LIBPATH-Umgebungsvariable [IBM AIX]“ auf Seite 470
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## SQLANY16-Umgebungsvariable

Gibt den Speicherort des Verzeichnisses an, das SQL Anywhere 16 enthält.

**Syntax**

**SQLANY16**=*directory-name*

**Standardwert**

Betriebssystem	Speicherort
Windows	<i>C:\Program Files\SQL Anywhere 16</i>

Betriebssystem	Speicherort
IBM AIX	<i>/usr/lpp/sqlanywhere16</i>
Mac OS X	<i>/Applications/SQLAnywhere16/System</i>
Andere Unix-Betriebssysteme	<i>/opt/sqlanywhere16</i>

**Bemerkungen**

Diese Umgebungsvariable sollte aus mehreren Gründen angegeben werden. So fragen z.B. Beispielskripten die Umgebungsvariable ab, um SQL Anywhere-Anwendungen zu finden.

Unter Windows erstellt das Installationsprogramm die SQLANY16-Umgebungsvariable (die in der Windows-Registrierung gespeichert wird).

Unter Unix sind die Dateien *sa\_config.sh* und *sa\_config.csh*, die vom Installationsprogramm erstellt werden, Skripten, die diese oder andere Umgebungsvariable erstellen oder ändern.

**Siehe auch**

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

# SQLANYSAMP16-Umgebungsvariable

Gibt den Speicherort des SQL Anywhere-Beispielverzeichnisses an.

**Syntax**

**SQLANYSAMP16**=*directory-name*

**Standardwert**

Betriebssystem	Standardspeicherort
Windows XP	<i>C:\Dokumente und Einstellungen\Alle Benutzer\Dokumente\SQL Anywhere 16\Samples<sup>1</sup></i>
Windows Vista und höher	<i>C:\Benutzer\Öffentlich\Dokumente\SQL Anywhere 16\Samples</i>
Unix (Einzelbenutzerinstallationen)	<i>\$SQLANY16/samples</i>

<sup>1</sup> Wenn Sie im Windows-Explorer auf das SQL Anywhere-Beispielverzeichnis zugreifen, ist der Speicherort *C:\Dokumente und Einstellungen\Alle Benutzer\Gemeinsame Dokumente\SQL Anywhere 16\Samples*. Wenn Sie jedoch von einer Eingabeaufforderung aus auf das SQL Anywhere-Beispielverzeichnis zugreifen, ist der Pfad *C:\Dokumente und Einstellungen\Alle Benutzer\Dokumente\SQL Anywhere 16\Samples*.

**Bemerkungen**

Unter Windows erstellt das Installationsprogramm die SQLANYSAMP16-Umgebungsvariable (die in der Windows-Registrierung gespeichert wird). Wenn Sie ein Windows-Explorer-Fenster in diesem Verzeichnis öffnen möchten, klicken Sie auf **Start » Programme » SQL Anywhere 16 » Beispielanwendungen und Projekte**.

Unter Unix, einschließlich Mac OS X, kann das Skript *sample\_config* verwendet werden, um eine benutzerspezifische Kopie der SQL Anywhere-Beispiele anzulegen. Sie müssen dieses Skript ausführen, um den Speicherort der SQLANYSAMP16-Umgebungsvariablen im Betriebssystem festzulegen.

Unter Unix setzt das Installationsprogramm die SQLANYSAMP16-Umgebungsvariable in den Skripten *sa\_config* und *sample\_config*. Diese Option ist bei einer Mehrbenutzer-Installation nützlich. Bei Einbenutzer-Installationen setzt das sa\_config-Skript die SQLANYSAMP16-Variable auf *\$\$SQLANY16/samples*.

**Siehe auch**

- „SQLANY16-Umgebungsvariable“ auf Seite 477
- Umgebungsvariablen unter Windows setzen auf Seite 467
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## SQLCONNECT-Umgebungsvariable

Gibt zusätzliche Verbindungsparameter an, die bei der Verbindungsherstellung zum Datenbankserver verwendet werden.

**Syntax**

**SQLCONNECT**=*parameter=value*; ...

**Bemerkungen**

Diese Zeichenfolge ist eine Liste von durch Semikola getrennten Parametereinstellungen in der Form *Parameter=Wert*.

Von der SQLCONNECT-Umgebungsvariable angegebene Verbindungsparameter werden nicht verwendet, wenn sie bereits in der Verbindungszeichenfolge angegeben wurden.

Hinweise zu den unterstützten Verbindungsparametern finden Sie unter „[Verbindungsparameter](#)“ auf Seite 337.

**Vorsicht**

Da das Kennwort ein normaler Text ist, stellt es ein Sicherheitsrisiko dar, wenn Sie es in die Umgebungsvariable SQLCONNECT setzen.

**Siehe auch**

- Umgebungsvariablen unter Windows setzen auf Seite 467
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467

## SQLPATH-Umgebungsvariable

Gibt den Speicherort von SQL-Skriptdateien und Hilfedateien an.

### Syntax

**SQLPATH**=*path-list*

### Bemerkungen

Interactive SQL durchsucht die in SQLPATH angegebenen Verzeichnisse nach Skript- und Hilfedateien, bevor der Systempfad durchsucht wird.

### Siehe auch

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## SQLREMOTE-Umgebungsvariable

Gibt Unterverzeichnisse an, die Adressen für die FILE-Meldungsverknüpfung in SQL Remote sind.

### Syntax

**SQLREMOTE**=*path*

### Bemerkungen

Adressen für die FILE-Meldungsverknüpfung in SQL Remote sind Unterverzeichnisse der SQLREMOTE-Umgebungsvariable. Diese Umgebungsvariable sollte ein gemeinsam genutztes Verzeichnis angeben.

Unter Windows-Betriebssystemen (außer Windows Mobile) kann als Alternative zum Einstellen der SQLREMOTE-Umgebungsvariable der Registrierungseintrag *SQL Remote\Directory* auf das entsprechende Verzeichnis gesetzt werden.

### Siehe auch

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## SYBASE-Umgebungsvariable

Gibt das Stammverzeichnis für die Installation bestimmter Sybase-Anwendungen an, darunter Adaptive Server Enterprise, Sybase Open Client, Sybase Open Server und Dienstprogramme wie DSEdit.

### Syntax

**SYBASE**=*directory-name*

### Bemerkungen

Sie müssen diese Umgebungsvariable nur setzen, wenn Sie andere Sybase-Anwendungen verwenden.

**Siehe auch**

- [Umgebungsvariablen unter Windows setzen auf Seite 467](#)
- [„Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467](#)

## Umgebungsvariablen TMP, TMPDIR und TEMP

Gibt den Speicherort von temporären Dateien in SQL Anywhere an.

**Syntax**

**TMP**=*path*

**TMPDIR**=*path*

**TEMP**=*path*

**Bemerkungen**

SQL Anywhere-Software erstellt temporäre Dateien für unterschiedliche Vorgänge, einschließlich einer temporären Datei, die beim Starten des Datenbankservers erstellt und beim Stoppen des Datenbankservers gelöscht wird. Wie schon der Name sagt, wird die temporäre Datei verwendet, um temporäre Daten zu speichern, während der Datenbankserver läuft. In der temporären Datei werden keine Daten gespeichert, die sitzungübergreifend erhalten bleiben müssen.

Temporäre Dateien werden in dem Verzeichnis gehalten, das von einer der Umgebungsvariablen TMP, TMPDIR oder TEMP angegeben wird. Wenn mehr als eine Umgebungsvariable angegeben wird, wird die erste von TMP, TMPDIR und TEMP verwendet. Sie können die SATMP-Umgebungsvariable auch so setzen, dass sie den Speicherort von temporären Dateien angibt, die vom Datenbankserver verwendet werden und von den SQL Anywhere-Befehlszeilen-Dienstprogrammen, die ein Verzeichnis für temporäre Dateien erfordern.

Der Speicherort der vom Datenbankserver verwendeten temporären Datei kann beim Starten des Datenbankservers mit der Serveroption -dt angegeben werden. Falls Sie beim Starten des Datenbankservers keinen Speicherort für die temporäre Datei angeben, prüft SQL Anywhere die folgenden Umgebungsvariablen, in dieser Reihenfolge: SATMP, TMP, TMPDIR, TEMP. Wenn keine Umgebungsvariable definiert ist, platziert SQL Anywhere die temporäre Datei unter UNIX in das */tmp*-Verzeichnis, und unter Windows in das aktuelle Verzeichnis.

Unter Unix wird das temporäre Verzeichnis zur Herstellung einer Shared Memory-Verbindung verwendet. Unter Windows Mobile können Sie die Registrierung verwenden, um anzugeben, welches Verzeichnis als temporäres Serververzeichnis verwendet werden soll. Weitere Hinweise zum Festlegen des Wertes für das temporäre Verzeichnis finden Sie unter [„Registrierungseinstellungen unter Windows Mobile“ auf Seite 491](#).

#### Hinweis

**Verbindungen über gemeinsam genutzten Speicher unter Unix mit älterer Software verwenden** In SQL Anywhere Version 9 und früher ist die Umgebungsvariable ASTMP mit SATMP äquivalent. Wenn Sie Shared Memory zum Verbinden von Software der Versionen 9 und 12 verwenden, müssen Sie die Umgebungsvariablen SATMP und ASTMP so setzen, dass sie den Speicherort der temporären Datei angeben.

#### Siehe auch

- „Datenbankserveroption -dt “ auf Seite 228
- „SATMP-Umgebungsvariable“ auf Seite 475
- Umgebungsvariablen unter Windows setzen auf Seite 467
- „Unix- und Mac OS X-Umgebungsvariablen“ auf Seite 467
- „Tipp: Verschiedene Dateien auf verschiedene Geräte platzieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Sicherstellen von genügend Festplattenspeicher für die temporäre Datei“ auf Seite 1110
- „Datenbankdateien“ [*SQL Anywhere 16 - Einführung*]

## Dateispeicherorte und Installationseinstellungen

Wenn Sie SQL Anywhere installieren, werden mehrere Verzeichnisse angelegt. Einige Dateien in diesen Verzeichnissen sind für die Programmausführung erforderlich, andere nicht.

Die Software von SQL Anywhere wird in einem eigenen Installationsverzeichnis installiert, gleichgültig ob Sie das Softwarepaket getrennt oder gemeinsam mit anderen Paketen erworben haben. Die SQLANY16-Umgebungsvariable gibt den Speicherort des Installationsverzeichnisses an.

### SQL Anywhere-Installationsverzeichnis

Das Installationsverzeichnis von SQL Anywhere enthält unter anderem folgende Elemente:

- **Readme-Datei** Eine Readme-Datei enthält aktuelle Informationen.

Bei anderen Plattformen als Windows Mobile enthält das Installationsverzeichnis mehrere Unterverzeichnisse:

- **Programmverzeichnisse** Es ist ein eigenes Verzeichnis für jede Betriebssystemplattform vorhanden, in dem Konfigurationsdateien und Dateien für die kontextsensitive Hilfe gespeichert sind.

Unter Windows mit Ausnahme von Windows Mobile werden diese Dateien im Verzeichnis *bin32* oder *bin64* installiert. Wenn Sie Unix verwenden, werden sie in den Verzeichnissen *bin32* bzw. *bin64* und *lib32* bzw. *lib64* installiert.

Es werden nur die Verzeichnisse installiert, die für Ihre Betriebssystemversion erforderlich sind.

- **Java-Verzeichnis** JAR-Dateien werden in diesem Verzeichnis gespeichert.

- **Verzeichnis für Skripten** Das Verzeichnis für Skripten enthält SQL-Skripten, die von den Dienstprogrammen für die Datenbankverwaltung und für Beispiele benutzt werden.
- **SDK\Include-Verzeichnis** Das Verzeichnis `\SDK\Include` enthält Header-Dateien für die Entwicklung von C/C++-Anwendungen für SQL Anywhere. Unter Unix heißt dieses Verzeichnis *include*.

### Windows Mobile-Dateispeicherorte

Siehe „SQL Anywhere-Installation auf einem Windows Mobile-Gerät“ auf Seite 430.

### Unix-Dateistandorte

Die Sprachenressourcen werden im Verzeichnis *res* installiert und die Shared Objects im Verzeichnis *lib32* bzw. *lib64*.

### Beispielverzeichnis

Wenn Sie SQL Anywhere installieren, können Sie wählen, in welchem Verzeichnis die Beispiele installiert werden. Das Installationsprogramm erstellt die SQLANYSAMP16-Umgebungsvariable, um diesen Speicherort zu kennzeichnen.

### Siehe auch

- „SQLANYSAMP16-Umgebungsvariable“ auf Seite 478
- „SQLANY16-Umgebungsvariable“ auf Seite 477

## Wie SQL Anywhere die Dateien findet

Die Clientbibliothek und der Datenbankserver müssen Dateien aus zwei Gründen finden können:

- DLLs und Initialisierungsdateien sind erforderlich, um SQL Anywhere auszuführen. Wenn eine falsche DLL gefunden wird, kann es zur Anzeige von Versionsfehlern kommen.
- Einige Dateien werden in SQL-Anweisungen definiert und müssen zur Laufzeit gefunden werden, wie z.B. INSTALL JAVA oder LOAD TABLE.

Beispiele für SQL-Anweisungen, die Dateinamen benutzen:

- **INSTALL JAVA-Anweisung** Der Name der Datei, in der die Java-Klassen untergebracht sind
- **LOAD TABLE- und UNLOAD TABLE-Anweisung** Der Name der Datei, aus der Daten geladen werden sollen oder in die die Daten eingelesen werden sollen
- **CREATE DATABASE-Anweisung** Ein Dateiname ist für diese Anweisung und ähnliche Anweisungen erforderlich, die Dateien erstellen können

In einigen Fällen benutzt SQL Anywhere einen einfachen Algorithmus, um den Speicherort von Dateien zu ermitteln. In anderen Fällen wird eine ausführlichere Suche durchgeführt.

## Einfache Dateisuche

In vielen SQL-Anweisungen (wie LOAD TABLE oder CREATE DATABASE) wird der Dateiname als relativ zum aktuellen Arbeitsverzeichnis des Datenbankservers interpretiert.

Wenn ein Datenbankserver gestartet und ein Datenbankdateiname (DatabaseFile (DBF)-Parameter) übergeben wird, kann der Pfad als relativ zum aktuellen Arbeitsverzeichnis interpretiert werden.

## Extensive Dateisuche unter Windows

Unter Windows können SQL Anywhere-Programme, darunter der Datenbankserver und die Administrationsdienstprogramme, eine ausführliche Suche nach erforderlichen Dateien durchführen, wie DLLs oder gemeinsam genutzte Bibliotheken. In diesen Fällen suchen SQL Anywhere-Programme nach Dateien in der nachstehenden Reihenfolge:

1. Das Verzeichnis des aktuellen Moduls (das Verzeichnis, in dem sich die derzeit ausgeführte Programmdatei oder Bibliotheksdatei befindet).
2. Das Verzeichnis der aktuellen Programmdatei (das Verzeichnis, in dem sich die derzeit ausgeführte Programmdatei befindet).
3. Der SQL Anywhere-Installationspfad ist ein einzelnes Verzeichnis, das durch die %SQLANY16%-Umgebungsvariable festgelegt wird, wenn diese definiert ist.
4. Der vollständige angegebene Pfad. Wenn kein Pfad angegeben ist, das aktuelle Arbeitsverzeichnis.
5. Das Verzeichnis %APPDATA%\SQL Anywhere 16.
6. Das Verzeichnis %ALLUSERSPROFILE%\SQL Anywhere 16.
7. Location-Registrierungseintrag.
8. Systemspezifische Verzeichnisse. Dazu gehören Verzeichnisse, in denen sich gemeinsam genutzte Dateien des Betriebssystems befinden, wie z.B. das Verzeichnis *Windows* und das Verzeichnis *Windows\system32* bei Windows-Betriebssystemen.
9. Die PATH-Verzeichnisse. Verzeichnisse im Systempfad und im Benutzerpfad werden durchsucht.

**Hinweis**

Unter Windows durchsucht SQL Anywhere die folgenden Pfade relativ zur vorhergehenden Liste:

- a. .
- b. ..
- c. .\bin32 und ..\bin32 (nur 32-Bit-Programme)
- d. .\bin64 und ..\bin64 (nur 64-Bit-Programme)
- e. .\java (für Java-Dateien)
- f. ..\java (für Java-Dateien)
- g. .\Scripts (für SQL-Skriptdateien)
- h. ..\Scripts (für SQL-Skriptdateien)

## Extensive Dateisuche unter Windows Mobile

Unter Windows Mobile können SQL Anywhere-Programme, darunter der Datenbankserver und die Administrationsdienstprogramme, eine ausführliche Suche nach erforderlichen Dateien durchführen, wie DLLs oder gemeinsam genutzte Bibliotheken. In diesen Fällen suchen SQL Anywhere-Programme nach Dateien in der nachstehenden Reihenfolge:

1. Verzeichnis des Moduls (Verzeichnis, in dem die Programmdatei oder Bibliotheksdatei gespeichert ist).
2. Verzeichnis der Programmdatei (Verzeichnis, in dem die Programmdatei oder Bibliothek gespeichert ist).
3. Der vollständige angegebene Pfad.
4. Location-Registrierungseintrag.
5. Systemspezifische Verzeichnisse. Dies umfasst Verzeichnisse, in denen Betriebssystemdateien gespeichert sind, wie z.B. *Windows*.

**Hinweis**

Unter Windows Mobile durchsucht SQL Anywhere die folgenden Pfade relativ zur vorhergehenden Liste:

- a. .
- b. ..
- c. .\bin32
- d. ..\bin32
- e. .\java (für Java-Dateien)
- f. ..\java (für Java-Dateien)
- g. .\Scripts (für SQL-Skriptdateien)
- h. ..\Scripts (für SQL-Skriptdateien)

## Extensive Dateisuche unter Unix

Unter Unix können SQL Anywhere-Programme, darunter der Datenbankserver und die Administrationsdienstprogramme, eine ausführliche Suche nach erforderlichen Dateien durchführen, wie DLLs oder gemeinsam genutzte Bibliotheken. In diesen Fällen suchen SQL Anywhere-Programme nach Dateien in der nachstehenden Reihenfolge:

1. Programmpfad (wenn er ermittelt werden kann).
2. Der SQL Anywhere-Installationspfad ist ein einzelnes Verzeichnis, das durch die \$SQLANY16-Umgebungsvariable festgelegt wird, wenn diese definiert ist.
3. Kein Pfad (das aktuelle Arbeitsverzeichnis).
4. Das Verzeichnis *HOME/.sqlanywhere16*.
5. Die PATH-Umgebungsvariable
6. die LIBPATH-Umgebungsvariablen:
  - LD\_LIBRARY\_PATH unter Linux und Solaris
  - LD\_LIBRARY\_PATH und SHLIB\_PATH auf HP-UX
  - LIBPATH unter IBM AIX
  - DYLD\_LIBRARY\_PATH unter Mac OS X

**Hinweis**

Unter Unix durchsucht SQL Anywhere die folgenden Pfade relativ zur vorhergehenden Liste:

1. .
2. ..
3. *./bin32* und *../bin32* (nur 32-Bit-Programme)
4. *./bin64* und *../bin64* (nur 64-Bit-Programme)
5. *./lib32* und *../lib32* (Bibliotheksdateien nur für 32-Bit-Programme)
6. *./lib64* und *../lib64* (Bibliotheksdateien nur für 64-Bit-Programme)
7. *./java* (für Java-Dateien)
8. *../java* (für Java-Dateien)
9. *./Scripts* (für SQL-Skriptdateien)
10. *../Scripts* (für SQL-Skriptdateien)
11. *./res* (für *.res*-Dateien)
12. *../res* (für *.res*-Dateien)
13. *./tix* (für *.tix*-Dateien)
14. *../tix* (für *.tix*-Dateien)

## Registrierung und INI-Dateien

Unter Windows-Betriebssystemen (außer Windows Mobile) verwendet SQL Anywhere verschiedene Registrierungseinstellungen. Unter Unix werden diese Einstellungen in Initialisierungsdateien gespeichert.

Diese Einstellungen werden von der Softwareinstallation vorgenommen, und im Normalbetrieb wird es sich nicht als nötig erweisen, auf die Registrierung zuzugreifen. Die Einstellungen werden hier für jene Benutzer festgehalten, die Änderungen in ihrer Betriebsumgebung durchführen müssen.

Der Inhalt der *.ini*-Dateien, die von SQL Anywhere verwendet werden, können mit einfacher Verschlüsselung unter Verwendung des Dienstprogramms zum Verschleiern von Dateien verschleiert werden.

**Vorsicht**

Unter Unix dürfen Sie keine einfache Verschlüsselung der Systeminformationsdatei (standardmäßig *.odbc.ini* genannt) mit dem Dienstprogramm zum Verschleiern von Dateien (dbfhide) hinzufügen, außer Sie verwenden ausschließlich SQL Anywhere-Datenquellen. Wenn Sie vorhaben, andere Datenquellen (wie z.B. für die MobiLink-Synchronisation) zu verwenden, kann das Verbergen des Inhalts der Systeminformationsdatei möglicherweise dazu führen, dass andere Treiber nicht richtig funktionieren.

**Siehe auch**

- [„Inhalte von .ini-Dateien verbergen“ auf Seite 489](#)

## Current User- und Local Machine-Einstellungen

Einige Betriebssysteme haben zwei Ebenen von Systemeinstellungen. Einige Einstellungen gelten nur für einen bestimmten Benutzer und werden nur benutzt, wenn dieser Benutzer angemeldet ist. Diese Einstellungen werden als **Current User** (aktueller Benutzer)-Einstellungen bezeichnet. Einige Einstellungen gelten global für den Computer und stehen allen Benutzern zur Verfügung. Sie werden als **Local Machine**-Einstellungen bezeichnet. Sie benötigen die Administratorberechtigung auf Ihrem Computer, um Änderungen in den Einstellungen für das lokale System vorzunehmen.

SQL Anywhere lässt Einstellungen sowohl für "Current User" als auch für "Local Machine" zu. Unter Windows XP werden diese beispielsweise in den Schlüsseln *HKEY\_CURRENT\_USER* bzw. *HKEY\_LOCAL\_MACHINE* registriert.

### "Current User" hat Vorrang

Wenn eine Einstellung in der "Current User"- und der "Local Machine"-Registrierung erfolgt, hat die Einstellung für den aktuellen Benutzer Vorrang gegenüber der Einstellung für das lokale System.

### "Local Machine"-Einstellungen erforderlich

Wenn Sie ein SQL Anywhere-Programm als **Dienst** unter Windows ausführen, müssen Sie sicherstellen, dass die Einstellungen auf der Ebene "Local Machine" vorgenommen werden.

Die Dienste können auf einem bestimmten Konto weiterlaufen, wenn Sie einen Benutzer abmelden, solange Sie den Computer nicht voll herunterfahren. Sie können von einzelnen Kontos unabhängig sein und müssen daher Zugriff auf die Einstellungen für den lokalen Computer haben.

Neben den SQL Anywhere-Programmen laufen auch einige Webserver als Dienste. Sie müssen die Einstellungen auf dem lokalen Computer für Apache oder Microsoft IIS vornehmen, um mit einem solchen Webserver arbeiten zu können.

Im Allgemeinen wird die Verwendung von "Local Machine"-Einstellungen empfohlen.

## Inhalte von *.ini*-Dateien verbergen

Um Kennwörter oder andere Informationen in einer *.ini*-Datei zu schützen, können Sie den Inhalt der Datei mithilfe einfacher Verschlüsselung und des Dienstprogramms zum Verschleiern von Dateien verbergen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

SQL Anywhere erwartet, dass eine *.ini*-Datei einen bestimmten Namen hat. Wenn Sie eine Datei, deren Name wichtig ist (z.B. *saldap.ini*), mit einfacher Verschlüsselung versehen möchten, müssen Sie eine Kopie der ursprünglichen Datei unter einem anderen Namen speichern. Wenn Sie keine Kopie der ursprünglichen Datei speichern, können Sie den Inhalt der Datei nach dem Verschleiern nicht mehr ändern.

#### Vorsicht

Unter Unix dürfen Sie keine einfache Verschlüsselung der Systeminformationsdatei (standardmäßig *.odbc.ini* genannt) mit dem Dienstprogramm zum Verschleiern von Dateien (*dbfhide*) hinzufügen, außer Sie verwenden ausschließlich SQL Anywhere-Datenquellen. Wenn Sie vorhaben, andere Datenquellen (wie z.B. für die MobiLink-Synchronisation) zu verwenden, kann das Verbergen des Inhalts der Systeminformationsdatei möglicherweise dazu führen, dass andere Treiber nicht richtig funktionieren.

### Aufgabe

1. Speichern Sie die Datei unter einem anderen Namen.

```
rename saldap.ini saldap.ini.org
```

2. Verschleiern Sie die Datei mit dem Dienstprogramm zum Verschleiern von Dateien, wobei Sie der verborgenen Datei den erforderlichen Dateinamen zuordnen.

```
dbfhide saldap.ini.org saldap.ini
```

3. Schützen Sie die *saldap.ini.org*-Datei unter Verwendung des Dateisystem- oder Betriebssystem-Schutzes, oder speichern Sie die Datei an einem sicheren Standort.

Um Änderungen an der *saldap.ini*-Datei vorzunehmen, bearbeiten Sie die *saldap.ini.org*-Datei und wiederholen Schritt 2.

### Ergebnisse

Der Inhalt der *.ini*-Datei wird verborgen.

### Siehe auch

- „Dienstprogramm zum Verschleiern von Dateien (*dbfhide*)“ auf Seite 922

## Aufbau der Registrierung

Unter Windows (außer Windows Mobile) können Sie die Registrierung direkt über den Registrierungseditor aufrufen. Die SQL Anywhere-Registrierungseinträge befinden sich in den Schlüsseln *HKEY\_CURRENT\_USER* oder *HKEY\_LOCAL\_MACHINE* an folgenden Standorten:

```
Software
  Sybase
    SQL Anywhere
      16.0
    Sybase Central
      16.0
```

### Vorsicht

Sie nehmen Änderungen an Ihrer Registrierung auf eigene Gefahr vor. Bevor Sie die Registrierung ändern, sollten Sie eine Sicherungskopie Ihres Systems erstellen.

## Registrierungseinstellungen bei der Installation

### Vorsicht

Um die Robustheit von Systemen mit bestimmten Intel-Speichertreibern bei Stromausfall zu verbessern, müssen bestimmte Registrierungseinträge angegeben werden. Wenn dieser Parameter nicht festgelegt wird, kann Datenverlust eintreten und bei Stromausfall können Datenbanken beschädigt werden. Siehe [„Robustheit bei Intel-Speichertreibern verbessern“ \[SQL Anywhere Server - Programmierung\]](#).

Unter Windows speichert das Installationsprogramm folgende Einstellungen in der Registrierung *HKEY\_LOCAL\_MACHINE\Software\Sybase*. Die nachstehende Liste zeigt einige Registrierungseinträge:

- **SQL Anywhere\16.0\Location** Dieser Eintrag enthält den Speicherort des Installationsverzeichnis für die SQL Anywhere-Software. Zum Beispiel:

```
Location "C:\Program Files\SQL Anywhere 16"
```

- **SQL Anywhere\16.0\Samples Location** Dieser Eintrag enthält den Speicherort des Installationsverzeichnis für Beispielprogramme. Zum Beispiel:

```
Samples Location "C:\Documents and Settings\All Users\Documents\SQL Anywhere 16\Samples\"
```

- **SQL Anywhere\16.0\Online Resources** Dieser Eintrag enthält den Standort der Online-Ressourcen-Dokumentation. Zum Beispiel:

```
Online Resources "C:\Program Files\SQL Anywhere 16\support\OnlineResources.html"
```

- **SQL Anywhere\16.0\Language** Dieser Eintrag enthält einen Zwei-Buchstabencode, der die aktuelle Sprache für Systemmeldungen und Fehlermeldungen angibt. Zum Beispiel:

```
Language "EN"
```

Die Sprache wird anhand der während der Installation angegebenen Sprachauswahl eingestellt. Siehe [„Sprache der Sprachumgebung“ auf Seite 510](#).

- **Sybase Central\16.0\Language** Dieser Eintrag enthält einen Zwei-Buchstabencode, der die aktuelle Sprache für Systemmeldungen und Fehlermeldungen angibt. Zum Beispiel:

Language "EN"

Dieser Eintrag wird von Sybase Central verwendet. Die Sprache wird anhand der während der Installation angegebenen Sprachauswahl eingestellt. Siehe „[Sprache der Sprachumgebung](#)“ auf Seite 510.

## Registrierungseinstellungen unter Windows Mobile

Unter Windows Mobile können Sie das Verzeichnis angeben, das vom Server als Temporärverzeichnis verwendet werden soll. Setzen Sie hierzu in der Registrierung den folgenden Wert:

*HKEY\_CURRENT\_USER\Software\Sybase\SQL Anywhere\16.0\TempVerzeichnis*

Der Wert von *TempFolder* ist der Name des zu nutzenden temporären Verzeichnisses. Der Server führt eine der folgenden Aktionen durch:

- Das angegebene Verzeichnis wird verwendet, sofern es existiert.
- Es wird der Versuch gestartet, dieses angegebene Verzeichnis zu erstellen, wenn es selbst nicht, aber das übergeordnete Verzeichnis existiert.

Falls dieses Verzeichnis nicht vorhanden ist und nicht erstellt werden kann, führt der Datenbankserver eine der beiden folgenden Aktionen durch:

- Das Verzeichnis *\Temp* wird verwendet, sofern es vorhanden ist.
- Es wird versucht, das Verzeichnis *\Temp* zu erstellen, sollte es noch nicht vorhanden sein.

Falls das Verzeichnis *\Temp* nicht existiert und nicht erstellt werden kann, verwendet der Server das aktuelle Verzeichnis.

## Internationale Sprachen und Zeichensätze

Internationalisierung bezieht sich auf die Fähigkeit der Software, verschiedene Sprachen und ihre entsprechenden Zeichensätze unabhängig von der Sprache, in der die Software ausgeführt wird, oder vom Betriebssystem, auf dem die Software läuft, zu handhaben. SQL Anywhere hat volle Internationalisierungsfähigkeiten. Die folgenden Features betreffen die am häufigsten angeforderten und verwendeten Fähigkeiten:

- **Unicode-Unterstützung** SQL Anywhere unterstützt Unicode folgendermaßen:
  - Client-Unterstützung für UTF-16 in SQL Anywhere Clientbibliotheken für ODBC, OLE DB, ADO.NET und JDBC
  - NCHAR-Datentypen zum Speichern von Unicode-Zeichendaten in UTF-8

- CHAR-Datentypen können UTF-8-Kodierung verwenden
- **Codepages und Zeichensätze** Der SQL Anywhere-Datenbankserver und dazugehörige Tools unterstützen Windows (ANSI/ISO)-, UTF-8- und Unix-Codepages und Zeichensätze.
- **Kollationen** SQL Anywhere unterstützt zwei Kollationsalgorithmen: den SQL Anywhere-Kollationsalgorithmus (SACA = SQL Anywhere Collation Algorithm) und den Unicode-Kollationsalgorithmus (UCA = Unicode Collation Algorithm) mithilfe von ICU (International Components for Unicode).

Weitere Hinweise zu ICU finden Sie unter [„Was ist ICU und wann wird es benötigt?“](#) auf Seite 495.

SACA bietet eine schnelle, kompakte und vernünftige Sortierung auf Kosten der linguistischen Korrektheit. UCA bietet linguistische Korrektheit, wenn auch mit etwas erhöhten Speicheranforderungen und längerer Ausführungszeit. Siehe [„Kollationen“](#) auf Seite 514.

Für erweiterte Sortier- und Vergleichsfähigkeiten stellt SQL Anywhere überdies die SORTKEY- und COMPARE-Funktionen zur Verfügung. Diese Funktionen bieten erweiterte linguistische Sortierfähigkeiten, wie z.B. die in einem Wörterbuch oder Telefonbuch verwendete Reihenfolge. Falls erforderlich, sind Sortierungen und Vergleiche ohne Berücksichtigung der Groß-/Kleinschreibung oder von Akzenten verfügbar. Siehe [„SORTKEY-Funktion \[Zeichenfolge\]“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*] und [„COMPARE-Funktion \[Zeichenfolge\]“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*].

SQL Anywhere enthält auch Designfeatures zur automatischen Verwendung einer auf SORTKEY basierenden Sortierung von Zeichenspalten. Die sort\_collation-Datenbankoption gibt die Sortierreihenfolge an, die verwendet wird, wenn ein ORDER BY für eine Zeichenspalte angegeben ist. Berechnete Spalten können auch verwendet werden, um Sortierschlüssel für Zeichenspalten zu speichern, damit sie nicht jedesmal berechnet werden müssen, wenn ORDER BY angegeben ist. Siehe [„sort\\_collation-Option“](#) auf Seite 670.

- **Zeichensatzkonvertierung** SQL Anywhere konvertiert Daten zwischen der Zeichensatzkodierung auf Ihren Server- und Clientsystemen, wodurch die Integrität Ihrer Daten selbst in Umgebungen mit gemischten Zeichensätzen gewährleistet wird. Siehe [„Zeichensatzkonvertierung“](#) auf Seite 502.
- **Bezeichner** SQL Anywhere unterstützt die Verwendung von Bezeichnern, ohne dass Anführungszeichen erforderlich sind, bei einem Großteil der Einbyte- und Mehrbyte-Zeichen. Ausnahmen sind üblicherweise auf Leerstellen und Satzzeichensymbole beschränkt.
- **Währung** Währungssymbole, einschließlich des Euro-Symbols, werden bei Sortierungen unterstützt. SQL Anywhere bietet keine Unterstützung für Währungsformatierung.
- **Datums- und Uhrzeitformate** SQL Anywhere unterstützt den Gregorianischen Kalender und stellt mehrere Formate für Datums- und Uhrzeit-Zeichenfolgen zur Verfügung. Benutzerdefinierte Formatierungen können unter Verwendung der Datenbankoptionen date\_format, time\_format und timestamp\_format durchgeführt werden. Die Optionen date\_format und timestamp\_format verwenden standardmäßig ein ISO-kompatibles Format für das Datum, YYYY-MM-DD. SQL Anywhere stellt

die CONVERT-Funktion zur Verfügung, die die Ausgabeformatierung von Datums- und Uhrzeitangaben in einer Vielzahl von populären Formaten ermöglicht. Siehe:

- „date\_format-Option“ auf Seite 599
- „time\_format-Option“ auf Seite 690
- „timestamp\_format-Option“ auf Seite 692
- „CONVERT-Funktion [Datentypkonvertierung]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

#### Siehe auch

- „Hinweise zur Kollation“ auf Seite 522
- „Empfohlene Zeichensätze und Kollationen“ auf Seite 529

## Lokalisierte Versionen von SQL Anywhere

Lokalisierung bezieht sich auf die linguistische und kulturelle Adaption eines Produkts an eine Ziel-Sprachumgebung, die üblicherweise eine Kombination aus Sprache und Land/Region ist. Eine Lokalisierung wirkt sich auf viele Komponenten aus, wie Verpackung, Installation, Dokumentation, Software-Benutzerschnittstelle und Fehler- bzw. Warnmeldungen sowie informative Meldungen.

SQL Anywhere-Software wird in fünf Sprachen bereitgestellt:

- Englisch
- Französisch
- Deutsch
- Japanisch
- Vereinfachtes Chinesisch

Die Sprachauswahl wird während der Installation festgelegt.

Übersetzte Versionen der Dokumentation stehen in den Sprachen Englisch, Deutsch, Japanisch und Chinesisch zur Verfügung.

Unter Windows ermöglichen es die Einträge im Menü **Start**, die Software zwischen der installierten Sprache und Englisch neu zu konfigurieren. Mit dem Dienstprogramm für die Sprachauswahl (dblang) können Sie die Software in einer der verfügbaren Sprachen neu konfigurieren, einschließlich der zusätzlichen Deployment-Sprachen. Siehe:

- „Deploymentsoftware-Lokalisierung unter Windows“ auf Seite 495
- „Dienstprogramm für die Sprachauswahl (dblang)“ auf Seite 946

Die folgende Tabelle zeigt die Verfügbarkeit der einzelnen Sprachen für die verschiedenen Betriebssystemplattformen.

Plattform	Englisch	Französisch	Deutsch	Japanisch	Vereinfachtes Chinesisch
Windows	Ja	Ja	Ja	Ja	Ja

Plattform	Englisch	Französisch	Deutsch	Japanisch	Vereinfachtes Chinesisch
Windows Mobile	Ja	Ja	Ja	Ja	Ja
Linux	Ja	Ja	Ja	Ja	Ja
Unix	Ja				
Mac OS X	Ja				

## Vollständige Software- und Dokumentationslokalisierung

SQL Anywhere für Windows steht in den folgenden Sprachen für Entwicklung, Deployment und Verwaltung zur Verfügung:

- Englisch
- Französisch
- Deutsch
- Japanisch
- Vereinfachtes Chinesisch

Für Englisch, Deutsch, Japanisch und Vereinfachtes Chinesisch werden alle SQL Anywhere-Komponenten übersetzt:

- Installationsprogramm
- Dokumentation und kontextsensitive Hilfe
- Software

Für Französisch sind das Installationsprogramm, die Software und die kontextsensitive Hilfe übersetzt.

SAP Sybase PowerDesigner Physical Data Model ist nicht lokalisiert und nur in englischer Sprache verfügbar.

## Deploymentsoftware-Lokalisierung unter Windows

Zusätzlich zu den fünf Hauptsprachen (Englisch, Französisch, Deutsch, Japanisch und vereinfachtes Chinesisch) stellt SQL Anywhere Deployment-Softwareressourcen für die folgenden Sprachen bereit:

- Italienisch
- Koreanisch
- Litauisch
- Polnisch
- Portugiesisch (Brasilien)
- Russisch
- Spanisch
- Traditionelles Chinesisch
- Ukrainisch

Deployment-Lokalisierung betrifft eine Teilmenge der Softwarekomponenten, die üblicherweise dem Endverbraucher bereit gestellt werden. Verpackung, Dokumentation, Verwaltung, Entwicklung und Installationssoftware werden nicht lokalisiert. Die lokalisierten Softwarekomponenten sind:

- Datenbankserver- und Clientbibliotheken
- MobiLink-Server und -Client
- SQL Remote-Client
- Befehlszeilen-Tools, z.B. dbinit und dbunload

## Was ist ICU und wann wird es benötigt?

ICU, oder International Components for Unicode, ist eine Open Source-Bibliothek, die von IBM entwickelt und gepflegt wird. ICU erleichtert die Software- Internationalisierung, indem Unicode-Unterstützung angeboten wird. SQL Anywhere implementiert bestimmte Zeichensatzkonvertierungen und Kollationsvorgänge mit ICU.

### Wann wird ICU auf dem Datenbankserver benötigt? (alle Plattformen außer Windows Mobile)

Idealerweise sollte ICU jederzeit zur Verwendung durch den Datenbankserver verfügbar sein. Die folgende Tabelle zeigt, wann und warum ICU benötigt wird:

ICU wird benötigt, wenn Folgendes auftritt	Hinweise
Unicode Collation Algorithm (UCA) wird als Kollation für den NCHAR- oder CHAR-Zeichensatz verwendet.	UCA erfordert ICU.
Der Datenbank-Zeichensatz ist nicht UTF-8, sondern ein Mehrbyte-Zeichensatz.	Für die Kennwortkonvertierung vom Datenbank-Zeichensatz in UTF-8 (Datenbank-Kennwörter werden intern in UTF-8 gespeichert).

ICU wird benötigt, wenn Folgendes auftritt	Hinweise
Die Client- und Datenbank-Zeichensätze sind verschieden und keiner ist ein Mehrbyte-Zeichensatz (einschließlich UTF-8). Dazu gehören Unicode ODBC-, OLE DB-, ADO.NET- und SQL Anywhere JDBC-Anwendungen, unabhängig vom Zeichensatz der Datenbank, wobei zumindest einer dieser Clients nicht über ICU verfügt.	Die korrekte Konvertierung in einen und aus einem Mehrbyte-Zeichensatz erfordert ICU.
Der Datenbank-Zeichensatz ist nicht UTF-8 und eine Konvertierung zwischen CHAR- und NCHAR-Werten ist erforderlich.	Der Datenbankserver benötigt ICU, um UTF-8 in einen anderen Zeichensatz zu konvertieren.
Ein Embedded SQL-Client verwendet einen anderen NCHAR-Zeichensatz als UTF-8.	Der Datenbankserver benötigt ICU, um UTF-8 in einen anderen Zeichensatz zu konvertieren. Der Standard-NCHAR-Zeichensatz des Embedded SQL-Clients ist derselbe wie der ursprüngliche Client-CHAR-Zeichensatz. Dies kann mit der Funktion <code>db_change_nchar_charset</code> geändert werden. Siehe <a href="#">„db_change_nchar_charset-Funktion“ [SQL Anywhere Server - Programmierung]</a> .
Die CSCONVERT- oder SORTKEY-Funktion wird verwendet. Die CSCONVERT-Funktion wird aufgerufen, um zwischen Zeichensätzen zu konvertieren, die den Anforderungen des dritten Punkts (s.o.) entsprechen.	Die Zeichensatzkonvertierung in einen und aus einem Mehrbyte-Zeichensatz erfordert ICU. Die Generierung von Sortierschlüsseln erfordert bei vielen Sortierschlüssellabels UCA, was wiederum ICU erfordert. Siehe <a href="#">„CSCONVERT-Funktion [Zeichenfolge]“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a> und <a href="#">„SORTKEY-Funktion [Zeichenfolge]“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a> .

### Wann wird ICU auf dem Datenbankserver benötigt? (Windows Mobile)

Die folgende Tabelle zeigt, wann und warum ICU bei Windows Mobile benötigt wird:

ICU wird benötigt, wenn Folgendes auftritt	Hinweise
UCA wird als NCHAR- bzw. CHAR-Kollation verwendet.	UCA erfordert ICU.

ICU wird benötigt, wenn Folgendes auftritt	Hinweise
Die SORTKEY-Funktion wird verwendet.	Die Generierung von Sortierschlüsseln erfordert bei vielen Sortierschlüssella-bels UCA, was wiederum ICU erfordert. Siehe „ <a href="#">SORTKEY-Funktion [Zeichenfolge]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
Der CHAR-Zeichensatz stimmt nicht mit dem Betriebssystem-Zeichensatz überein.	Auch wenn die Zeichensätze übereinstimmen, wird ICU empfohlen, weil dadurch die Zeichensatzkonvertierung verbessert wird, wenn Sie NCHAR verwenden oder wenn der CHAR-Zeichensatz ein Mehrbyte-Zeichensatz ist.

**Hinweis**

Wenn Sie die ICU-Bibliothek nicht installieren, müssen Sie bei der Erstellung der Datenbank entweder eine Kollation, deren Zeichensatz dem Windows Mobile-Zeichensatz entspricht, oder UTF8BIN als NCHAR-Kollation wählen. Außerdem müssen Sie bei der Erstellung der Datenbank die UTF8BIN-Kollation als NCHAR-Kollation wählen.

**Wann erhalte ich eine korrekte Zeichensatzkonvertierung auf dem Datenbankserver ohne ICU?**

Sie erhalten eine korrekte Zeichensatzkonvertierung ohne ICU, wenn der Datenbank-Zeichensatz und der Client-Zeichensatz beide Einbyte-Zeichensätze sind und *sqlany.cvf* verfügbar ist (alle Plattformen), oder wenn das Betriebssystem die Konvertierung unterstützt (nur Windows). Dies liegt daran, dass Einbyte-zu-Einbyte-Konvertierungen ohne ICU verarbeitet werden können, wenn die Datei *sqlany.cvf* verfügbar ist bzw. das Host-Betriebssystem die entsprechenden Konverter installiert hat.

**Wann wird ICU auf dem Client benötigt? (alle Plattformen außer Windows Mobile)**

Bei Unicode-Clientanwendungen erhalten Sie wahrscheinlich eine bessere Gesamtperformance bei Client und Datenbankserver, wenn alle Clients UCI installiert haben, unabhängig vom Datenbank-Zeichensatz. Dies liegt daran, dass möglicherweise einige der erforderlichen Konvertierungsaktivitäten vom Datenbankserver auf den Client übertragen werden können, und weil weniger Konvertierungen erforderlich sind.

Wenn Sie ODBC auf Windows-Plattformen verwenden, müssen Sie überdies ICU auf dem Client installiert haben, sogar bei ANSI-Anwendungen. Dies liegt daran, dass der Treibermanager ANSI ODBC-Aufrufe in Unicode ODBC-Aufrufe konvertiert.

## Zeichensätze

Jede Softwarekomponente arbeitet mit einem **Zeichensatz**. Ein Zeichensatz ist eine Menge von Symbolen wie Buchstaben, Ziffern, Leerstellen und andere Symbole. Ein Beispiel eines Zeichensatzes ist ISO-8859-1, auch Latin1 genannt.

Um diese Zeichen intern korrekt darzustellen, verwendet jede Softwarekomponente eine **Kodierung**, auch **Zeichenkodierung** genannt. Eine Kodierung ist eine Methode, bei der jedes Zeichen einem oder mehreren Informationsbytes zugeordnet und als eine hexadezimale Zahl dargestellt wird. Ein Beispiel einer Kodierung ist UTF-8.

Manchmal werden die Ausdrücke "Zeichensatz" und "Kodierung" undifferenziert verwendet, da die beiden Aspekte eng zusammenhängen.

Eine **Codepage** ist eine Kodierungsform. Eine Codepage ist eine Zuordnung von Zeichen zu numerischen Darstellungen, üblicherweise einer Ganzzahl zwischen 0 und 255. Ein Beispiel für eine Codepage ist Windows Codepage 1252.

In dieser Dokumentation werden die Ausdrücke "Kodierung", "Zeichenkodierung", "Zeichensatzkodierung" und "Codepages" als Synonyme verwendet.

Datenbankserver, die Zeichen sortieren (z.B. alphabetische Auflistung von Namen) verwenden eine **Kollation**. Eine Kollation ist eine Kombination aus einer Zeichenkodierung (einer Zuordnung zwischen Zeichen und ihrer Darstellung) und einer **Sortierreihenfolge** für die Zeichen. Es kann mehr als eine Sortierreihenfolge bei den einzelnen Zeichensätzen geben, wie z.B. eine die Groß-/Kleinschreibung berücksichtigende bzw. nicht-berücksichtigende Reihenfolge, oder zwei Sprachen sortieren dasselbe Zeichen möglicherweise in einer unterschiedlichen Reihenfolge.

Die Zeichen werden auf einem Bildschirm mit einer **Schriftart** ausgegeben, der eine Zuordnung zwischen den Zeichen im Zeichensatz und ihrer grafischen Form zugrunde liegt. Schriftarten werden vom Betriebssystem verwaltet.

Die Betriebssysteme benutzen auch eine **Tastaturzuordnung**, um Tasten und Tastenkombinationen bestimmten Zeichen im Zeichensatz zuzuordnen.

## Sprachen in der Client/Server-Umgebung

Datenbankbenutzer, die mit Clientanwendungen arbeiten, können Zeichenfolgen aus folgenden Quellen sehen oder darauf zugreifen:

- **Daten in der Datenbank** Zeichenfolgen und andere Textdaten werden in der Datenbank gespeichert. Der Datenbankserver verarbeitet diese Zeichenfolgen, wenn er Anforderungen beantwortet. Beispiel: Vom Datenbankserver kann gefordert werden, alle Nachnamen zu liefern, die in einer Tabelle nach "N" kommen. Diese Anforderung erfordert Zeichenfolgenvergleiche und nimmt eine Zeichensatz-Reihenfolge an.
- **Meldungen des Datenbankservers** Eine Anwendung kann einen Fehler bewirken, der gemeldet wird. Beispiel: Eine Anwendung sendet eine Abfrage, die auf eine nicht existierende Spalte Bezug nimmt. In diesem Fall gibt der Datenbankserver eine Warnung oder eine Fehlermeldung zurück. Diese Meldung wird in einer **Sprachenressourcenbibliothek** aufbewahrt, die eine verwendete DLL oder von SQL Anywhere gemeinsam genutzte Bibliothek ist.
- **Clientanwendung** Die Schnittstelle der Clientanwendung zeigt Text an und die Clientanwendung kann Text verarbeiten.

- **Meldungen der Clientsoftware** Die Clientbibliothek benutzt dieselbe Sprachenbibliothek wie der Datenbankserver, um für die Clientanwendung Meldungen bereitzustellen.
- **Betriebssysteme** Die Client- und Server-Betriebssysteme können Meldungen liefern oder Text verarbeiten.

In einer zufriedenstellenden Arbeitsumgebung müssen alle diese Textelemente zueinander passen. Oder anders gesagt, sie müssen in der Sprache des Benutzers bzw. seines Zeichensatzes funktionieren.

## Einbyte-Zeichensätze

Bei vielen Sprachen ist die Anzahl der Zeichen so gering, dass ein Byte ausreicht, um alle Zeichen zu beschreiben. In einem solchen Einbyte-Zeichensatz wird jedes Zeichen durch ein Byte repräsentiert, eine zweistellige hexadezimale Zahl.

Insgesamt können nicht mehr als 256 Zeichen in einem Einbyte-Zeichensatz dargestellt werden. In keinem Einbyte-Zeichensatz können alle weltweit verwendeten Buchstaben, einschließlich aller Sonderzeichen, gespeichert werden. Dieses Problem wurde durch die Entwicklung so genannter Codepages gelöst, in denen eine Gruppe von Zeichen beschrieben wird, die jeweils für eine Sprache geeignet sind. Codepage 1253 z.B. enthält den griechischen Zeichensatz und Codepage 1252 westeuropäische Sprachen. Es gibt viele Codepages, und viele Namen für Codepages. Die oben angeführten Codepages sind solche für Windows.

### Untere und obere Seiten

Mit wenigen Ausnahmen sind die Zeichen 0 bis 127 bei allen Codepages gleich. Die Zuordnung dieses Zeichenbereichs nennt man **ASCII-Zeichensatz**. Er enthält das Alphabet der englischen Sprache in Groß- und Kleinschreibung sowie übliche Satzzeichen und die Ziffern. Dieser Bereich wird auch als **7-Bit-ASCII** (da nur sieben Bit für die Darstellung der Zahlen bis 127 benötigt werden) oder **untere Codepage** bezeichnet. Die Zeichen von 128 bis 255 werden **erweiterte Zeichen** oder **obere-Codepage-Zeichen** genannt und unterscheiden sich von Codepage zu Codepage.

Probleme mit der Kompatibilität von Codepages treten nur selten auf, wenn die einzigen benutzten Zeichen aus dem englischen Alphabet stammen, da diese im ASCII-Bereich der Codepage (0 bis 127) vorkommen. Wenn hingegen andere Zeichen benutzt werden, wie dies im Allgemeinen bei Deutsch der Fall ist, kann es zu Problemen kommen, wenn die Datenbank und die Anwendung unterschiedliche Codepages verwenden.

Nehmen wir z.B. eine Datenbank, die den UTF-8-Zeichensatz verwendet und eine Tabelle aus einer Datei lädt, die cp1252-Daten enthält, ohne dass in der LOAD TABLE-Anweisung die Kodierung als cp1252 angegeben ist. Da keine Kodierung angegeben ist, werden die Daten als in UTF-8 kodiert angesehen, daher findet keine Zeichenkonvertierung statt und die cp1252-Kodierung wird direkt in der Datenbank gespeichert. Zeichen wie z.B. das Euro-Symbol, die in cp1252 als hex 80 dargestellt werden, können nicht in UTF-8 konvertiert werden. Das Euro-Symbol in UTF-8 wird durch die Drei-Byte-Sequenz E2 82 AC dargestellt, aber in diesem Fall in der Datenbank als 80 gespeichert. Wenn dann eine Anwendung Daten anfordert, versucht der Datenbankserver, die Daten aus UTF-8 in den Zeichensatz des Clients zu konvertieren. Die Konvertierung erzeugt falsche Zeichen.

## Mehrbyte-Zeichensätze

Einige Sprachen, wie beispielsweise Japanisch und Chinesisch, haben wesentlich mehr als 256 Zeichen. Diese Zeichen können nicht mit einem einzelnen Byte angezeigt werden und müssen daher mit einer Mehrbyte-Kodierung kodiert werden. Außerdem benutzen einige Zeichensätze die viel größere Anzahl von Zeichen in der Mehrbyte-Darstellung, um Zeichen aus vielen Sprachen in einem einzigen, umfassenderen Zeichensatz darzustellen. Ein Beispiel dafür ist UTF-8.

Mehrbyte-Zeichensätze haben möglicherweise eine **variable Breite**, wobei manche Zeichen Einbytezeichen, andere Zweibyte-Zeichen usw., sind.

### Beispiel

Zeichen in Codepage 932 (Japanisch) z.B. sind entweder ein Byte oder zwei Byte lang. Wenn der Wert des ersten Byte, auch **Führungsbyte** genannt, im Bereich der hexadezimalen Werte von \x81 bis \x9F oder von \xE0 bis \xFC (Dezimalwerte 129-159 oder 224-252) liegt, ist das Zeichen ein Zweibyte-Zeichen, und das nachfolgende Byte, auch **Folgebyte** genannt, vervollständigt das Zeichen. Alle Bytes außer dem ersten Byte sind Folgebytes.

Wenn das erste Byte außerhalb des Führungsbyte-Bereichs liegt, ist das Zeichen ein Einbytezeichen und das nächste Byte das erste Byte des folgenden Zeichens.

### Siehe auch

- „[SQL Anywhere-Kollationsalgorithmus \(SACA\)](#)“ auf Seite 515

## ANSI- und OEM-Codepages in Windows

Unter Windows werden zwei Codepages verwendet. Anwendungen, die die grafische Windows-Benutzeroberfläche verwenden, verwenden die Windows-Codepage. Windows-Codepages sind mit ISO-Zeichensätzen sowie mit ANSI-Zeichensätzen kompatibel. Sie werden häufig **ANSI-Codepages** genannt.

Zeichenmodusanwendungen (die das Befehlszeilenfenster verwenden) unter Windows verwenden Codepages, die unter DOS verwendet wurden. Sie werden aus entwicklungsgeschichtlichen Gründen als **OEM-Codepages** (OEM = Original Equipment Manufacturer) bezeichnet.

SQL Anywhere unterstützt Kollationen, die sowohl auf OEM- als auch auf ANSI-Codepages basieren. Die OEM-Kollationen werden aus Kompatibilitätsgründen bereitgestellt und sollten nicht für neue Datenbanken verwendet werden.

### Siehe auch

- „[Alternative Kollationen](#)“ auf Seite 518

## Zeichensätze in SQL Anywhere-Datenbanken

Eine SQL Anywhere-Datenbank kann einen oder zwei Zeichensätze (Kodierungen) zum Speichern von Zeichendaten verwenden. Die CHAR-Datentypen wie CHAR, VARCHAR und LONG VARCHAR verwenden einen Einbyte- oder einen Mehrbyte-Zeichensatz. UTF-8 kann verwendet werden. Die NCHAR-Datentypen wie NCHAR, NVARCHAR und LONG NVARCHAR verwenden UTF-8.

SQL-Anweisungen wie LOAD TABLE und Funktionen wie CSCONVERT, TO\_CHAR und TO\_NCHAR verweisen mit den Parametern **db\_charset** und **nchar\_charset** auf den CHAR- bzw. NCHAR-Zeichensatz der Datenbank.

### Siehe auch

- „Zeichendatentypen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CSCONVERT-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „TO\_CHAR-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „TO\_NCHAR-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Unterstützte Zeichensätze

SQL Anywhere unterstützt eine wachsende Liste von mehreren hundert Zeichensätzen und Labels. Zeichensatzkodierungen haben eine Vielzahl von Namen und Labels. Um eine Liste der Zeichensätze zu erhalten, die von SQL Anywhere unterstützt werden, führen Sie den folgenden Befehl aus:

```
dbinit -le
```

Jede Zeile der Ausgabe listet die gebräuchlichsten Labels für eine gegebene Zeichensatzkodierung, durch Kommata getrennt, auf. Das erste Label in jeder Zeile der Ausgabe ist der bevorzugte SQL Anywhere-Name für die Zeichensatzkodierung. Die anderen Labels sind solche, die von verschiedenen Behörden, Organisationen oder Standards verwendet werden. Diese sind IANA (Internet Assigned Numbers Authority), MIME (Multipurpose Internet Mail Extensions), ICU (International Components for Unicode), JAVA oder ASE (Adaptive Server Enterprise).

Wenn Sie den gewünschten Zeichensatz nicht finden, können Sie auch den folgenden Befehl ausführen, um eine längere Liste anzuzeigen, die weniger gängige Labels enthält:

```
dbinit -le+
```

Wenn ein Zeichensatzlabel angegeben wird, sucht SQL Anywhere nach dem Label in der Menge ihm bekannter Labels. Verschiedene Behörden verwenden manchmal dasselbe Label für unterschiedliche Zeichensätze. SQL Anywhere bemüht sich, Mehrdeutigkeiten anhand des Inhalts zu lösen. Beispiel: Einer JDBC-Anwendung, die einen Zeichensatz mit einem mehrdeutigen Label referenziert, wird ein Java-Standardlabel zugeordnet. Es wird empfohlen, immer das SQL Anywhere-Label zu verwenden, um Mehrdeutigkeiten zu vermeiden. Weitere Informationen über die Zeichensatzlabel finden Sie unter <http://site.icu-project.org/>.

Zusätzlich zu den Zeichensatzlabels, die von der dbinit-Option -le zurückgegeben werden, können Sie auch die folgenden Aliasnamen für Zeichensätze verwenden:

- **os\_charset** Alias für den Zeichensatz, der vom Betriebssystem verwendet wird, das den Datenbankserver hostet.
- **char\_charset** Alias für den von der Datenbank verwendeten CHAR-Zeichensatz
- **nchar\_charset** Alias für den von der Datenbank verwendeten NCHAR-Zeichensatz

Eine einfache Möglichkeit zu bestimmen, ob ein Zeichensatz oder ein Label unterstützt wird, ist die Verwendung der CSCONVERT-Funktion.

### Siehe auch

- [„CSCONVERT-Funktion \[Zeichenfolge\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Fragen und Antworten zu Zeichensätzen

In der folgenden Tabelle wird angegeben, wo Sie Antworten auf Fragen finden.

Frage	Empfohlene Lektüre
Welche Kollation soll ich für meine Datenbank verwenden?	<a href="#">„Kollationen“</a>
Wie werden Zeichen in der Software, besonders in SQL Anywhere dargestellt?	<a href="#">„Zeichensätze“</a>
Welche Kollationen stellt SQL Anywhere bereit?	<a href="#">„Hinweise zur Kollation“</a>
Welche Zeichensatzkodierungen werden von SQL Anywhere unterstützt?	<a href="#">„Unterstützte Zeichensätze“</a>
Meine Clientcomputer verwenden einen anderen Zeichensatz als die Datenbank. Wie kann ich die Zeichen korrekt zwischen Client und Server austauschen lassen?	<a href="#">„Zeichensatzkonvertierung“</a>
Welche Zeichensätze kann ich bei Verbindungszeichenfolgen verwenden?	<a href="#">„Verbindungszeichenfolgen und Zeichensätze“</a>
Wie ändere ich die Kollationssequenz einer bestehenden Datenbank?	<a href="#">„Datenbankkollationen ändern“</a>

## Zeichensatzkonvertierung

SQL Anywhere kann eine Zeichensatzkonvertierung bei Zeichensätzen durchführen, die dieselben Zeichen darstellen, aber eine unterschiedliche Position im Zeichensatz oder auf der Codepage haben. Eine gewisse Kompatibilität zwischen den Zeichensätzen muss daher gegeben sein. Eine Zeichensatzkonvertierung ist z.B. zwischen EUC-JIS- und cp932-Zeichensätzen möglich, aber nicht zwischen EUC-JIS und cp1252.

SQL Anywhere implementiert eine Zeichensatzkonvertierung unter Verwendung der Open Source-Bibliothek ICU (International Components for Unicode), die von IBM entwickelt und unterhalten wird.

**Siehe auch**

- „Datentypvergleiche“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Verbindungszeichenfolgen und Zeichensätze

Wenn nicht alle Ihre Clients dieselben Zeichensätze verwenden, können Verbindungszeichenfolgen während der Zeichensatzkonvertierung zu einem Problem werden. Das ist so, weil die Verbindungszeichenfolge vom Client syntaktisch analysiert wird, um einen Datenbankserver zu finden oder zu starten. Diese Analyse wird jedoch ohne Kenntnisse des vom Datenbankserver verwendeten Zeichensatzes bzw. der Sprache durchgeführt.

Die Interface-Bibliothek führt folgendermaßen eine syntaktische Analyse der Verbindungszeichenfolge durch:

1. Die Verbindungszeichenfolge wird in ihre *Schlüsselwort=Wert*-Paare aufgegliedert. Dies kann unabhängig vom Zeichensatz erfolgen, sofern die Verbindungsparameter CommLinks (LINKS) nicht in geschweifte Klammern "{}" gesetzt werden. Benutzen Sie stattdessen die empfohlenen Klammern (). Geschweifte Klammern sind gültige **Folgebytes** (Bytes nach dem ersten Byte) in einigen Mehrbyte-Zeichensätzen.
2. Der Standort des Datenbankservers wird ermittelt. Beim Servernamen wird keine Zeichensatzkonvertierung durchgeführt. Wenn der Client- und der Serverzeichensatz verschieden sind, kann die Verwendung von erweiterten Zeichen im Servernamen dazu führen, dass der Server nicht gefunden wird.

Wenn Ihre Clients und Server auf unterschiedlichen Betriebssystemen oder in verschiedenen Sprachumgebungen laufen, sollten Sie 7-Bit-ASCII-Zeichen im Datenbankservernamen verwenden.

3. Die Verbindungsparameter DatabaseName (DBN) oder DatabaseFile (DBF) werden aus dem Clientzeichensatz in den Zeichensatz des Datenbankservers konvertiert.
4. Wenn die Datenbank gefunden wurde, werden die verbliebenen Verbindungsparameter in den Zeichensatz der Datenbank konvertiert.

## SQL-Anweisungen und Zeichensätze

Die Zeichensatzkonvertierung von SQL Anywhere-Server bewirkt, dass SQL-Anweisungen vor der syntaktischen Analyse und der Ausführung in den Zeichensatz der Datenbank konvertiert werden. Eine Nebenwirkung dieser Konvertierung ist, dass Zeichen in der SQL-Anweisung, die nicht in den Zeichensatz der Datenbank konvertiert werden können, in ein Ersatzzeichen konvertiert werden. Eine SQL-Anweisung mit einem beliebigen Unicode-Zeichen kann auf eine der folgenden Arten ausgeführt werden:

- Verwenden Sie die Funktion UNISTR, um die Unicode-Zeichenwerte anzugeben.
- Verwenden Sie eine Hostvariable, um die Unicode-Zeichenwerte anzugeben.

- Verwenden Sie UTF-8 als den Zeichensatz der Datenbank.

Wenn Sie UTF8BIN als CHAR-Kollation auswählen, ist der Zeichensatz der Datenbank UTF-8. Wenn Sie UCA als CHAR-Kollation auswählen, können Sie UTF-8-Kodierung als Zeichensatz wählen.

Der Unicode-Kollationsalgorithmus (UCA, Unicode Collation Algorithm) stellt erweiterte Vergleiche, Sortierungen und Groß-/Kleinschreibungs-Konvertierungen bereit, aber er kann sich auf die Performance auswirken. Auch wenn UTF8BIN Platz sparend und schnell ist, so sind Sortierreihenfolge und Vergleiche binär. Geben Sie die CHAR-Kollation als UTF8BIN an, wenn Sie Unicode-Zeichen in Ihren SQL-Anweisungen benötigen, aber nicht die volle Funktionalität von UCA für Sortierungen und Vergleiche brauchen. Verwenden Sie UCA nur wenn nötig, indem Sie die Funktionen SORTKEY und COMPARE benutzen.

### Siehe auch

- „SORTKEY-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „COMPARE-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Unicode-Kollationsalgorithmus (UCA)“ auf Seite 516
- „SQL Anywhere-Kollationsalgorithmus (SACA)“ auf Seite 515
- [Als Verbindungszeichenfolge übergebene Verbindungsparameter auf Seite 31](#)

## Fehlerbehandlung von unerwarteten Symbolen bei der Anzeige von Daten

Wenn Sie Daten unter Verwendung einer Clientanwendung wie z.B. Interactive SQL auswählen und anzeigen, können unerwartete Symbole wie Quadrate, Pfeile und Fragezeichen als Zeichen in den Daten auftreten.

Der wichtigste Grund für die Darstellung von unerwarteten Symbolen ist, dass die zum Anzeigen der Daten verwendete Schriftart die Zeichen nicht unterstützt. Sie können dieses Problem beheben, indem Sie zu einer Unicode-Schriftart wechseln. Wenn es nicht möglich ist, die Schriftart für die Clientanwendung zu ändern, können Sie auch die Standardschriftart des Betriebssystems ändern.

Unerwartete Symbole können auch in der Clientanwendung auftreten, wenn es ein Problem mit den darunterliegenden Daten gibt, die in der Datenbank gespeichert sind. Beispiel: Wenn eine Zeichensatzkonvertierung erforderlich war, als die Daten in die Datenbank eingefügt wurden, und manche Zeichen im ursprünglichen Zeichensatz kein gleichwertiges Zeichen im Zeichensatz der Datenbank hatten, wurden stattdessen Ersatzzeichen eingefügt.

Beispiel: In Windows unterstützt die Standard-Schriftart Tahoma keine japanischen Zeichen. Wenn der Zeichensatz Ihrer Datenbank cp932 ist und die Datenbank japanische Daten enthält, werden bei einer Abfrage der Datenbank die Ergebnisse als kleine Quadrate dargestellt. In Interactive SQL können Sie die im Fensterausschnitt **Ergebnisse** verwendete Schriftart ändern, indem Sie auf **Extras » Optionen » SQL Anywhere/UltraLite » Ergebnisse » Schriftart** klicken und eine Unicode-Schriftart wie Arial Unicode MS oder Lucida Sans Unicode angeben. Unicode-Schriftarten sind eine gute Wahl, weil sie in der Lage sind, Zeichen aus vielen Sprachen anzuzeigen.

Wenn Ihre Clientanwendung keine Änderung der Schriftarteinstellungen ermöglicht, verwendet sie wahrscheinlich die Standardschriftart Ihres Betriebssystems. In diesem Fall finden Sie in der

Dokumentation zu Ihrem Betriebssystem Hinweise darüber, wie Sie die Standardschriftart des Systems in eine Unicode-Schriftart ändern.

#### Siehe auch

- „Verlustreiche Konvertierung und Ersetzungszeichen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Interactive SQL“ auf Seite 814

## Internationale Aspekte der Groß-/Kleinschreibung

In SQL Anywhere wird bei Bezeichnern wie Systemansichtsnamen oder Spaltennamen immer die **Groß-/Kleinschreibung beibehalten** und die **Groß-/Kleinschreibung nicht berücksichtigt**. Die Namen werden in der Groß-/Kleinschreibung, in der sie erstellt wurden, gespeichert, aber beim Zugriff auf die Bezeichner wird die Groß-/Kleinschreibung nicht berücksichtigt.

Die Namen von Systemansichten z.B. werden in Großbuchstaben (SYSDOMAIN, SYSTAB etc.) gespeichert, aber beim Zugriff wird die Groß-/Kleinschreibung nicht berücksichtigt, daher sind die beiden folgenden Anweisungen äquivalent:

```
SELECT * FROM systab;  
SELECT * FROM SYSTAB;
```

Die Äquivalenz von Groß- und Kleinbuchstaben wird in der Kollation festgelegt. Es gibt Kollationen, bei denen Sie mit der Annahme der Nichtberücksichtigung von Groß-/Kleinschreibung bei den Bezeichnern vorsichtig sein müssen. Türkische Kollationen z.B. haben ein Groß-/Kleinbuchstaben-Konvertierungsverhalten, das unerwartete und subtile Fehler zur Folge haben kann. Der häufigste Fehler ist, dass ein Systemobjekt, das einen Buchstaben **I** oder **i** enthält, nicht gefunden wird. Siehe „[Türkische Zeichensätze und Kollationen](#)“ auf Seite 532.

## Zeichensatzkonvertierung und Client-APIs

In Umgebungen mit mehreren Zeichensätzen können Probleme mit der Zeichensatzkonvertierung auftreten. Dabei kann es schwierig werden zu ermitteln, wo das Konvertierungsproblem aufgetreten ist. Wenn sich bei Client-APIs Probleme mit der Zeichensatzkonvertierung ergeben, überprüfen Sie die Datenbank und die Verbindungsoptionen sowie die Eigenschaften zum Steuern der Zeichensatzkonvertierung.

Es gibt zwei Kategorien von Konvertierungsproblemen. Die erste betrifft das Senden von Daten an die Client-API im falschen Format. Obwohl dies bei Unicode-APIs nicht auftreten kann, ist es bei allen anderen Client-APIs und Ergebnissen in Garbage-Daten möglich.

Die zweite Problemkategorie betrifft Zeichen, die keine Entsprechung im endgültigen Zeichensatz oder im Zeichensatz einer Zwischenstufe haben. In diesem Fall wird ein Ersetzungszeichen verwendet. Hierbei handelt es sich um eine so genannte verlustreiche Konvertierung, die bei jeder beliebigen Client-API auftreten kann. Sie können verlustreiche Konvertierungen umgehen, indem Sie UTF-8 als Zeichensatz der Datenbank festlegen. Siehe „[Verlustreiche Konvertierung und Ersetzungszeichen](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

## Options- und Eigenschaftseinstellungen, die sich auf die Zeichensatzkonvertierung auswirken

Die Datenbankoptionen, Datenbankeigenschaften und Verbindungseigenschaften, die für eine Verbindung gelten, stehen in der Regel in der vollständigen Verbindungszeichenfolge zur Verfügung. Sie können die Einstellungen jedoch auch mithilfe von Funktionen wie PROPERTY, DB\_PROPERTY und CONNECTION\_PROPERTY abfragen. Zum Beispiel:

Abfrage	Beschreibung
SELECT PROPERTY( "CharSet");	Gibt den Betriebssystem-Zeichensatz des Datenbankservers zurück.
SELECT DB_PROPERTY( "CharSet");	Gibt den CHAR-Zeichensatz der Datenbank zurück.
SELECT DB_PROPERTY( "Nchar-CharSet");	Gibt den NCHAR-Zeichensatz der Datenbank zurück.
SELECT DB_PROPERTY( "Multibyte-CharSet");	Gibt zurück, ob CHAR-Daten einen Mehrbyte-Zeichensatz verwenden (On=ja, Off=nein)
SELECT CONNECTION_PROPERTY( "CharSet");	Gibt den CHAR-Zeichensatz des Clients zurück.
SELECT CONNECTION_PROPERTY( "NcharCharSet");	Gibt den NCHAR-Zeichensatz des Clients zurück.
SELECT CONNECTION_PROPERTY("on_charset_conversion_failure");	Gibt den Wert der on_charset_conversion_warning-Option zurück.

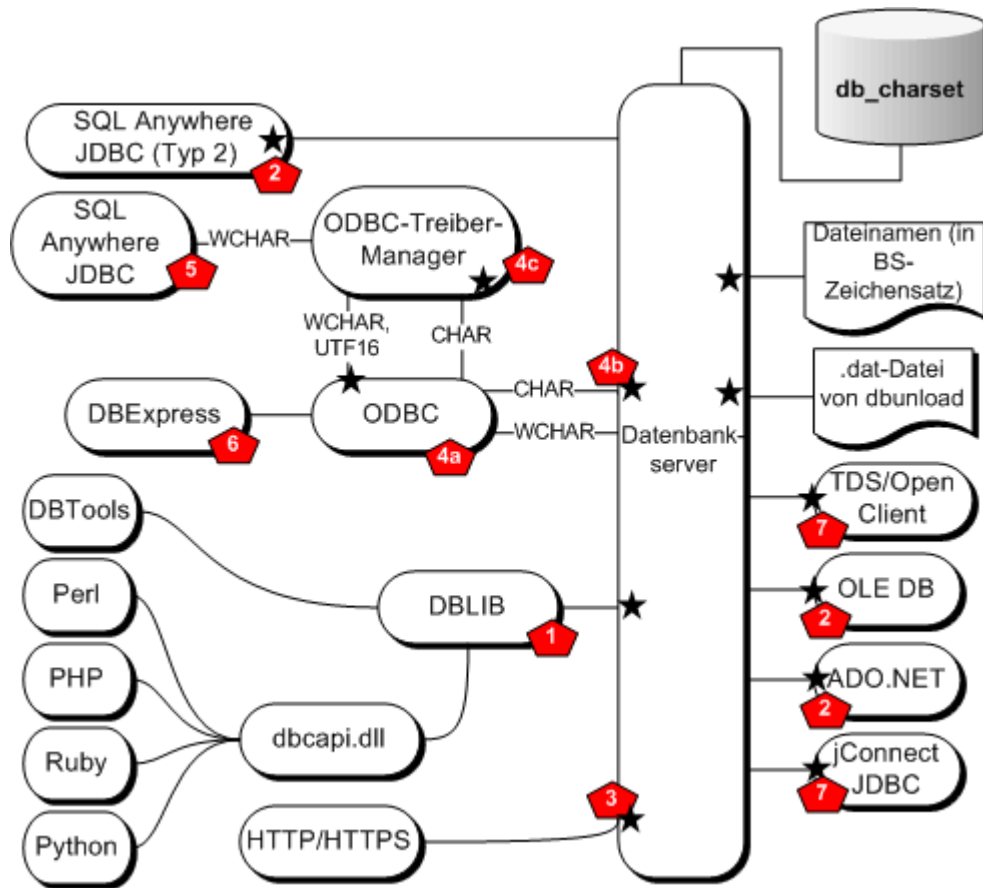
### Siehe auch

- „PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DB\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CONNECTION\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „on\_charset\_conversion\_failure-Option“ auf Seite 645

## Client-API und Punkte für die Zeichensatzkonvertierung

Das folgende Diagramm veranschaulicht, an welchen Punkten eine Zeichensatzkonvertierung möglich ist, wenn Client-APIs mit dem Datenbankserver interagieren.

Die schwarzen Sterne im Diagramm zeigen an, wo diese Zeichensatzkonvertierung erfolgen kann. Die Zahlen in der Abbildung entsprechen denjenigen in den zusätzlichen Hinweisen im Anschluss.



- 1 – DBLIB** Der Standardwert für die Zeichensätze DBLIB CHAR und NCHAR ist der Zeichensatz des Client-Betriebssystems. Der CHAR-Zeichensatz wird für alle Zeichenfolgendaten mit Ausnahme von BINARY und NCHAR verwendet. Der NCHAR-Zeichensatz wird für Hostvariablen mit dem Datentyp NCHAR und Host-Parameter verwendet (diese stehen in den DBTools- oder DBCAPI-Schnittstellen nicht zur Verfügung). Der Datenbankserver führt alle Zeichensatzkonvertierungen durch.

Sie legen die Zeichensätze CHAR und NCHAR mithilfe des Verbindungsparameters CharSet bzw. der Funktion `db_change_nchar_charset` fest. Siehe „[Verbindungsparameter CharSet \(CS\)](#)“ auf Seite 343 und „[db\\_change\\_nchar\\_charset-Funktion](#)“ [*SQL Anywhere Server - Programmierung*].

- 2 – Unicode-APIs** Bei Unicode-APIs konvertiert ein Treiber die Unicode UTF-16-Zeichendaten in den und aus dem Zeichensatz der Datenbank. Der Treiber konvertiert Unicode-Host-Parameter in den NCHAR-Zeichensatz (UTF-8), bevor er sie an den Datenbankserver sendet. Die als NCHAR beschriebenen Spalten einer Ergebnismenge werden im NCHAR-Zeichensatz (UTF-8) abgerufen und, nachdem sie empfangen wurden, in Unicode konvertiert. Es wird nicht empfohlen, den Verbindungsparameter CharSet zu setzen, da dies zu einer verlustreichen Konvertierung führen kann. Siehe „[Verlustreiche Konvertierung und Ersetzungszeichen](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

- **3 – HTTP/HTTPS HTTP-Dienste (SQL Anywhere als Server):** Bei HTTP-Diensten gibt es zwei Anforderungstypen: URL-kodierte und Multipart/Formdaten-Anforderungen.

**URL-kodiert:** Die Anforderungen haben das Format "application/x-www-form-urlencoded". Hierbei werden die Variablen als Schlüssel/Wert-Paare übergeben. Der Datenbankserver dekodiert %-kodierte Daten (UTF-8 oder Zeichensatz der Datenbank) automatisch und konvertiert die Schlüssel/Wert-Paare in den Zeichensatz der Datenbank. Die verarbeiteten Werte können mithilfe der HTTP\_VARIABLE-Funktion extrahiert werden. Dabei kann mithilfe der @BINARY- oder @TRANSPORT-Attribute ein Wert zurückgegeben werden, der zwar %-dekodiert wird, dessen Zeichensatz aber nicht konvertiert wird. Alternativ kann der unformatierte HTTP-(Transport-)Wert zurückgegeben werden.

**Multipart/Formdaten:** Die Anforderungen werden als binär betrachtet, d. h. die Attribute @BINARY und @TRANSPORT geben identische Werte zurück.

Die Zeichensatzkonvertierung einer HTTP-Dienstantwort hängt von den HTTP-Optionen CharSetConversion und AcceptCharset ab. Sie können diese mit der Systemprozedur sa\_set\_http\_option einstellen. Siehe „sa\_set\_http\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Des Weiteren können sich die folgenden Einstellungen auf die Zeichensatzkonvertierung für Anforderungen und Antworten auswirken: der Accept-Charset-Header, der für die Festlegung der bevorzugten Zeichensätze benutzt wird, und der Content-Type-Header, mit dessen Hilfe der Zeichensatz des Inhalts gekennzeichnet wird.

**HTTP-gespeicherte Prozeduren (SQL Anywhere als Client):** Bei HTTP-gespeicherten Prozeduren werden CHAR-Daten im Zeichensatz der Datenbank gesendet. Wenn ein Parameter ein NCHAR-Typ ist, werden alle Daten als UTF-8 gesendet (alle CHAR-Parameter werden in UTF-8 konvertiert). Die Anforderung sendet einen Accept-Charset-HTTP-Header, der den Zeichensatz der Datenbank als bevorzugten Zeichensatz kennzeichnet. UTF-8 ist immer in der Liste der bevorzugten Zeichensätze enthalten. Wenn die Antwort im Content-Type-Header einen anderen Zeichensatz angibt als den Zeichensatz der Datenbank, dann konvertiert der Client die Antwort in den Zeichensatz der Datenbank.

- **4a – ODBC mit Unicode-Eintrittspunkten** Wenn eine ODBC-Anwendung Unicode-Eintrittspunkte benutzt, wird sie als Unicode-Client-API betrachtet. WCHAR-Daten werden auf die gleiche Weise verarbeitet wie für Unicode-APIs. Wenn eine ODBC-Anwendung die Unicode-Eintrittspunkte und CHAR-(ANSI)-Daten benutzt, wird angenommen, dass die Daten im Zeichensatz der Datenbank vorliegen. Es wird nicht empfohlen, CHAR- und WCHAR-Daten in einer Anwendung zu mischen.
- **4b – ODBC mit ANSI-Eintrittspunkten** Wenn eine ODBC-Anwendung ANSI-Eintrittspunkte benutzt, wird sie als Unicode-Client-API betrachtet. Der CHAR-Zeichensatz hat standardmäßig den Wert des Zeichensatzes des Client-Betriebssystems. Der CHAR-Zeichensatz kann mithilfe des Verbindungsparameters CharSet geändert werden. Siehe „[Verbindungsparameter CharSet \(CS\)](#)“ auf Seite 343.

Jede Konvertierung von ANSI-Daten erfolgt durch den Datenbankserver. Das Abrufen von WCHAR-Hostvariablen kann zu einer verlustreichen Konvertierung von CHAR-Daten auf dem

Datenbankserver führen. Es wird nicht empfohlen, CHAR- und WCHAR-Daten in einer Anwendung zu mischen.

- **4c – ODBC-Treibermanager** Einige ODBC-Treibermanager konvertieren alle CHAR-Daten in WCHAR-Daten und rufen dann die Unicode-Eintrittspunkte auf.
- **5 – SQL Anywhere JDBC-Treiber** Der SQL Anywhere JDBC-Treiber führt keine Zeichensatzkonvertierung durch und verwendet die Unicode-Eintrittspunkte und WCHAR-Typen des ODBC-Treibers. Es handelt sich um den gleichen Fall wie unter ODBC mit Unicode-Eintrittspunkten beschrieben.
- **6 – Embarcadero dbExpress** Der Embarcadero DBExpress-Treiber verwendet ODBC als ANSI-Client-API. Der CHAR-Zeichensatz hat standardmäßig den Wert des Zeichensatzes des Client-Betriebssystems. Sie können ihn zwar mithilfe des Verbindungsparameters CharSet ändern, jedoch ist dies nicht empfehlenswert, da es zu fehlerhaften Daten führen kann.
- **7 – TDS-Clients** TDS-Clients wie etwa Sybase Open Client und jConnect verhandeln zur Verbindungszeit mit dem Datenbankserver und ziehen es vor, dass die Zeichensatzkonvertierung auf dem Client stattfindet. Während der Aushandlung wird der Datenbankserver angewiesen, den Zeichensatz nicht zu konvertieren.

#### Siehe auch

- „Datentypkonvertierungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Verlustreiche Konvertierung und Ersetzungszeichen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Konvertierungen von NCHAR in CHAR“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SQL Anywhere-C-API-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „Perl/DBI-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „Python-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „SQL Anywhere-PHP-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „SQL Anywhere-Ruby-API-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „Sybase Open Client-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „SQL Anywhere als HTTP-Webserver“ [[SQL Anywhere Server - Programmierung](#)]
- „OLE DB“ [[SQL Anywhere Server - Programmierung](#)]
- „SQL Anywhere .NET-Datenprovider“ [[SQL Anywhere Server - Programmierung](#)]
- „ODBC-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]
- „JDBC-Unterstützung“ [[SQL Anywhere Server - Programmierung](#)]

## Sprachumgebungen

Sowohl der Datenbankserver als auch die Clientbibliothek erkennen die Sprachen- und Zeichensatzumgebung, indem Sie eine **Sprachumgebungsdefinition** verwenden.

Die Anwendungssprachumgebung bzw. Clientsprachumgebung wird vom Client oder der Clientbibliothek bei Anforderungen an den Datenbankserver verwendet, um den Zeichensatz, in dem Ergebnisse zurückgegeben werden sollen, wie auch die Sprache von Fehlermeldungen, Warnungen und anderen Meldungen zu bestimmen. Der Datenbankserver vergleicht seine Sprachumgebung mit der Anwendungssprachumgebung, um zu bestimmen, ob eine Zeichensatzkonvertierung erforderlich ist.

Verschiedene Datenbanken auf einem Server können unterschiedliche Sprachumgebungen haben, und jeder Client kann seine eigene Sprachumgebung haben.

Die Sprachumgebung besteht aus folgenden Komponenten:

- **Sprache** Die Sprache ist ein zweistelliger Code, der Standardwerte gemäß ISO-639-1 verwendet (zum Beispiel DE für Deutsch). Der Datenbankserver und der Client haben Sprachwerte für ihre Locale.

Der Datenbankserver verwendet die Sprachumgebungsangabe, um zu ermitteln, welche Sprachenbibliotheken er laden soll. Wenn beim Erstellen einer Datenbank keine Kollation angegeben wird, verwendet der Datenbankserver neben dem Zeichensatz auch die Sprache, um zu bestimmen, welche Kollation verwendet werden soll.

Die Clientbibliothek verwendet die Sprachumgebungsangabe, um die zu ladenden Sprachenbibliotheken sowie die Sprache zu bestimmen, die von der Datenbank angefordert wird.

- **Zeichensatz** Der Zeichensatz ist die verwendete Codepage bzw. Kodierung. Sowohl Client als auch Server verwenden Zeichensatzwerte, und die Werte können unterschiedlich sein. Wenn sie sich unterscheiden, wird eine Zeichensatzkonvertierung verwendet, um Interoperabilität zu ermöglichen.

## Sprache der Sprachumgebung

Die Sprachumgebung ist die Sprache, die vom Benutzer der Clientanwendung verwendet wird bzw. von der erwartet wird, dass sie Benutzer des Datenbankservers verwenden. Weitere Hinweise darüber, wie Sie Sprachumgebungseinstellungen ermitteln, finden Sie unter [„Informationen zur Sprachumgebung“ auf Seite 512](#).

Die Clientbibliothek und der Datenbankserver ermitteln beide die Sprachkomponente der Sprachumgebung auf dieselbe Art:

1. Den Wert der Umgebungsvariable SALANG verwenden, falls vorhanden. Siehe [„SALANG-Umgebungsvariable“ auf Seite 473](#).
2. Wenn unter Windows die Umgebungsvariable SALANG nicht vorhanden ist, überprüfen Sie den SQL Anywhere-Registrierungseintrag "Sprache". Siehe [„Registrierungseinstellungen bei der Installation“ auf Seite 490](#).
3. Die Spracheinstellung des Betriebssystems überprüfen.
4. Wenn die Sprache weiterhin nicht anhand der oben genannten Einstellungen ermittelt werden kann, standardmäßig Englisch verwenden.

## Werte der Sprachen-Labels

Die folgende Tabelle zeigt die gültigen Werte für Sprachen-Labels, zusammen mit den äquivalenten ISO 639-Sprachcodes:

<b>Sprache</b>	<b>ISO-639-1-Sprachencode</b>	<b>Sprachen-Label</b>	<b>Alternatives Label</b>
Arabisch	AR	arabic	k.A.
Tschechisch	CS	czech	k.A.
Dänisch	DA	danish	k.A.
Holländisch	NL	dutch	k.A.
Englisch	EN	us_english	english
Finnisch	FI	finnish	k.A.
Französisch	FR	french	k.A.
Deutsch	DE	german	k.A.
Griechisch	EL	greek	k.A.
Hebräisch	HE	hebrew	k.A.
Ungarisch	HU	hungarian	k.A.
Italienisch	IT	italian	k.A.
Japanisch	JA	japanese	k.A.
Koreanisch	KO	korean	k.A.
Litauisch	LT	lithuanian	k.A.
Norwegisch	NO	norwegian	norweg
Polnisch	PL	polish	k.A.
Portugiesisch	PT	portuguese	portugue
Russisch	RU	russian	k.A.
Vereinfachtes Chinesisch	ZH	chinese	simpchin
Spanisch	ES	spanish	k.A.
Schwedisch	SV	swedish	k.A.
Thailändisch	TH	thai	k.A.
Traditionelles Chinesisch	TW	tchinese	tradchin

Sprache	ISO-639-1-Sprachencode	Sprachen-Label	Alternatives Label
Türkisch	TR	turkish	k.A.
Ukrainisch	UK	ukrainian	k.A.

## Zeichensatz der Sprachumgebung

Die Sprachumgebungsdefinitionen sowohl der Anwendung als auch des Servers verwenden einen Zeichensatz. Die Anwendung benutzt ihren Zeichensatz, wenn Text vom Datenbankserver angefordert wird. Der Datenbankserver vergleicht den Datenbank-Zeichensatz mit dem der Anwendung, um zu bestimmen, ob eine Zeichensatzkonvertierung erforderlich ist. Wenn der Datenbankserver nicht in der Lage ist, in den und aus dem Clientzeichensatz zu konvertieren, schlägt die Verbindung fehl.

1. Wenn die Umgebungsvariable `SACHARSET` gesetzt ist, wird ihr Wert verwendet, um den Zeichensatz zu bestimmen.

Der Datenbankserver verwendet `SACHARSET` nur bei der Erstellung von neuen Datenbanken, und dann nur, wenn keine Kollation angegeben ist.

2. Wenn in der Verbindungszeichenfolge ein Zeichensatz angegeben ist, wird dieser benutzt. Siehe [„Verbindungsparameter CharSet \(CS\)“ auf Seite 343](#).
3. Sybase Open Client-Anwendungen überprüfen die Datei *locales.dat* im Unterverzeichnis *Sprachumgebungen* des Sybase-Versionsverzeichnisses.
4. Zeichensatzinformationen des Betriebssystems werden verwendet, um die Sprachumgebung zu bestimmen:
  - Auf Windows-Betriebssystemen wird die aktuelle Windows ANSI-Codepage verwendet.
  - Auf UNIX-Plattformen werden die folgenden Sprachumgebungsvariablen in der angegebenen Reihenfolge überprüft: `LC_ALL`, `LC_MESSAGES`, `LC_CTYPE`, `LANG`. Der Wert der ersten Umgebungsvariablen, die als gesetzt erkannt wird, wird zur Bestimmung des Zeichensatzes verwendet. Wenn der Zeichensatz nicht anhand des Betriebssystems bestimmt werden kann, wird der Standard von `iso_1` (auch als Windows Codepage 28591, ISO 8859-1 Latin I, ISO 8859-1 Latin-1 oder `iso_8859-1:1987` referenziert) verwendet.
5. Auf allen anderen Plattformen wird eine Standard-Codepage `cp1252` verwendet.

### Siehe auch

- [„Informationen zur Sprachumgebung“ auf Seite 512](#)
- [„SACHARSET-Umgebungsvariable“ auf Seite 472](#)

## Informationen zur Sprachumgebung

Sie können Sprachumgebungsinformationen mithilfe von Funktionen wie `PROPERTY`, `DB_PROPERTY` und `CONNECTION_PROPERTY` bestimmen. Die folgende Tabelle zeigt, wie Sie diese Funktionen

verwenden, um Sprachumgebungsinformationen über die Clientverbindung, die Datenbank und den Datenbankserver zu erhalten.

Systemfunktion und Parameter	Rückgabewert
<code>SELECT PROPERTY( 'CharSet' );</code>	Zeichensatz des Datenbankservers. In der Regel der Zeichensatz des Computers, auf dem der Datenbankserver läuft.
<code>SELECT PROPERTY( 'DefaultCollation' );</code>	Standard-CHAR-Kollation, die vom Datenbankserver zum Erstellen von Datenbanken verwendet wird
<code>SELECT PROPERTY( 'DefaultNcharCollation' );</code>	Standard-NCHAR-Kollation, die vom Datenbankserver zum Erstellen von Datenbanken verwendet wird
<code>SELECT PROPERTY( 'Language' );</code>	Die Sprachumgebungsangabe für den Datenbankserver.
<code>SELECT DB_PROPERTY( 'CharSet' );</code>	Zeichensatz, der zum Speichern von CHAR-Daten in der Datenbank verwendet wird
<code>SELECT DB_PROPERTY( 'NcharCharSet' );</code>	Zeichensatz, der zum Speichern von NCHAR-Daten in der Datenbank verwendet wird
<code>SELECT DB_PROPERTY( 'MultiByteCharSet' );</code>	Ob CHAR-Daten einen Mehrbyte-Zeichensatz verwenden (On=ja, Off=nein)
<code>SELECT DB_PROPERTY( 'Language' );</code>	Kommagetrennte Liste von Codes aus zwei Buchstaben, die die von der CHAR-Kollation der Datenbank unterstützten Sprachen darstellen
<code>SELECT DB_PROPERTY( 'Collation' );</code>	Vom Datenbankserver verwendeter CHAR-Kollationsname
<code>SELECT DB_PROPERTY( 'NcharCollation' );</code>	Vom Datenbankserver verwendeter NCHAR-Kollationsname
<code>SELECT CONNECTION_PROPERTY( 'CharSet' );</code>	CHAR-Daten-Zeichensatz des Clients
<code>SELECT CONNECTION_PROPERTY( 'NcharCharSet' );</code>	Zeichensatz von NCHAR-Daten für die Verbindung
<code>SELECT CONNECTION_PROPERTY( 'Language' );</code>	Clientsprache für die Verbindung

### Siehe auch

- „PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DB\_PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CONNECTION\_PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Sprachumgebung festlegen

Die Sprachumgebung besteht aus Sprache und Zeichensatz und wird von Datenbankserver und Clientbibliothek zum Erkennen der Umgebung verwendet. Wenn die Standardsprachumgebung Ihren Anforderungen genügt, brauchen Sie nichts zu unternehmen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

- Wenn Sie die Sprachumgebung ändern müssen, können Sie die Umgebungsvariablen SALANG und SACHARSET bzw. eine davon setzen:

```
SACHARSET=charset SALANG=language-code
```

Der *charset* ist ein gültiges Zeichensatzlabel und der *language-code* ein Sprachcode aus der Liste gültiger Sprachen.

### Ergebnisse

Die Sprachumgebung wird festgelegt.

### Siehe auch

- „Informationen zur Sprachumgebung“ auf Seite 512
- Werte der Sprachen-Labels auf Seite 510
- „SACHARSET-Umgebungsvariable“ auf Seite 472
- „SALANG-Umgebungsvariable“ auf Seite 473
- „Unterstützte Zeichensätze“ auf Seite 501
- „Hinweise zur Kollation“ auf Seite 522

## Kollationen

Eine Kollation beschreibt, wie Zeichen aus einem bestimmten Zeichensatz bzw. Kodierung sortiert und verglichen werden. SQL Anywhere unterstützt zwei Kollationsalgorithmen: Den SQL Anywhere-Kollationsalgorithmus (SACA) und den Unicode-Kollationsalgorithmus (UCA). SACA bietet eine schnelle, kompakte und vernünftige Sortierung auf Kosten der linguistischen Korrektheit. UCA bietet linguistische Korrektheit, wenn auch mit etwas erhöhten Speicheranforderungen und längerer Ausführungszeit.

Weitere Hinweise zum Erstellen einer Datenbank mit einer bestimmten Kollation finden Sie unter [„Hinweise zur Kollation“ auf Seite 522](#), [„Datenbankkollationen ändern“ auf Seite 527](#) und [„Dienstprogramm Initialisierung \(dbinit\)“ auf Seite 927](#).

Hinweise zum Anpassen der UCA-Kollation mithilfe der Syntax für die Kollationsanpassung finden Sie unter [„Optionen der Kollationsanpassung“ auf Seite 523](#).

## Kollationen in SQL Anywhere-Datenbanken

### CHAR-Kollation

Für CHAR-Datentypen wie CHAR, VARCHAR und LONG VARCHAR gibt es zwei Kollationsoptionen: den SQL Anywhere-Kollationsalgorithmus (SACA) sowie den Unicode-Kollationsalgorithmus (UCA). In beiden Fällen wird die Kollation als CHAR-Kollation bezeichnet.

### NCHAR-Kollation

Für NCHAR-Datentypen wie NCHAR, NVARCHAR und LONG NVARCHAR kann der Unicode-Kollationsalgorithmus (UCA) verwendet werden oder die UTF8BIN-Kollation mit dem SQL Anywhere-Kollationsalgorithmus (SACA).

### Berücksichtigung der Groß-/Kleinschreibung und von Akzenten wählen

Wenn beim Erstellen einer SQL Anywhere-Datenbank keine Berücksichtigung der Groß-/Kleinschreibung angegeben wurde, wird die Groß-/Kleinschreibung in der Datenbank nicht berücksichtigt. Die Berücksichtigung der Groß-/Kleinschreibung kann eingestellt werden, indem die entsprechende Option angegeben wird. Nachdem die Datenbank erstellt wurde, ist es nicht möglich, die Berücksichtigung der Groß-/Kleinschreibung zu ändern, ohne die Datenbank neu aufzubauen.

Die Berücksichtigung der Groß-/Kleinschreibung für die Datenbank legt diese bei sowohl der SACA- als auch der UCA-Kollation fest, und bestimmt daher auch die Berücksichtigung der Groß-/Kleinschreibung bei den CHAR- und NCHAR-Kollationen.

Wenn beim Erstellen einer SQL Anywhere-Datenbank keine Akzent-Berücksichtigung angegeben wurde, wird die Akzent-Berücksichtigung in der Datenbank nicht aktiviert. Die Akzentberücksichtigung kann eingestellt werden, indem die entsprechende Option angegeben wird. Nachdem die Datenbank erstellt wurde, ist es nicht möglich, die Akzentberücksichtigung zu ändern, ohne die Datenbank neu aufzubauen.

Die Akzentberücksichtigung für die Datenbank wirkt sich nur auf die UCA-Kollation aus, unabhängig davon, ob sie für die CHAR- bzw. NCHAR-Kollationen oder für beide verwendet wird. Wenn Sie SACA-Kollationen für CHAR- und NCHAR-Kollationen wählen, haben die Optionen für die Akzent-Berücksichtigung keine Auswirkungen. Die Akzent-Berücksichtigung ist ein Attribut der SACA-Kollationen und kann nicht unter Verwendung der Optionen angegeben werden, die bei der Erstellung der Datenbank zur Verfügung stehen.

## SQL Anywhere-Kollationsalgorithmus (SACA)

Der SQL Anywhere-Kollationsalgorithmus (SACA) bietet angemessene Möglichkeiten für Vergleiche, Sortierungen und Groß-/Kleinschreibungskonvertierungen von Einbyte- und Mehrbyte-Zeichensätzen. Der Algorithmus ist platzsparend und schnell. Die zugeordnete Form einer Zeichenfolge, wie z.B. ein

Index, hat dieselbe Länge wie die ursprüngliche Zeichenfolge. Die Zuordnungen für Vergleiche, Sortierungen und Groß-/Kleinschreibungskonvertierungen schlagen für jeden Bytewert in der Zeichenfolge einfach in der Tabelle nach.

### Einbyte-Zeichensätze

In einer typischen Kollation für einen Einbyte-Zeichensatz werden alle Formen eines Zeichens mit bzw. ohne Akzente demselben Wert zugeordnet, sodass die Kollation Akzente nicht berücksichtigt. Formen desselben Buchstabens mit bzw. ohne Akzente werden als genau gleich erkannt und zusammen sortiert.

Die Kollation bietet auch eine Konvertierung zwischen Groß- und Kleinbuchstaben, wobei Akzente bewahrt werden.

### Mehrbyte-Zeichensätze

In Mehrbyte-Zeichensätzen werden die Führungsbyte den 256 unterschiedlichen Werten zugeordnet. Folgebytes werden unter Verwendung ihres Binärwerts verglichen.

Bei den meisten Kollationen für Mehrbyte-Zeichensätze bietet diese Zuordnungstechnik eine annehmbare Sortierung, weil die Zeichensatzkodierung Zeichen in 256-Byte-Seiten gruppiert, die durch das Führungsbyte identifiziert werden. Die Seiten und die Zeichen auf den einzelnen Seiten sind im Zeichensatz in einer vernünftigen Reihenfolge angeordnet. Die Kollationen bewahren üblicherweise die Sortierung der Seiten (Führungsbyte) innerhalb des Zeichensatzes. Einige Seiten können anhand anderer Merkmale sortiert werden. Die 932JPN-Kollation für die japanische Codepage 932 z.B. gruppiert die Langzeichen (Kanji) und die Kurzzeichen (katakana).

Groß-/Kleinschreibungskonvertierung steht nur für englische 7-Bit-Zeichen zur Verfügung.

### UTF-8-Zeichensätze

UTF-8 ist ein Mehrbyte-Zeichensatz. Jedes Zeichen enthält ein bis vier Bytes. SQL Anywhere stellt die UTF8BIN-Kollation für die Sortierung von UTF-8-Zeichen zur Verfügung.

In UTF8BIN werden Führungsbytes 256 unterschiedlichen Werten zugeordnet, und Folgebytes werden anhand ihrer Binärwerte verglichen. Aufgrund der Darstellung von Zeichen in UTF-8 und der Begrenzung auf 256 unterschiedliche Zuordnungswerte ist es nicht möglich, verwandte Zeichen wie Formen desselben Buchstabens mit Akzent bzw. ohne Akzent zu gruppieren. Die Reihenfolge ist im Grunde binär.

Groß-/Kleinschreibungskonvertierung wird nur für englische 7-Bit-Zeichen unterstützt.

## Unicode-Kollationsalgorithmus (UCA)

Der Unicode-Kollationsalgorithmus (UCA) ist ein Algorithmus zum Sortieren des gesamten Unicode-Zeichensatzes. Er bietet linguistisch korrekte Vergleiche, Sortierungen und Groß-/Kleinschreibungskonvertierungen. Der UCA wurde als Teil des Unicode-Standards entwickelt. SQL Anywhere implementiert den UCA unter Verwendung der Open Source-Bibliothek ICU (International Components for Unicode), die von IBM entwickelt und gepflegt wird.

**Hinweis**

Die Standard-UCA-Sortierung ordnet die meisten Zeichen in den meisten Sprachen in einer passenden Reihenfolge an. Aufgrund der Sortier- und Vergleichsvariationen zwischen Sprachen, die gemeinsame Zeichen enthalten, ist der UCA nicht in der Lage, eine korrekte Sortierung bei allen Sprachen zu bieten. Aus diesem Grund bietet ICU eine Syntax zum Anpassen des UCA. Siehe „[Optionen der Kollationsanpassung](#)“ auf Seite 523.

Der UCA bietet erweiterte Möglichkeiten für Vergleiche, Sortierungen und Groß-/Kleinschreibungskonvertierungen bei geringem Platz- und Zeitaufwand.

Die zugeordnete Form einer Zeichenfolge ist länger als die ursprüngliche Zeichenfolge. Der Algorithmus stellt eine differenzierte Behandlung von komplexeren Zeichen zur Verfügung.

Im Gegensatz zum SQL Anywhere-Kollationsalgorithmus (SACA) ist der Unicode-Kollationsalgorithmus (UCA) nur für die Verwendung mit Einbyte- und UTF-8-Zeichensätzen bestimmt. Er teilt jedes Zeichen in ein oder mehrere Attribute auf. Bei Buchstaben sind diese Attribute Basiszeichen, Akzent und Groß-/Kleinschreibung.

Nicht-Buchstaben haben üblicherweise nur ein Attribut, das Basiszeichen.

UCA vergleicht Zeichenfolgen folgendermaßen:

- Die Basiszeichen vergleichen. Wenn eine Zeichenfolge von Basiszeichen sich von der anderen unterscheidet, ist der Vergleich abgeschlossen. Akzente und Groß-/Kleinschreibung werden nicht berücksichtigt.
- Wenn die Datenbank Akzente berücksichtigt, die Akzente vergleichen. Wenn sich die Akzente unterscheiden, ist der Vergleich abgeschlossen. Groß-/Kleinschreibung wird nicht berücksichtigt.
- Wenn die Datenbank die Groß-/Kleinschreibung berücksichtigt, die Groß-/Kleinschreibung von jedem Zeichen vergleichen.

Die ursprünglichen Zeichenfolgenwerte sind nur dann gleich, wenn die Basiszeichen, Akzente und die Groß-/Kleinschreibung bei beiden Zeichenfolgen gleich sind.

**Beispiel**

Nehmen wir an, UCA wird verwendet, um die Zeichenfolgen in der ersten Spalte der untenstehenden Tabelle zu vergleichen. Die nachfolgenden Spalten beschreiben die drei Attribute für jede Zeichenfolge. Beachten Sie, dass die Basiszeichen identisch sind. Die Wörter unterscheiden sich nur bei den Akzenten und der Groß-/Kleinschreibung.

Zeichenfolge	Basiszeichen	Akzente	Groß-/Kleinschreibung
noel	noel	kein, kein, kein, kein	klein, klein, klein, klein
noël	noel	kein, kein, Akzent, kein	klein, klein, klein, klein
Noel	noel	kein, kein, kein, kein	groß, klein, klein, klein

Zeichenfolge	Basiszeichen	Akzente	Groß-/Kleinschreibung
Noël	noel	kein, kein, Akzent, kein	groß, klein, klein, klein

Die folgende Tabelle zeigt die Reihenfolge, die bei den vier möglichen Kombinationen der Berücksichtigung von Akzenten und der Groß-/Kleinschreibung auftreten können, wenn UCA verwendet wird.

Akzentberücksichtigung	Groß- und Kleinschreibung	ORDER BY-Ergebnis	Erklärung
N	N	Noel, Noël, Noël, noel in beliebiger Reihenfolge	<ul style="list-style-type: none"><li>• Akzente ignoriert</li><li>• Groß-/Kleinschreibung ignoriert</li><li>• Alle Werte werden als gleich angesehen</li><li>• Zufällige Reihenfolge in der Vierergruppe</li></ul>
J	N	Noel, noel in beliebiger Reihenfolge, gefolgt von Noël, Noël beliebiger Reihenfolge	<ul style="list-style-type: none"><li>• Nicht-Akzente vor Akzenten, daher e vor ë</li><li>• Groß-/Kleinschreibung ignoriert, N und n in zufälliger Reihenfolge in jeder Zweiergruppe</li></ul>
N	J	Noel, Noël in beliebiger Reihenfolge, gefolgt von Noël, noel in beliebiger Reihenfolge	<ul style="list-style-type: none"><li>• Großbuchstaben vor Kleinbuchstaben, daher N vor n</li><li>• Akzente ignoriert, e und ë in zufälliger Reihenfolge in jeder Zweiergruppe</li></ul>
J	J	Noel  noel  Noël  noël	<ul style="list-style-type: none"><li>• Nicht-Akzente vor Akzenten, daher e vor ë</li><li>• Großbuchstaben vor Kleinbuchstaben, daher N vor n</li></ul>

## Alternative Kollationen

Die folgende Tabelle enthält Kollationen für Kompatibilitätszwecke, die mit den Funktionen SORTKEY und COMPARE verwendet werden können.

Kollationslabel	Beschreibung
874THAIBIN	Codepage 874, Windows Thailändisch, ISO8859-11, binäre Sortierung
932JPN	Codepage 932, Japanisch, Shift-JIS mit Microsoft-Erweiterungen
936ZHO	Codepage 936, vereinfachtes Chinesisch, PRC GBK 2312-80 8-Bit-Kodierung
949KOR	Codepage 949, Koreanische KS C 5601-1987-Kodierung, Wansung
950ZHO_HK	Codepage 950, Traditionelles Chinesisch, Big 5-Kodierung mit HKSCS
950ZHO_TW	Codepage 950, Traditionelles Chinesisch, Big 5-Kodierung
1250LATIN2	Codepage 1250, Windows Latin 2, Zentral-/Osteuropäisch
1250POL	Codepage 1250, Windows Latin 2, Polnisch
1251CYR	Codepage 1251, Kyrillisch
1252BIN	Codepage 1252, Windows Latin 1, binäre Sortierung
1252LATIN1	Codepage 1252, Windows Latin 1, Western
1252NOR	Codepage 1252, Windows Latin 1, Norwegisch
1252SPA	Codepage 1252, Windows Latin 1, Spanisch
1252SWEFIN	Codepage 1252, Windows Latin 1, Schwedisch/Finnisch
1253ELL	Codepage 1253, Windows Griechisch, ISO8859-7 mit Erweiterungen
1254TRK	Codepage 1254, Windows Latin 5, Türkisch, ISO 8859-9 mit Erweiterungen
1254TRKALT	Codepage 1254, Windows Türkisch, ISO8859-9 mit Erweiterungen, I mit I-Punkt gleich I ohne I-Punkt
1255HEB	Codepage 1255, Windows Hebräisch, ISO8859-8 mit Erweiterungen
1256ARA	Codepage 1255, Windows Arabisch, ISO8859-6 mit Erweiterungen
1257LIT	Codepage 1257, Litauisch
CESU8BIN	CESU-8, 8-Bit-Mehrbyte-Kodierung für Unicode, binäre Sortierung
EUC_CHINA	Vereinfachtes Chinesisch, GB 2312-80-Kodierung
EUC_JAPAN	Japanische EUC JIS X 0208-1990 und JIS X 0212-1990-Kodierung

Kollationslabel	Beschreibung
EUC_KOREA	Koreanische KS C 5601-1992-Kodierung, Johab
EUC_TAIWAN	Taiwanesische Big 5-Kodierung
ISO1LATIN1	ISO8859-1, ISO Latin 1, Western, Latin 1-Sortierung
ISO9LATIN1	ISO8859-15, ISO Latin 9, Western, Latin 1-Sortierung
ISO_1	ISO8859-1, Latin 1, Western
ISO_BINENG	Binäre Sortierung, Englisch ISO/ASCII 7-Bit Buchstaben-Fall-Zuordnungen
UCA	UCA-Standardkollation
UTF8BIN	UTF-8, 8-Bit-Mehrbyte-Kodierung für Unicode, binäre Reihenfolge

### Alternative Kollationen

Alternative Kollationen werden aus Gründen der Kompatibilität mit älteren Versionen von SQL Anywhere oder für spezielle Zwecke bereitgestellt. Um eine vollständige Liste der unterstützten alternativen Kollationen anzuzeigen, führen Sie den folgenden Befehl aus:

```
dbinit -l+
```

### Adaptive Server Enterprise-Kollationen

Die folgende Tabelle listet die unterstützten Adaptive Server Enterprise-Kollationen auf, die mit Funktionalitäten wie der SORTKEY-Funktion verwendet werden.

Beschreibung	Kollationsname	Kollations-ID
Standard Unicode multilingual	default	0
CP 850 Alternativ: Kein Akzent	altnoacc	39
CP 850 Alternativ: Kleinbuchstaben zuerst	altdict	45
CP 850 Westeuropäisch: Keine Berücksichtigung von Groß- und Kleinschreibung	altnocsp	46
CP 850 Skandinavisch lexikalisch	scandict	47
CP 850 Skandinavisch: Keine Berücksichtigung von Groß- und Kleinschreibung	scannocp	48
GB Pinyin	gbpinyin	Nicht zutreffend

Beschreibung	Kollationsname	Kollations-ID
Binäre Sortierung	binary	50
Latin-1 Englisch, Französisch, Deutsch lexikalisch	dict	51
Latin-1 Englisch, Französisch, Deutsch ohne Berücksichtigung von Groß- und Kleinschreibung	nocase	52
Latin-1 Englisch, Französisch, Deutsch ohne Bevorzugung von Groß- und Kleinschreibung	nocasep	53
Latin-1 Englisch, Französisch, Deutsch ohne Akzente	noaccent	54
Latin-1 Spanisch lexikalisch	espdict	55
Latin-1 Spanisch ohne Berücksichtigung von Groß- und Kleinschreibung	espnocs	56
Latin-1 Spanisch ohne Akzent	espnoac	57
ISO 8859-5 Russisch lexikalisch	rusdict	58
ISO 8859-5 Russisch ohne Berücksichtigung von Groß- und Kleinschreibung	rusnocs	59
ISO 8859-5 Kyrillisch lexikalisch	cyrdict	63
ISO 8859-5 Kyrillisch ohne Berücksichtigung von Groß- und Kleinschreibung	cyrnocs	64
ISO 8859-7 Griechisch lexikalisch	elldict	65
ISO 8859-2 Ungarisch lexikalisch	hundict	69
ISO 8859-2 Ungarisch ohne Akzente	hunnoac	70
ISO 8859-2 Ungarisch ohne Berücksichtigung von Groß- und Kleinschreibung	hunnocs	71
ISO 8859-5 Türkisch lexikalisch	turdict	72
ISO 8859-5 Türkisch ohne Akzente	turnoac	73
ISO 8859-5 Türkisch ohne Berücksichtigung von Groß- und Kleinschreibung	turnocs	74
CP 874 (TIS 620) Royal Thai, lexikalisch	thaidict	1

Beschreibung	Kollationsname	Kollations-ID
ISO 14651 Sortierungsstandard	14651	22
Shift-JIS binär	sjisbin	179
Unicode UTF-8 binär	utf8bin	24
EUC JIS binär	eucjisbn	192
GB2312 binäre Sortierung	gb2312bn	137
CP932 MS binär	cp932bin	129
Big5 binär	big5bin	194
EUC KSC binär	euckscbn	161

#### Siehe auch

- „COMPARE-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SORTKEY-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Was ist ICU und wann wird es benötigt?“ auf Seite 495

## Hinweise zur Kollation

Sie können die Kollation für eine Datenbank festlegen, wenn Sie die Datenbank erstellen. Die Standardkollation wird aus der Codepage und der Sprache für das Betriebssystem des Datenbankservers abgeleitet. In der Regel ist die Standardkollation eine gute Wahl. Sie können jedoch auch explizit die Kollation aus der großen Auswahl von mitgelieferten Kollationen angeben, die Ihren Anforderungen am besten entspricht. SQL Anywhere kann je Sprache mehr als eine Kollation unterstützen.

Sie sollten eine Kollation wählen, deren Zeichensatz und Sortierreihenfolge für die Daten in Ihrer Datenbank geeignet sind. Sie können auch Optionen der Kollationsanpassung als zusätzliche Steuerung bei Zeichensortierungen und -vergleichen angeben.

Beachten Sie Folgendes, wenn Sie eine Kollation für die Datenbank wählen:

- Es geht auf Kosten der Performance und führt zu einer zusätzlichen Komplexität in der Systemkonfiguration, wenn Sie eine Zeichensatzkonvertierung verwenden. Wählen Sie daher eine Kollation aus, die keine Zeichensatzkonvertierung erfordert. Es wird keine Zeichensatzkonvertierung benötigt, wenn der Datenbankserver und der Client denselben Zeichensatz verwenden.

Sie können die Zeichensatzkonvertierung vermeiden, indem Sie eine Kollationssequenz in der Datenbank verwenden, die dem Zeichensatz entspricht, der vom Betriebssystem Ihres Clientcomputers benutzt wird. Wählen Sie auf dem Clientcomputer den ANSI-Zeichensatz für Windows-Betriebssysteme.

- Wenn Ihr Computer mehrere Zeichensätze verwendet oder wenn die Datenbank Unicode-Daten speichern soll, sollten Sie die UCA- bzw. die UTF8BIN-Kollation verwenden. Die UCA-Kollation kann jedoch nicht mit anderen Mehrbyte-Zeichensätzen als UTF-8 verwendet werden.
- Wählen Sie eine Kollation, deren Zeichensatz und Sortierreihenfolge für die Daten in der Datenbank geeignet sind. Es ist häufig der Fall, dass es mehrere Kollationen gibt, die dieser Anforderung entsprechen.

### Siehe auch

- „Datenbankerstellung“ auf Seite 121
- „Empfohlene Zeichensätze und Kollationen“ auf Seite 529
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Datenbanken erstellen (Sybase Central)“ auf Seite 125
- „Datenbanken erstellen (Dienstprogramm dbinit)“ auf Seite 126

## Optionen der Kollationsanpassung

Wenn Sie bei der Erstellung einer Datenbank die UCA-Kollation auswählen, haben Sie die Möglichkeit, Optionen der Kollationsanpassung festzulegen. Wenn Sie nicht UCA als Kollation auswählen, können Sie trotzdem Anpassungssyntax verwenden, um die Berücksichtigung von Groß- und Kleinschreibung zu steuern. Sie können auch Anpassungen den Vergleich oder das Sortieren von Daten angeben, indem Sie die Funktionen COMPARE und SORTKEY verwenden.

### Schwedische Kollationsanpassung

Um eine UCA-Kollation anzupassen, damit sie den Standards der Schwedischen Akademie von 2005 entspricht, bei denen V und W als unterschiedliche Zeichen auf der Primärstufe angesehen werden, geben Sie UCA (locale=swe;sorttype=phonebook) an. Ohne sorttype=phonebook werden V und W in der schwedischen Sprachumgebung als dasselbe Zeichen angesehen.

### Japanische Kollationsanpassung

UCA unterscheidet einige Hiragana- und Katakana-Buchstaben erst auf der dritten Ebene und diese Unterschiede gehen bei Kollationen, bei denen die Groß-/Kleinschreibung nicht berücksichtigt wird, verloren. Um eine UCA-Kollation so anzupassen, dass sie auf der ersten Ebene die Unterschiede zwischen allen Hiragana-Buchstaben sowie allen Katakana-Buchstaben definiert, geben Sie UCA (locale=ja;sorttype=direct;...) an. Obwohl diese Optionen für Kollationsanpassungen keine absolut korrekte Sortierungssemantik enthalten, bieten sie eine korrekte Gleichheitssemantik.

## Übersicht über Optionen der Kollationsanpassung

Optionen der Kollationsanpassung haben die Form von Schlüsselwort/Wert-Paaren. Es folgt eine Tabelle der unterstützten Schlüsselwörter, einschließlich ihrer zulässigen Alternativformen und ihrer zulässigen Werte.

### Hinweis

Datenbanken, die mit Optionen der Kollationsanpassung erstellt wurden, können nicht mit einem Datenbankserver der Version 10.0.0 oder früher gestartet werden.

Schlüsselwort	Kollation	Alternativformen	Zulässige Werte
Locale	UCA	(keine)	Jeder gültige Sprachumgebungscode. Zum Beispiel: en.
CaseSensitivity	Alle unterstützten Kollationen	CaseSensitive, Case	<ul style="list-style-type: none"> <li>• <b>respect</b> Unterschiede in der Groß-/ Kleinschreibung von Buchstaben berücksichtigen. Bei der UCA-Kollation entspricht dies UpperFirst. Bei anderen Kollationen ist dies von der Kollation selbst abhängig.</li> <li>• <b>ignore</b> Unterschiede in der Groß-/ Kleinschreibung von Buchstaben ignorieren</li> <li>• <b>UpperFirst</b> Großbuchstaben immer an erste Stelle setzen (Aa)</li> <li>• <b>LowerFirst</b> Kleinbuchstaben immer an erste Stelle setzen (aA)</li> </ul>
AccentSensitivity	UCA	AccentSensitive, Accent	<ul style="list-style-type: none"> <li>• <b>respect</b> Akzentunterschiede bei Buchstaben berücksichtigen</li> <li>• <b>ignore</b> Akzentunterschiede bei Buchstaben ignorieren</li> <li>• <b>French</b> Französische Akzentregeln berücksichtigen</li> </ul>

Schlüsselwort	Kollation	Alternativformen	Zulässige Werte
PunctuationSensitivity	UCA	PunctuationSensitive, Punct	<ul style="list-style-type: none"> <li>• <b>ignore</b> Unterschiede bei Satzzeichen ignorieren</li> <li>• <b>primary</b> Sortierungen der ersten Stufe verwenden (nur Buchstaben berücksichtigen). Zum Beispiel: a &gt; b</li> <li>• <b>quaternary</b> Sortierungen der vierten Stufe verwenden: Buchstaben zuerst berücksichtigen, dann die Groß-/ Kleinschreibung, dann Akzent und schließlich Satzzeichen. Zum Beispiel: multiByte, multibyte, multi-byte und multi-Byte werden folgendermaßen sortiert: <ul style="list-style-type: none"> <li>○ multiByte</li> <li>○ multibyte</li> <li>○ multi-Byte</li> <li>○ multi-byte</li> </ul> <p>Sie können "quaternary" nicht für eine Datenbank angeben, in der Akzente und Groß- und Kleinschreibung nicht berücksichtigt werden.</p> </li> </ul>

Schlüsselwort	Kollation	Alternativformen	Zulässige Werte
SortType	UCA	(keine)	<p>Der zu verwendende Sortiertyp. Zu den möglichen Werten gehören:</p> <ul style="list-style-type: none"> <li>• phonebook</li> <li>• traditional</li> <li>• standard</li> <li>• pinyin</li> <li>• stroke</li> <li>• direct</li> <li>• posix</li> <li>• big5han</li> <li>• gb2312han</li> </ul> <p>Weitere Informationen zu diesen Sortiertypen finden Sie unter "Unicode Technical Standard #35" auf der Website <a href="http://www.unicode.org/reports/tr35/">http://www.unicode.org/reports/tr35/</a>.</p>

**Siehe auch**

- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „COMPARE-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SORTKEY-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Auswahl der Standardkollation für neue SQL Anywhere-Datenbanken

Wenn eine Datenbank erstellt wird und keine Kollation explizit angegeben wird, verwendet SQL Anywhere die Sprache und den Zeichensatz, um die Kollation zu bestimmen.

- Die Sprache kommt von der Umgebungsvariablen SALANG (falls vorhanden), der Registrierung oder dem Betriebssystem.
- Der Zeichensatz kommt von der Umgebungsvariablen SCHARSET (falls vorhanden) oder dem Betriebssystem.

**Siehe auch**

- „SALANG-Umgebungsvariable“ auf Seite 473
- „SCHARSET-Umgebungsvariable“ auf Seite 472

## Die Standardkollation bestimmen

Eine Kollation beschreibt, wie Zeichen aus einem bestimmten Zeichensatz bzw. Kodierung sortiert und verglichen werden. Wenn Sie beim Erstellen einer Datenbank nicht ausdrücklich eine Kollation angeben, wird eine Standardkollation verwendet, die vom Betriebssystem abhängt.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie die folgende Anweisung aus:

```
SELECT PROPERTY( 'DefaultCollation' );
```

### Ergebnisse

Die Standardkollation für die Datenbank wird zurückgegeben.

### Siehe auch

- „Hinweise zur Kollation“ auf Seite 522
- „Zeichensätze“ auf Seite 497

## Datenbankkollationen ändern

Sie können die Datenbankkollation von einer Kollation in eine andere ändern, indem Sie die Datenbank entladen und in die gewünschte Kollation neu laden. Kollationen werden zum Zeitpunkt der Datenbankerstellung gewählt und können nicht geändert werden, ohne die Datenbank neu aufzubauen.

### Voraussetzungen

Sie müssen die Systemprivilegien SELECT ANY TABLE und SERVER OPERATOR haben.

Standardmäßig benötigen Sie zum Ausführen einer UNLOAD-Anweisung das SELECT ANY TABLE-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gl geändert werden.

### Aufgabe

1. Starten Sie die Datenbank:

```
START databasefile
```

2. Ermitteln Sie folgendermaßen den Zeichensatz für die vorhandene Datenbank:

```
SELECT DB_PROPERTY( 'CharSet' );
```

Bei frühen Versionen von SQL Anywhere ist diese Eigenschaft möglicherweise nicht vorhanden. Der Zeichensatz ist aus dem Kollationsnamen ableitbar. Beispiel: 1252LATIN1-Kollation verwendet Codepage 1252.

Der Zeichensatz in der vorhandenen Datenbank muss mit den Zeichensätzen von Betriebssystem und Client übereinstimmen oder zumindest kompatibel sein. Wenn dies nicht der Fall ist, bietet dies eine gute Gelegenheit, die Datenbank neu aufzubauen, was allerdings mit größter Umsicht geschehen muss.

Insbesondere gilt: Wenn Sie eine Datenbank mit 1252LATIN1-Kollation in früheren Versionen von SQL Anywhere verwendet haben, die die Zeichensatzkonvertierung entweder nicht unterstützen (Version 5 und früher) oder standardmäßig deaktiviert haben (Versionen 6 und 7), und Ihre Clientanwendungen normale Windows-Anwendungen waren, haben Sie möglicherweise Codepage 1252-Zeichendaten in einer Datenbank, die Daten gemäß Codepage 850 interpretiert.

3. Ermitteln Sie den Zeichensatz für die Daten in der vorhandenen Datenbank:

```
UNLOAD TABLE mytable TO 'mytable-data-in-utf8.dat' ENCODING 'UTF-8';
```

Zeigen Sie die Ergebnisse in einem Texteditor an.

Wenn Daten mit Akzenten korrekt angezeigt werden, entsprechen die Zeichendaten in der Datenbank der ANSI-Codepage für Windows, die für Englisch und andere westeuropäische Sprachen Codepage 1252 ist. Wenn die Daten in einem DOS-basierten Editor korrekt angezeigt werden, entsprechen die Daten der OEM-Codepage für Windows, die wahrscheinlich 437 oder 850 ist.

4. Entladen Sie die Datenbank.

Wenn der Datenzeichensatz mit dem Zeichensatz der Datenbank inkompatibel ist, müssen die Daten unbedingt ohne Zeichensatzkonvertierung entladen werden. Je nachdem, mit welcher Version von SQL Anywhere Sie arbeiten, können Sie die interne Entladefunktion von `dbunload` verwenden oder die Daten mithilfe der `UNLOAD TABLE`-Anweisung manuell entladen.

5. Erstellen Sie die neue Datenbank unter Angabe der Kollationen und Zeichensätze, die Sie verwenden möchten, und legen Sie DBA-Benutzer-ID und DBA-Kennwort auf "DBA" und "sql" fest:

```
dbinit -dba DBA,sql -z 1252LATIN1 c:\newdatabase.db
```

6. Stoppen Sie den alten Datenbankserver und starten Sie den neuen Datenbankserver:

```
dbsrv16 -n new-server c:\newdatabase.db
```

7. Laden Sie die Daten in die neue Datenbank.

Wenn die entladenen Daten und das Schema (*reload.sql*) dem Zeichensatz des Computers entsprechen, auf dem das Neuladen durchgeführt wird, können Sie die externe Neuladefunktion von `dbunload` verwenden. Die Daten werden automatisch in den korrekten Datensatz für die Datenbank konvertiert. Zum Beispiel:

```
dbunload -ix c:\databasefile
```

Wenn die Kodierung der Daten nicht dem Zeichensatz der Datenbank entspricht und Sie die Daten mithilfe von `LOAD TABLE`-Anweisungen laden (internes Neuladen), müssen Sie die `ENCODING`-

Klausel verwenden, weil der Datenbankserver standardmäßig keine Zeichensatzkonvertierung für Daten durchführt, die mit LOAD TABLE-Anweisungen geladen werden.

Wenn die Kodierung der Daten nicht der Codepage auf dem Computer entspricht, mit dem Sie arbeiten, und Sie mithilfe von INPUT-Anweisungen laden (externes Neuladen), müssen Sie die ENCODING-Klausel verwenden, weil der Datenbankserver sonst annimmt, dass die Daten im systemeigenen Zeichensatz des Computers vorliegen.

## Ergebnisse

Die Datenbank wird mit der neuen Kollation neu erstellt.

## Beispiel

Nehmen Sie beispielsweise an, Sie haben eine Datenbank mit ISO1LATIN1-Kollation und stellen fest, dass Sie das Euro-Währungssymbol unterstützen müssen. Da ISO1LATIN1 im Gegensatz zu anderen europäischen Zeichensätzen wie 1252LATIN1 das Euro-Symbol nicht unterstützt, können Sie Ihre Datenbank entladen, eine neue Datenbank mit 1252LATIN1 erstellen und Ihre Datenbank neu laden.

Weitere Hinweise finden Sie unter [Changing the Collation and Codepage When Rebuilding a SQL Anywhere Database](#).

## Siehe auch

- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UNLOAD-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „INPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Hinweise zur Kollation“ auf Seite 522
- „Dienstprogramm zum Entladen (dbunload)“ auf Seite 1000
- „Neuaufbau von Datenbanken“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Verbindungsparameter CharSet (CS)“ auf Seite 343
- „Datenbankserveroption -gl“ auf Seite 242

## Empfohlene Zeichensätze und Kollationen

SQL Anywhere erkennt die Namen von mehreren hundert Zeichensätzen, Codepages, Kodierungen und Kollationen. In diesem Thema werden diejenigen aufgelistet, die je nach verwendeter Sprache für Windows- und Unix-Plattformen empfohlen werden.

Rufen Sie mithilfe der dbinit-Option -le eine Liste aller verfügbaren Zeichensatzlabels für eine SQL Anywhere-Datenbank ab. Verwenden Sie die dbinit-Option -l, um eine Liste aller verfügbaren Kollationen für eine SQL Anywhere-Datenbank abzurufen. Siehe „[Dienstprogramm Initialisierung \(dbinit\)](#)“ auf Seite 927.

Wenn eine Zeichensatzkodierung oder ein Label angegeben werden muss, verwenden Sie den Wert aus der Spalte "Zeichensatzlabel" oder eines der mithilfe der dbinit-Option -le aufgelisteten Labels. Wenn eine Kollation angegeben werden muss, verwenden Sie den Wert aus der Spalte "Kollation" oder "Alternative Kollation" oder eines der mithilfe der dbinit-Option -l aufgelisteten Labels.

**Hinweis**

Unter Mac OS X und bei Sprachen, die nicht in den nachfolgenden Tabellen enthalten sind, sollte die UTF-8-Kodierung mit UCA- oder UTF8BIN-Kollation verwendet werden.

**Windows-Plattformen**

<b>Sprache</b>	<b>Windows-Codepages</b>	<b>Zeichensatzlabel</b>	<b>Kollation</b>	<b>Alternative Kollation</b>
Arabisch	1256	Windows-1256	1256ARA	
Zentral- und Osteuropäisch	1250	Windows-1250	1250LATIN2	
Dänisch	1252	Windows-1252	1252LATIN1	
Holländisch	1252	Windows-1252	1252LATIN1	
Englisch	1252	Windows-1252	1252LATIN1	
Finnisch	1252	Windows-1252	1252SWEFIN	
Französisch	1252	Windows-1252	1252LATIN1	
Deutsch	1252	Windows-1252	1252LATIN1	
Griechisch	1253	Windows-1253	1253ELL	
Hebräisch	1253	Windows-1253	1255HEB	
Italienisch	1252	Windows-1252	1252LATIN1	
Japanisch	932	Windows-31J	932JPN	
Koreanisch	949	IBM949	949KOR	
Litauisch	1257	Windows-1257	1257LIT	
Norwegisch	1252	Windows-1252	1252NOR	
Polnisch	1250	Windows-1250	1250POL	
Portugiesisch	1252	Windows-1252	1252LATIN1	
Russisch	1251	Windows-1251	1251CYR	
Vereinfachtes Chinesisch	936	GBK	936ZHO	
Spanisch	1252	Windows-1252	1252SPA	

<b>Sprache</b>	<b>Windows-Codepages</b>	<b>Zeichensatzlabel</b>	<b>Kollation</b>	<b>Alternative Kollation</b>
Schwedisch	1252	Windows-1252	1252SWEFIN	
Thailändisch	874	TIS-620	874THAIBIN	
Traditionelles Chinesisch - Hongkong	950	Big5-HKSCS	950ZHO_HK	
Traditionelles Chinesisch - Taiwan	950	Big5	950ZHO_TW	
Türkisch	1254	Windows-1254	1254TRK	1254TRKALT
Ukrainisch	1251	Windows-1251	1251CYR	
Westeuropäisch	1252	Windows-1252	1252LATIN1	

### Unix-Plattformen

<b>Sprache</b>	<b>Zeichensatzlabel</b>	<b>Kollation</b>	<b>Alternative Kollation</b>
Arabisch	ISO_8859-6:1987	UCA	
Zentral- und Osteuropäisch	ISO_8859-2:1987	UCA	
Dänisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Holländisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Englisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Finnisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Französisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Deutsch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Griechisch	ISO_8859-7:1987	UCA	
Hebräisch	ISO_8859-8:1988	UCA	
Italienisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Japanisch	EUC-JP <sup>1</sup>	EUC_JAPAN	
Koreanisch	EUC-KR	EUC_KOREA	

Sprache	Zeichensatzlabel	Kollation	Alternative Kollation
Litauisch	(UTF-8 verwenden)	UCA oder UTF8BIN	
Norwegisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Polnisch	ISO_8859-2:1987	UCA	
Portugiesisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Russisch	ISO_8859-5:1988	UCA	
Vereinfachtes Chinesisch	GB2312	EUC_CHINA	
Spanisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Schwedisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1
Thailändisch	(UTF-8 verwenden)	UCA oder UTF8BIN	
Traditionelles Chinesisch - Hong-kong	Big5-HKSCS	950ZHO_HK	950TWN
Traditionelles Chinesisch - Taiwan	EUC-TW	EUC_TAIWAN	
Traditionelles Chinesisch - Taiwan	Big5	950ZHO_TW	
Türkisch	ISO_8859-9:1989	920TRK	
Ukrainisch	ISO_8859-5:1988	UCA	
Westeuropäisch	ISO-8859-15	ISO9LATIN1	ISO1LATIN1

<sup>1</sup> EUC-JP ist ein alternatives Label für das SQL Anywhere-Label Extended\_UNIX\_Code\_Packed\_Format\_for\_Japanese.

## Türkische Zeichensätze und Kollationen

Die türkische Sprache kennt zwei Formen des Buchstabens, der uns als **I** erscheint. Eine Form, genannt **I-dot**, erscheint folgendermaßen:

**ı, İ**

Die zweite Form, genannt **I-no-dot**, erscheint folgendermaßen:

**ı, İ**

Auch wenn diese beiden Buchstaben als Varianten ein und desselben Buchstabens erscheinen, werden sie im türkischen Alphabet als verschiedene Buchstaben behandelt. SQL Anywhere stellt die türkische Kollation 1254TRK bereit, um diese Variationen zu unterstützen.

Die türkischen Regeln für die Groß-/Kleinschreibungs-Konvertierung sind nicht kompatibel mit den entsprechenden ANSI SQL-Standardregeln. Im Türkischen ist z.B. das Kleinbuchstaben-Äquivalent von İ:

**ı**

Im ANSI-Standard dagegen ist es:

**i**

Aus diesem Grunde hängt die korrekte Groß-/Kleinschreibungs-Konvertierung davon ab, ob für den zu vergleichenden Text türkisches oder englisches ANSI festgelegt ist. In vielen Fällen ist es nicht möglich diese Unterscheidung zu treffen, was in den betroffenen Datenbanken zu nicht standardmäßigem Verhalten führt.

Nehmen wir z.B. folgende Anweisungen, die in einer Datenbank ausgeführt werden, die die 1254TRK-Kollation verwendet:

```
SELECT * FROM syshistory    //actual table name is SYSHISTORY
SELECT * FROM fig          //actual name is FİG
```

Die erste Anweisung referenziert ein Systemobjekt, und ANSI SQL-Konvertierungsregeln sind für die Namensabgleichung erforderlich. Die zweite Anweisung referenziert ein Benutzerobjekt, und türkische Konvertierungsregeln sind für die Namensabgleichung erforderlich. Der Datenbankserver kann jedoch erst bestimmen, welche Konvertierungsregeln er verwenden soll, wenn er erkennt, um welches Objekt es sich handelt. Dabei erkennt er das Objekt erst, wenn er weiß, welche Konvertierungsregeln er verwenden soll. Weder für System- noch für Benutzerobjekte kann diese Situation zufriedenstellend aufgelöst werden. Da der Datenbankserver in diesem Beispiel die türkische Kollation 1254TRK verwendet, schlägt die erste Anweisung fehl, weil ein kleines "ı" nicht als äquivalent zu einem großen "İ" angesehen wird. Die zweite Anweisung führt zum Erfolg.

Die Inkompatibilität des türkischen Standards und des ANSI-Standards erfordert, dass Referenzen auf Systemobjekte in türkischen Datenbanken den Objektnamen korrekt in Groß- bzw. Kleinbuchstaben wiedergeben, d.h. so, wie bei der Erstellung des Objektes. Die erste Anweisung oben müsste folgendermaßen geschrieben werden:

```
SELECT * FROM SYSHISTORY
```

Genau genommen muss nur der Buchstabe "İ" in der korrekten Groß-/Kleinschreibung angegeben werden.

Als Alternative wäre es akzeptabel, wenn auch ungewöhnlich, die Anweisung folgendermaßen zu schreiben:

```
SELECT * FROM syshistory //I-no-dot
```

Bei Schlüsselwörtern wie INSERT wird die Groß-/Kleinschreibung auch in türkischen Datenbanken nicht berücksichtigt. SQL Anywhere weiß, dass alle Schlüsselwörter nur englische Buchstaben verwenden, daher werden ANSI-Konvertierungsregeln für die Groß-/Kleinschreibung bei der Abgleichung von Schlüsselwörtern verwendet. SQL Anywhere wendet dieses Wissen auch bei bestimmten anderen Bezeichnungen an, wie z.B. bei integrierten Funktionen. Objekte, deren Namen im Katalog gespeichert werden, müssen jedoch in der korrekten Groß-/Kleinschreibung angegeben werden, wie oben beschrieben. Um die korrekte Schreibweise zu ermitteln, suchen Sie zunächst in der Systemansicht, die das Systemobjekt definiert.

### Siehe auch

- „Systemansichten“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Daten in türkischen Datenbanken, in denen die Groß-/Kleinschreibung nicht berücksichtigt wird

Ähnliche Regeln gelten bei türkischen Datenbanken, in denen die Groß-/Kleinschreibung nicht berücksichtigt wird. Nehmen Sie beispielsweise den folgenden Datenwert:

**FIG**

In diesem Fall muss ein Verweis auf diese Daten in Kleinbuchstaben wie folgt aussehen:

**fig**

So wird in beiden Formen dasselbe I-Punkt-Zeichen verwendet.

## Alternative türkische Kollation 1254TRKALT

Einigen Anwendungsentwicklern kann das Problem mit dem türkischen "I" erhebliche Schwierigkeiten bereiten. Die korrekte Lösung besteht darin, sicherzustellen, dass alle Objektreferenzen in der korrekten Groß-/Kleinschreibung vorliegen oder dass die richtige Form des Buchstabens I verwendet wird. Es kann jedoch sinnvoller sein, zugunsten der ANSI-Regeln gegen die türkischen Regeln zu verstoßen.

SQL Anywhere stellt die 1254TRKALT-Kollation bereit, die mit 1254TRK identisch ist, bis auf die Tatsache, dass "I-Punkt" und "I-ohne-Punkt" als äquivalente Zeichen behandelt werden.

Es ist wichtig, die Konsequenz dieser Änderung zu verstehen. In einer 1254TRKALT-Datenbank sind die folgenden Zeichenfolgen gleichwertig:

```
fig
fig
```

Dies ist zwar für türkische Benutzer nicht korrekt, kann jedoch für andere Benutzer akzeptabel sein.

Das zweite Problem taucht auf, wenn ORDER BY benutzt wird. Sehen Sie sich die folgenden Zeichenfolgen an:

```
ia
ia
is
is
```

In einer 1254TRK-Datenbank würde eine ORDER BY-Klausel bei diesen Zeichenfolgen Folgendes bewirken:

```
ia
is
ia
is
```

Und zwar, weil "I-ohne-Punkt" in der alphabetischen Folge vor "I-Punkt" steht. In einer 1254TRKALT-Datenbank ergäbe sich folgende Reihenfolge:

```
ia
ia
is
is
```

Und zwar, weil "I-ohne-Punkt" gleichwertig ist mit "I-Punkt".

## Login-Richtlinien

Eine **Login-Richtlinie** besteht aus einer Reihe von Regeln, die angewendet werden, wenn Sie eine Datenbankverbindung für einen Benutzer erstellen. Login-Richtlinien steuern nur die Regeln für Benutzer-Logins und sind von Rollen und Privilegien getrennt. Login-Richtlinien werden nicht geerbt. Allen Benutzern in einer Datenbank wird eine Login-Richtlinie zugeordnet.

Sie können Login-Richtlinien erstellen, bearbeiten und löschen. Außerdem können Sie Benutzer erstellen, bearbeiten und löschen sowie ihnen Login-Richtlinien zuordnen. Mit der sa\_get\_user\_status-Systemprozedur können Sie Informationen zum aktuellen Status eines Benutzers abrufen, einschließlich der Login-Richtlinie.

## Vererbung von Login-Richtlinieneinstellungen

Eine Standard-Login-Richtlinie namens **Root** wird in der Datenbank gespeichert und enthält die Standard-Optionswerte für alle Richtlinien. Wenn Sie andere Einstellungen als die Standardwerte verwenden möchten, können Sie entweder die Root-Richtlinie ändern oder eine Richtlinie erstellen und diese anschließend so ändern, dass sie Aufhebungen für die Standardwerte enthält. Eine Richtlinie übernimmt Standardeinstellungen von der Root-Richtlinie, außer sie wird geändert, um Aufhebungen zu enthalten.

Beispiel: Angenommen, der Root-Richtlinienwert für `max_connections` ist 5. Sie erstellen eine Richtlinie namens "myPolicy" und ändern sie, um `max_connections` auf "Unbegrenzt" zu setzen. Anschließend erstellen Sie einen Benutzer und ordnen ihm die Login-Richtlinie "myPolicy" zu. Wenn der Benutzer sich anmeldet, werden seine Login-Richtlinien-Optionseinstellungen von der Root-Login-Richtlinie abgeleitet, ausgenommen `max_connections`, deren Wert auf "Unbegrenzt" gesetzt ist.

Es ist wichtig, das Konzept der Vererbung von Standardwerten der Root-Richtlinie zu verstehen, weil eine nachfolgende Änderung des Werts einer Optionseinstellung in der Root-Richtlinie sich auf Benutzer von Richtlinien auswirkt, die vom Standardwert für diese Einstellung abhängen. Gleichmaßen gilt: Wenn ein Root-Wert geändert wird, wirkt sich das nicht auf Benutzer von Richtlinien aus, die diese Einstellung außer Kraft setzen.

### Siehe auch

- „CREATE LOGIN POLICY-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER LOGIN POLICY-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DROP LOGIN POLICY-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_get\_user\_status-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_get\_user\_status-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Root-Login-Richtlinie

Alle neuen Datenbanken enthalten die **root**-Login-Richtlinie. Sie können die Werte für die Optionen der Root-Login-Richtlinie ändern, jedoch nicht die Richtlinie löschen.

Einem Benutzerkonto wird die "root"-Login-Richtlinie unter folgenden Bedingungen zugeordnet:

- Wenn Sie einen neuen Benutzer erstellen und keine Login-Richtlinie angeben
- Wenn Sie das Entladedienstprogramm (dbunload) verwenden, um eine Datenbank neu aufzusetzen, die von einer früheren Version von SQL Anywhere erstellt wurde.
- Wenn Sie ein Upgrade einer SQL Anywhere Version 10-Datenbank durchführen, indem Sie das Dienstprogramm zum Upgrade (dbupgrad) oder die Anweisung ALTER DATABASE UPGRADE verwenden.

### Login-Richtlinienoptionen und Standardwerte

Die folgende Tabelle enthält die Optionen, die durch eine Login-Richtlinie gesteuert werden, sowie die Standardwerte für die **root**-Login-Richtlinie:

Richtlinienoptionsname	Beschreibung	Standardwert	Gilt für:
auto_unlock_time	Die Zeitspanne, nach der gesperrte Konten automatisch freigegeben werden.	Unlimited	Alle Benutzer außer denjenigen mit MANAGE ANY USER-Systemprivileg
change_password_dual_control	Wenn der Wert für diese Option ON ist, muss das Kennwort von zwei Administratoren festgelegt werden.  Die Einstellung für die verify_password_function-Option wird ignoriert, wenn diese Option auf ON gesetzt ist, weil das Kennwort separat in zwei Teilen konfiguriert wird. Es wird keine Überprüfung durchgeführt.	OFF	Alle Benutzer
ldap_primary_server	Der Name des LDAP-Primärservers.	(keiner)	Alle Benutzer
ldap_secondary_server	Der Name des LDAP-Sekundärservers.	(keiner)	Alle Benutzer
ldap_auto_failback_period	Die Zeitspanne in Minuten, nach der ein automatischer Failback auf den Primärserver versucht wird.	15 Minuten	Alle Benutzer
ldap_failover_to_std	Angabe, ob die Authentifizierung mit Standardauthentifizierung zulässig sein soll, wenn die Authentifizierung über den LDAP-Server fehlschlägt, weil der Distinguished Name (DN) für einen Benutzer nicht gefunden wird, Systemressourcen fehlen bzw. Netzwerkausfälle, Verbindungs-Timeouts oder ähnliche Systemfehler auftreten. Diese Einstellung lässt nicht zu, dass bei Rückgabe eines tatsächlichen Authentifizierungsfehlers durch einen LDAP-Server ein Failover auf die Standardauthentifizierung erfolgt (wie es der Fall ist, wenn der Benutzer gefunden wird, aber das angegebene Kennwort nicht passt).	ON	Alle Benutzer

Richtlinienoptionsname	Beschreibung	Standardwert	Gilt für:
ldap_refresh_dn	<p>Zum Zeitpunkt der Festlegung dieser Richtlinienoption durch eine CREATE LOGIN POLICY- oder ALTER LOGIN POLICY-Anweisung wird der aktuelle Zeitwert mit der Login-Richtlinie gespeichert. Dieser Wert ist der Zeitstempel, der bei der Benutzerauthentifizierung mit dem in ISYSUSER für den betreffenden Benutzer gefundenen user_dn_cached_at-Wert verglichen wird. Wenn der Wert in der Richtlinie neuer ist als der user_dn_cached_at-Wert in ISYSUSER, wird nach dem Distinguished Name (DN) eines Benutzers gesucht, um den user_dn-Wert in ISYSUSER zu aktualisieren.</p> <p>Der Wert NOW ist der einzige gültige Wert, der dieser Richtlinienoption zugeordnet werden kann. Alle anderen führen zu einer Fehlermeldung. Der Wert wird in der Coordinated Universal Time (UTC) angegeben und als Zeichenfolge im Standardformat des Servers gespeichert.</p>	(keiner)	Alle Benutzer
locked	Wenn der Wert für diese Option ON ist, dürfen die Benutzer keine neuen Verbindungen mehr herstellen. Die reason_locked-Spalte der sa_get_user_status-Systemprozedur gibt eine vom Datenbankserver erstellte Zeichenfolge zurück, die anzeigt, warum ein Benutzer gesperrt ist.	OFF	Alle Benutzer außer denjenigen mit MANAGE ANY USER-Systemprivileg
max_connections	Die maximale Anzahl gleichzeitiger Verbindungen, die einem Benutzer gestattet sind.	Unlimited	Alle Benutzer außer denjenigen mit SERVER OPERATOR- oder DROP CONNECTION-Systemprivileg

Richtlinienoptionsname	Beschreibung	Standardwert	Gilt für:
max_failed_login_attempts	Die maximale Anzahl fehlgeschlagener Login-Versuche seit dem letzten erfolgreichen Versuch, bevor der Benutzer gesperrt wird. Benutzer mit SYS_AUTH_DBA_ROLE-Kompatibilitätsrolle werden freigegeben, wenn seit dem letzten gescheiterten Login-Versuch eine Minute vergangen ist.	Unlimited	
max_days_since_login	Die maximale Anzahl von Tagen zwischen erfolgreichen Logins durch denselben Benutzer.	Unlimited	Alle Benutzer außer denjenigen mit MANAGE ANY USER-Systemprivileg
max_non_dba_connections	Die maximale Anzahl gleichzeitiger Verbindungen, die Benutzer herstellen können. Diese Option wird nur bei der Root-Login-Richtlinie verwendet.	Unlimited	Alle Benutzer außer denjenigen mit SERVER OPERATOR- oder DROP CONNECTION-Systemprivileg
password_life_time	Die maximale Anzahl von Tagen, bis ein Kennwort geändert werden muss	Unlimited	Alle Benutzer
password_grace_time	Die Anzahl der Tage bis zum Kennwortablauf. Das Login ist möglich, aber die Standardprozedur post_login gibt Warnungen aus.	0	Alle Benutzer
password_expiry_on_next_login	Wenn der Wert für diese Option ON ist, läuft das Kennwort des Benutzers nach dem nächsten Login ab.	OFF	Alle Benutzer

Richtlinienoptionsname	Beschreibung	Standardwert	Gilt für:
root_auto_unlock_time	Die Zeitspanne, nach der gesperrte Konten automatisch freigegeben werden. Diese Option wird nur von der Root-Login-Richtlinie unterstützt.	1 Minute	Benutzer mit MANAGE ANY USER-Systemprivileg

#### Siehe auch

- „ALTER LOGIN POLICY-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Automatisches Entsperrern von Benutzerkonten“ auf Seite 544
- „Kennwörter für die Doppelkontrolle festlegen (SQL)“ auf Seite 1370

## Neue Login-Richtlinien erstellen

Erstellen Sie benutzerdefinierte Login-Richtlinien auf Basis der Root-Login-Richtlinie.

#### Voraussetzungen

Sie müssen das MANAGE ANY LOGIN POLICY-Systemprivileg haben.

#### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Login-Richtlinien** und klicken Sie dann auf **Neu » Login-Richtlinie**.
3. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen einer Login-Richtlinie**.

#### Ergebnisse

Eine neue Login-Richtlinie wird erstellt.

#### Nächste Schritte

Ordnen Sie die neue Login-Richtlinie einem Benutzer zu.

#### Siehe auch

- „CREATE LOGIN POLICY-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Login-Richtlinien vorhandenen Benutzern zuordnen“ auf Seite 541
- „Login-Richtlinien ändern“ auf Seite 541

## Login-Richtlinien vorhandenen Benutzern zuordnen

Wenn Sie die einem Benutzer zugeordnete Login-Richtlinie ändern möchten, ordnen Sie dem Benutzer eine neue Login-Richtlinie zu. Allen Benutzern ist eine Login-Richtlinie zugeordnet. Sie können die Login-Richtlinie nicht aus einem Benutzer löschen, sondern nur die dem Benutzer zugeordnete Login-Richtlinie ändern.

### Voraussetzungen

Sie müssen das **MANAGE ANY USER**-Systemprivileg haben.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **Benutzer**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf einen Benutzer und klicken Sie dann auf **Datei » Login-Richtlinie festlegen**.
4. In der Liste **Login-Richtlinie** wählen Sie eine Login-Richtlinie aus.
5. Klicken Sie auf **OK**.

### Ergebnisse

Die Login-Richtlinie des Benutzers wird neu zugeordnet. Die Einstellungen treten sofort in Kraft.

### Siehe auch

- „**ALTER USER**-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Login-Richtlinien ändern

Wenn Sie eine Login-Richtlinie bearbeiten möchten, ändern Sie ihre Optionen. Sie können jede Login-Richtlinie bearbeiten, einschließlich der Root-Login-Richtlinie.

### Voraussetzungen

Sie müssen das **MANAGE ANY LOGIN POLICY**-Systemprivileg haben.

### Kontext und Bemerkungen

#### Hinweis

Wenn Sie den Wert einer Optionseinstellung in der Root-Login-Richtlinie ändern, hat dies Auswirkungen auf alle Benutzer, die auf diesen Standardwert angewiesen sind und denen die Root-Login-Richtlinie zugeordnet ist. Umgekehrt sind keine Benutzer betroffen, die benutzerdefinierten Login-Richtlinien mit Aufhebungen für diese Einstellung zugeordnet sind.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Im linken Fensterausschnitt klicken Sie auf **Login-Richtlinien**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf einen Benutzer und klicken Sie auf **Eigenschaften**.

Wenn Sie die Root-Login-Richtlinie ändern möchten, rechtsklicken Sie auf **Root** und klicken Sie dann auf **Eigenschaften**.

4. Ändern Sie die Richtlinienwerte und klicken Sie dann auf **OK**.

### Ergebnisse

Die Login-Richtlinie wird geändert. Die Einstellungen treten sofort in Kraft.

### Siehe auch

- [Login-Richtlinienoptionen und Standardwerte auf Seite 536](#)
- [„ALTER LOGIN POLICY-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Login-Richtlinien vorhandenen Benutzern zuordnen“ auf Seite 541](#)

## Login-Richtlinien löschen

Sie können jede benutzerdefinierte Login-Richtlinie löschen, die keinem Benutzer zugeordnet ist. Die Root-Login-Richtlinie kann nicht gelöscht, aber bearbeitet werden.

### Voraussetzungen

Sie müssen das **MANAGE ANY LOGIN POLICY**-Systemprivileg haben.

Sie können eine Login-Richtlinie nicht löschen, wenn sie noch einem Benutzer zugeordnet ist. Sie müssen Benutzer einer anderen Login-Richtlinie zuordnen, bevor Sie eine angepasste Login-Richtlinie löschen.

Die Root-Login-Richtlinie kann nicht gelöscht werden.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Im linken Fensterausschnitt klicken Sie auf **Login-Richtlinien**.
3. Rechtsklicken Sie im Fensterausschnitt **Login-Richtlinien** auf eine Login-Richtlinie und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Ja**.

## Ergebnisse

Die Login-Richtlinie wird gelöscht.

### Siehe auch

- „DROP LOGIN POLICY-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Login-Richtlinienverwaltung für schreibgeschützte Datenbanken

Wenn Sie eine Datenbank im schreibgeschützten Modus starten, basieren die Login-Richtlinien auf dem jeweiligen beständigen Zustand der Datenbank. Die Auswirkung von Login-Richtlinien, die Sie zuordnen, beschränkt sich auf die aktuelle Sitzung.

Wenn die Login-Verwaltung in einer Datenbank aktiviert ist, die Sie später im schreibgeschützten Modus starten, gelten die folgenden Einschränkungen:

- Die Login-Verwaltung durch den Datenbankserver basiert auf dem Status der Datenbank vor ihrem Start.
- Explizite Anweisungen, die den Status der Datenbank ändern, werden abgelehnt und ergeben einen Fehler.
- Der Datenbankserver verwaltet weiterhin für jeden Benutzer dynamische Informationen wie `failed_login_attempts` und `last_login_time`. Diese Informationen werden allerdings im flüchtigen Speicher aufrechterhalten und gehen verloren, wenn Sie die Datenbank herunterfahren. Die Datenbank kehrt in den Status zurück, den sie vor ihrem Start hatte.
- Wenn das Konto durch die bestehende Login-Verwaltungsrichtlinie gesperrt ist, kann sich ein Benutzer nicht anmelden. Überdies stehen auch die üblichen Methoden zum Ändern eines Kennworts während des Anmeldens nicht zur Verfügung.
- Wenn die Datenbank aufgrund ihrer Rolle als Spiegeldatenbank in einem System mit hoher Verfügbarkeit schreibgeschützt ist, wirkt sich eine Anweisung in der Primärdatenbank auch in der Spiegeldatenbank aus. Die auf dem Primärserver gesammelten dynamischen Informationen werden an die Spiegeldatenbank gesendet und mit den für die Spiegeldatenbank im Zwischenspeicher gesammelten Informationen zusammengeführt.
- Wenn die Datenbank aufgrund ihrer Rolle als Spiegeldatenbank in einem System mit hoher Verfügbarkeit oder als Kopierknoten in einem Scale-Out-System mit Schreibschutz schreibgeschützt ist, dann werden die Auswirkungen aller in der Primärdatenbank ausgeführten Anweisungen auch in der schreibgeschützten Datenbank widerspiegelt. Die auf dem Primärserver gesammelten dynamischen Informationen werden an die schreibgeschützte Datenbank gesendet und mit den für die schreibgeschützte Datenbank im Zwischenspeicher gesammelten Informationen zusammengeführt.

## Automatisches Entsperren von Benutzerkonten

Eine Sperrung einiger oder aller Dienste einer Datenbank kann eintreten, wenn alle Administrator-Benutzer mit `MANAGE ANY USER`-Systemprivileg aufgrund fehlgeschlagener Login-Versuche aus der Datenbank ausgesperrt sind.

Ein Benutzerkonto wird automatisch gesperrt, wenn der Benutzer die in der Login-Richtlinie festgelegten maximal zulässigen Login-Versuche (`max_failed_login_attempts`) überschreitet. Nach dem Sperren muss das Benutzerkonto manuell entsperrt werden, und zwar von einem Benutzer, dem das `MANAGE ANY USER`-Systemprivileg erteilt wurde. Wenn jedoch alle Benutzer mit `MANAGE ANY USER`-Systemprivileg selbst aufgrund fehlgeschlagener Login-Versuche gesperrt sind, ist eine Sperrung einiger oder aller Dienste für eine Datenbank möglich.

Um zu verhindern, dass dieses Szenario eintritt, sind zwei Login-Richtlinienoptionen verfügbar:

- **root\_auto\_lock\_time** Definiert einen Zeitraum, nach dem Benutzer mit `MANAGE ANY USER`-Systemprivileg automatisch entsperrt werden. Setzen Sie diese Option auf einen kleinen Wert (z.B. 15 Minuten). Für diesen Wert gibt es eine vom Server festgelegte Obergrenze von ein paar Stunden. Diese Option kann nur in der Root-Login-Richtlinie festgelegt werden.
- **auto\_unlock\_time** Definiert einen Zeitraum, nach dem alle anderen Benutzer automatisch entsperrt werden. Setzen Sie die `auto_unlock_time`-Option auf `UNLIMITED` (Standardwert). Sie kann in jeder Login-Richtlinie, einschließlich der Root-Login-Richtlinie, festgelegt werden.

Die Konfiguration dieser Werte erfordert das `MANAGE ANY LOGIN POLICY`-Systemprivileg.

Basierend auf den einem Benutzer erteilten Berechtigungen wird zum Zeitpunkt des Entsperrens eine der beiden Login-Richtlinienoptionen überprüft. Das automatische Entsperren gilt nur für Konten, die aufgrund fehlgeschlagener Login-Versuche gesperrt wurden, und nicht für Konten, die aus einem anderen Grund gesperrt wurden. Der gesperrte Status eines Benutzers wird während des Logins überprüft, und wenn der angegebene Zeitraum bis zum automatischen Entsperren erreicht oder überschritten ist, darf der Benutzer sich anmelden und der `failed_login_attempts`-Zähler wird auf Null zurückgesetzt.

### Siehe auch

- [Login-Richtlinienoptionen und Standardwerte auf Seite 536](#)

## Datenbankoptionen

Mit den folgenden Optionen können Sie das Verhalten einer SQL Anywhere-Datenbank konfigurieren.

Option	Werte	Standardwert	Erforderliches Privileg
„allow_nulls_by_default-Option“	On, Off	On  Off für Sybase Open Client- und jConnect-Verbindungen	SET ANY PUBLIC OPTION
„allow_read_client_file-Option“	On, Off	Off	SET ANY SECURITY OPTION
„allow_snapshot_isolation-Option“	On, Off	Off	SET ANY SYSTEM OPTION
„allow_write_client_file-Option“	On, Off	Off	SET ANY SECURITY OPTION
„ansi_blanks-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„ansi_close_cursors_on_rollback-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„ansi_permissions-Option“	On, Off	On	SET ANY SYSTEM OPTION
„ansi_substring-Option“	On, Off	On	SET ANY PUBLIC OPTION
„ansi_update_constraints-Option“	Off, Cursors, Strict	Cursors	SET ANY PUBLIC OPTION
„ansinull-Option“	On, Off	On	SET ANY PUBLIC OPTION
„auditing-Option“	On, Off	Off	SET ANY SECURITY OPTION
„auditing_options-Option (für die Verwendung durch das System reserviert)“	Reserviert	Reserviert	SET ANY SECURITY OPTION
„auto_commit_on_create_local_temp_index-Option“	On, Off	Off	SET ANY SYSTEM OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„background_priority-Option [nicht mehr empfohlen]“	On, Off	Off	SET ANY PUBLIC OPTION
„blocking-Option“	On, Off	On	SET ANY PUBLIC OPTION
„blocking_others_timeout-Option“	Ganzzahl, in Millisekunden	0	SET ANY PUBLIC OPTION
„blocking_timeout-Option“	Ganzzahl, in Millisekunden	0	SET ANY PUBLIC OPTION
„chained-Option“	On, Off	On  Off für Sybase Open Client- und jConnect-Verbindungen	SET ANY PUBLIC OPTION
„checkpoint_time-Option“	Anzahl von Minuten	60	SET ANY SYSTEM OPTION
„cis_option-Option“	0, 7	0	SET ANY PUBLIC OPTION
„cis_rowset_size-Option“	Ganzzahl	50	SET ANY PUBLIC OPTION
„close_on_endtrans-Option“	On, Off	On  Off bei jConnect-Verbindungen	SET ANY PUBLIC OPTION
„collect_statistics_on_dml_updates-Option“	On, Off	On	SET ANY PUBLIC OPTION
„conn_auditing-Option“	On, Off	On	SET ANY SECURITY OPTION
„connection_authentication-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„continue_after_raiser- ror-Option“	On, Off	On	SET ANY PUBLIC OPTION
„conversion_error- Option“	On, Off	On	SET ANY PUBLIC OPTION
„cooperative_com- mit_timeout-Option“	Ganzzahl, in Mil- lisekunden	250	SET ANY PUBLIC OPTION
„cooperative_commits- Option“	On, Off	On	SET ANY PUBLIC OPTION
„database_authenticati- on-Option“	Zeichenfolge	Leere Zei- chenfolge	SET ANY SECURITY OPTION
„date_format-Option“	Zeichenfolge	YYYY-MM- DD	SET ANY PUBLIC OPTION
„date_order-Option“	MDY, YMD, DMY	YMD	SET ANY PUBLIC OPTION
„db_publisher-Opti- on“ auf Seite 602	Benutzer-ID	-1	SET ANY SYSTEM OPTION
„debug_messages-Opti- on“	On, Off	Off	SET ANY PUBLIC OPTION
„dedicated_task-Opti- on“	On, Off	Off	SET ANY SYSTEM OPTION
„default_dbspace-Opti- on“	Zeichenfolge	Leere Zei- chenfolge (System- DBSpace ver- wenden)	SET ANY PUBLIC OPTION
„default_time- stamp_increment-Opti- on“	Ganzzahl, in Mik- rosekunden von 1 bis 1000000	1	SET ANY PUBLIC OPTION
„delayed_com- mit_timeout-Option“	Ganzzahl, in Mil- lisekunden	500	SET ANY PUBLIC OPTION
„delayed_commits- Option“	On, Off	Off	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„disk_sandbox-Option“ auf Seite 608	On, Off	Off	SET ANY SECURITY OPTION
„divide_by_zero_error-Option“	On, Off	On	SET ANY PUBLIC OPTION
„escape_character-Option“	Reserviert	Reserviert	SET ANY PUBLIC OPTION
„exclude_operators-Option“	Reserviert	Reserviert	SET ANY SYSTEM OPTION
„extended_join_syntax-Option“	On, Off	On	SET ANY PUBLIC OPTION
„extern_login_credentials-Option“ auf Seite 611	Login_user, Effective_user	Login_user	SET ANY SECURITY OPTION
„fire_triggers-Option“	On, Off	On	SET ANY SYSTEM OPTION
„first_day_of_week-Option“	1, 2, 3, 4, 5, 6, 7	7 (Sonntag ist der erste Wochentag)	SET ANY PUBLIC OPTION
„for_xml_null_treatment-Option“	Empty, Omit	Omit	SET ANY PUBLIC OPTION
„force_view_creation-Option“	Reserviert	Reserviert	SET ANY SYSTEM OPTION
„global_database_id-Option“	Ganzzahl	2147483647	SET ANY SYSTEM OPTION
„http_connection_pool_basesize-Option“	Ganzzahl (zwischen 0 und 1000)	10	SET ANY SYSTEM OPTION
„http_connection_pool_timeout-Option“	Ganzzahl, in Sekunden von 1 bis 86400	60	SET ANY SYSTEM OPTION
„http_session_timeout“	Ganzzahl	30	SET ANY PUBLIC OPTION
„integrated_server_name-Option“	Zeichenfolge	NULL	SET ANY SECURITY OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„isolation_level-Option“	0, 1, 2, 3, Snapshot, Statement-snapshot, Read-only-statement-snapshot	0	SET ANY PUBLIC OPTION
„java_class_path-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„java_location-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„java_main_userid-Option (nicht mehr empfohlen)“ auf Seite 622	Zeichenfolge	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„java_vm_options-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„log_deadlocks-Option“	On, Off	Off	SET ANY SYSTEM OPTION
„login_mode-Option“	Standard, Integrated, Kerberos, LDAPUA, CloudAdmin, Mixed (nicht mehr empfohlen)	Standard	SET ANY SECURITY OPTION
„login_procedure-Option“	Zeichenfolge	sp_login_environment	SET ANY SECURITY OPTION
„materialized_view_optimization-Option“	Disabled, Fresh, Stale, $N \{ \text{Minute[s]}   \text{Hour[s]}   \text{Day[s]}   \text{Week[s]}   \text{Month[s]} \}$	Stale	SET ANY PUBLIC OPTION
„max_client_statements_cached-Option“	Ganzzahl	10	SET ANY PUBLIC OPTION
„max_cursor_count-Option“	Ganzzahl	50	SET ANY SYSTEM OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„max_plans_cached-Option“	Ganzzahl	20	SET ANY PUBLIC OPTION
„max_priority-Option“	Critical, High, Above Normal, Normal, Below normal, Low, Background	Normal	SET ANY SYSTEM OPTION
„max_query_tasks-Option“	Ganzzahl	0	SET ANY PUBLIC OPTION
„max_recursive_iterations-Option“	Ganzzahl	100	SET ANY PUBLIC OPTION
„max_statement_count-Option“	Ganzzahl $\geq 0$	50	SET ANY SYSTEM OPTION
„max_temp_space-Option“	Ganzzahl [k m g p]	0	SET ANY SYSTEM OPTION
„min_password_length-Option“	Ganzzahl $\geq 0$	0 Zeichen	SET ANY SECURITY OPTION
„min_role_admins-Option“ auf Seite 638	Ganzzahl zwischen 1 und 10 (inklusive)	1	SET ANY SECURITY OPTION
„nearest_century-Option“	Ganzzahl zwischen 0 und 100	50	SET ANY PUBLIC OPTION
„non_keywords-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY PUBLIC OPTION
„odbc_describe_binary_as_varbinary“	On, Off	Off	SET ANY PUBLIC OPTION
„odbc_distinguish_char_and_varchar-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„oem_string-Option“	Zeichenfolge (bis zu 128 Byte)	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„on_charset_conversion_failure-Option“	Ignore, Warning, Error	Ignore	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„on_tsq_error-Option“	Stop, Conditional, Continue	Conditional Continue bei jConnect- Verbindun- gen	SET ANY PUBLIC OPTION
„optimization_goal-Option“	First-row oder All-rows (Erste Zeile oder Alle Zeilen)	All-rows	SET ANY PUBLIC OPTION
„optimization_level-Option“	0-15	9	SET ANY PUBLIC OPTION
„optimization_workload-Option“	Mixed, OLAP	Mixed	SET ANY SYSTEM OPTION
„pinned_cursor_percent_of_cache-Option“	Ganzzahl zwischen 0 und 100	10	SET ANY SYSTEM OPTION
„post_login_procedure-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SECURITY OPTION
„precision-Option“	Ganzzahl zwischen 1 und 127	30	SET ANY PUBLIC OPTION
„prefetch-Option“	Off, Conditional, Always	Conditional	SET ANY PUBLIC OPTION
„preserve_source_format-Option“	On, Off	On	SET ANY SYSTEM OPTION
„prevent_article_pkey_update-Option“	On, Off	On	SET ANY PUBLIC OPTION
„priority-Option“	Critical, High, Above Normal, Normal, Below normal, Low, Background	Normal	SET ANY PUBLIC OPTION
„progress_messages-Option“	Off, Formatted, RAW	Off	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„query_mem_timeout-Option“	-1, 0, positive Ganzzahl	-1	SET ANY PUBLIC OPTION
„quoted_identifier-Option“	On, Off	On	SET ANY PUBLIC OPTION
„read_past_deleted-Option“	On, Off	On	SET ANY PUBLIC OPTION
„recovery_time-Option“	Ganzzahl in Minuten	2	SET ANY SYSTEM OPTION
„remote_idle_timeout-Option“	Ganzzahl in Sekunden	15	SET ANY PUBLIC OPTION
„request_timeout-Option“	Ganzzahl, 0 bis 86400, in Sekunden	0	SET ANY PUBLIC OPTION
„reserved_keywords-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SYSTEM OPTION
„return_date_time_as_string-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„rollback_on_deadlock-Option“	On, Off	On	SET ANY PUBLIC OPTION
„row_counts-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„scale-Option“	Ganzzahl zwischen 0 und 127 (inklusive), die kleiner ist als der für die Datenbankoption precision angegebene Wert	6	SET ANY PUBLIC OPTION
„secure_feature_key-Option (nicht mehr empfohlen)“	Zeichenfolge	NULL	SET ANY PUBLIC OPTION
„sort_collation-Option“	Internal, collation_name oder collation_id	Internal	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„sql_flagger_error_level-Option“	Off, SQL:1992/Entry, SQL:1992/Intermediate, SQL:1992/Full, SQL:1999/Core, SQL:1999/Package, SQL:2003/Core, SQL:2003/Package, UltraLite	Off	SET ANY PUBLIC OPTION
„sql_flagger_warning_level-Option“	Off, SQL:1992/Entry, SQL:1992/Intermediate, SQL:1992/Full, SQL:1999/Core, SQL:1999/Package, SQL:2003/Core, SQL:2003/Package, UltraLite	Off	SET ANY PUBLIC OPTION
„string_truncation-Option“	On, Off	On	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„st_geometry_asbinary_format-Option“	Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste der Parameter (einschließlich Unterparameter), die für die ST_AsBinary-Methode beim ST_Geometry-Typ dokumentiert sind. Siehe <a href="#">ST_AsBinary-Methode für den ST_Geometry-Datentyp [SQL Anywhere Server - Unterstützung für räumliche Daten]</a> .	WKB	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„st_geometry_astext_format-Option“	Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste der Parameter (einschließlich Unterparameter), die für die ST_AsText-Methode beim ST_Geometry-Typ dokumentiert sind. Siehe <a href="#">ST_AsText-Methode für den ST_Geometry-Datentyp [SQL Anywhere Server - Unterstützung für räumliche Daten]</a> .	WKT	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„st_geometry_asxml_format-Option“	Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste der Parameter (einschließlich Unterparameter), die für die ST_AsXML-Methode beim ST_Geometry-Typ dokumentiert sind. Siehe <a href="#">ST_AsXML-Methode für den ST_Geometry-Datentyp [SQL Anywhere Server - Unterstützung für räumliche Daten]</a> .	XML	SET ANY PUBLIC OPTION
„st_geometry_describe_type-Option“	CHAR, NCHAR, BINARY	CHAR	SET ANY PUBLIC OPTION
„st_geometry_interpolation-Option“	Eine Gruppe von Schlüssel=Wert-Paaren, formatiert als: key1=value1; key2=value2; . Gültige Schlüssel sind: relative-tolerance-percent= <i>DOUBLE</i> absolute-tolerance= <i>DOUBLE</i>	Weitere Hinweise finden Sie unter der Beschreibung des Standardverhaltens unter <a href="#">„st_geometry_interpolation-Option“</a> auf Seite 683.	SET ANY PUBLIC OPTION
„st_geometry_on_invalid-Option“	Ignore, Error	Error	SET ANY PUBLIC OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„subsume_row_locks-Option“	On, Off	On	SET ANY PUBLIC OPTION
„suppress_tds_debugging-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„synchronize_mirror_on_commit“	On, Off	Off	SET ANY PUBLIC OPTION
„tds_empty_string_is_null-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„temp_space_limit_check-Option“	On, Off	On	SET ANY SYSTEM OPTION
„time_format-Option“	Zeichenfolge	HH:NN:SS.SS	SET ANY PUBLIC OPTION
„time_zone_adjustment-Option“	Ganzzahl oder negative Ganzzahl in Anführungszeichen oder Zeichenfolge als Darstellung der Zeit in Stunden und Minuten, mit Vorzeichen "+" oder "-", in Anführungszeichen gesetzt	Wird von der Zeitzone des Clients oder des Datenbankservers gesetzt, abhängig vom Verbindungstyp des Clients	SET ANY PUBLIC OPTION
„timestamp_format-Option“	Zeichenfolge	YYYY-MM-DD HH:NN:SS.SS	SET ANY PUBLIC OPTION
„timestamp_with_time_zone_format-Option“	Zeichenfolge	YYYY-MM-DD HH:NN:SS.SS+HH:NN	SET ANY PUBLIC OPTION
„truncate_timestamp_values-Option“	On, Off	Off	SET ANY SYSTEM OPTION

Option	Werte	Standardwert	Erforderliches Privileg
„trusted_certificates_file-Option“ auf Seite 696	NULL, 'Dateipfad_zum_Zertifikat'	NULL	SET ANY SECURITY OPTION
„tsql_outter_joins-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„tsql_variables-Option“	On, Off	Off  On für Sybase Open Client- und jConnect-Verbindungen	SET ANY PUBLIC OPTION
„updatable_statement_isolation-Option“	0, 1, 2, 3	0	SET ANY PUBLIC OPTION
„update_statistics-Option“	On, Off	On	SET ANY PUBLIC OPTION
„user_estimates-Option“	Enabled, Disabled, Override-Magic	Override-Magic	SET ANY PUBLIC OPTION
„uuid_has_hyphens-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„verify_password_function-Option“	Zeichenfolge	Leere Zeichenfolge	SET ANY SECURITY OPTION
„wait_for_commit-Option“	On, Off	Off	SET ANY PUBLIC OPTION
„webservice_namespace_host-Option“	NULL, Hostname-Zeichenfolge	NULL	SET ANY SYSTEM OPTION
„webservice_sessionid_name-Option“ auf Seite 709	NULL, SessionID-Zeichenfolge	NULL	SET ANY SYSTEM OPTION

**Siehe auch**

- „Unterschiedliche Typen von Datenbankoptionen“ auf Seite 559

## Unterschiedliche Typen von Datenbankoptionen

SQL Anywhere bietet unterschiedliche Typen von Datenbankoptionen, die folgendermaßen klassifiziert werden können:

- Datenbankoptionen. Siehe „[Datenbankoptionen](#)“ auf Seite 544.
- Kompatibilitätsoptionen. Siehe „[Kompatibilitätsoptionen](#)“ auf Seite 559.
- Synchronisationsoptionen. Siehe „[Synchronisationsoptionen](#)“ auf Seite 562.
- SQL Remote-Optionen. Siehe „[SQL Remote-Optionen](#)“ auf Seite 563.
- Interactive SQL-Optionen. Siehe „[Interactive SQL-Optionen](#)“ auf Seite 851.

## Kompatibilitätsoptionen

Mit den folgenden Optionen können Sie das Verhalten von SQL Anywhere mit dem von Adaptive Server Enterprise kompatibel machen oder sowohl das alte Verhalten unterstützen als auch das ISO SQL/2008-Verhalten zulassen.

Um die Kompatibilität mit Adaptive Server Enterprise zu erhöhen, können einige dieser Optionen für die Dauer der aktuellen Verbindung gesetzt werden, indem Sie die Transact-SQL SET-Anweisung anstelle der SQL Anywhere SET OPTION-Anweisung benutzen. Siehe „[SET-Anweisung \[T-SQL\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

### Standardeinstellungen

Die Standardeinstellung für einige dieser Optionen unterscheidet sich von der Standardeinstellung in Adaptive Server Enterprise. Um die Kompatibilität zwischen Ihren SQL Anywhere- und Adaptive Server Enterprise-Datenbanken zu gewährleisten, sollten Sie jede in diesem Abschnitt aufgelistete Kompatibilitätsoption explizit setzen.

Wenn eine Verbindung mit den Sybase Open Client- oder JDBC-Schnittstellen eingerichtet wird, werden einige Optionen speziell für die aktuelle Verbindung eingestellt, damit die Kompatibilität mit Adaptive Server Enterprise gesichert ist. Siehe „[Optionen für Sybase Open Client- und JDBC-Verbindungskompatibilität mit Adaptive Server Enterprise](#)“ auf Seite 559.

### Optionen für Sybase Open Client- und JDBC-Verbindungskompatibilität mit Adaptive Server Enterprise

Option	Einstellung
allow_nulls_by_default	Off
ansi_blanks	Off
ansi_substring	On
ansinull	On

Option	Einstellung
chained	Off
continue_after_raisererror	On
escape_character	Off
on_tsq_l_error	Continue bei jConnect-Verbindungen
time_format	HH:NN:SS.SSS
timestamp_format	YYYY-MM-DD HH:NN:SS.SSS
tsq_l_outer_joins	Off
tsq_l_variables	On

## Transact-SQL- und SQL/2008-Kompatibilitätsoptionen

Die folgende Tabelle listet die Kompatibilitätsoptionen mit den zulässigen Werten und Standardeinstellungen auf.

Option	Werte	Standardwert
„allow_nulls_by_default-Option“ auf Seite 572	On, Off	On
„ansi_blanks-Option“ auf Seite 575	On, Off	Off
„ansi_close_cursors_on_rollback-Option“ auf Seite 576	On, Off	Off
„ansi_permissions-Option“ auf Seite 577	On, Off	On
„ansi_update_constraints-Option“ auf Seite 579	Off, Cursors, Strict	Cursors
„ansinull-Option“ auf Seite 580	On, Off	On
„chained-Option“ auf Seite 587	On, Off	On
„close_on_endtrans-Option“ auf Seite 590	On, Off	On
„continue_after_raisererror-Option“ auf Seite 594	On, Off	On
„conversion_error-Option“ auf Seite 595	On, Off	On

Option	Werte	Standardwert
„date_format-Option“ auf Seite 599	Zeichenfolge	YYYY-MM-DD
„date_order-Option“ auf Seite 601	MDY, YMD, DMY	YMD
„divide_by_zero_error-Option“ auf Seite 609	On, Off	On
„escape_character-Option“ auf Seite 609	Reserviert	Reserviert
„fire_triggers-Option“ auf Seite 612	On, Off	On
„isolation_level-Option“ auf Seite 619	0, 1, 2, 3	0
„nearest_century-Option“ auf Seite 640	Ganzzahl (zwischen 0 und inklusive 100)	50
„non_keywords-Option“ auf Seite 641	Zeichenfolge (kommagetrennte Schlüsselwörterliste)	Leere Zeichenfolge (keine Schlüsselwörter deaktiviert)
„on_tsq_error-Option“ auf Seite 646	Stop, Conditional, Continue	Conditional
„quoted_identifier-Option“ auf Seite 660	On, Off	On
„reserved_keywords-Option“ auf Seite 665	Zeichenfolge (kommagetrennte Schlüsselwörterliste)	Leere Zeichenfolge (keine Schlüsselwörter deaktiviert)
„sql_flagger_error_level-Option“ auf Seite 671	Off, SQL:1992/Entry, SQL:1992/Intermediate, SQL:1992/Full, SQL:1999/Core, SQL:1999/Package, SQL:2003/Core, SQL:2003/Package, UltraLite	Off

Option	Werte	Standardwert
„sql_flagger_warning_level-Option“ auf Seite 672	Off, SQL:1992/Entry, SQL:1992/Intermediate, SQL:1992/Full, SQL:1999/Core, SQL:1999/Package, SQL:2003/Core, SQL:2003/Package, UltraLite	Off
„string_rtruncation-Option“ auf Seite 685	On, Off	On
„time_format-Option“ auf Seite 690	Zeichenfolge	HH:NN:SS.SSS
„timestamp_format-Option“ auf Seite 692	Zeichenfolge	YYYY-MM-DD HH:NN:SS.SSS
„tsql_outer_joins-Option“ auf Seite 699	On, Off	Off
„tsql_variables-Option“ auf Seite 699	On, Off	Off

## Synchronisationsoptionen

Die folgenden Datenbankoptionen können gesetzt werden, um SQL Anywhere-Datenbanken zur Verwendung als MobiLink-Synchronisations-Clients zu konfigurieren.

Option	Werte	Standardwert
„default_timestamp_increment-Option“ auf Seite 605	Ganzzahl, in Mikrosekunden von 1 bis 1000000	1
„delete_old_logs-Option [SQL Remote]“ auf Seite 607	On, Off, Delay, <i>n</i> Tage	Off
„ml_remote_id-Option“ auf Seite 639	Ein beliebiger Wert, der die Datenbank für die MobiLink-Synchronisation eindeutig identifiziert	NULL
„prevent_article_pkey_update-Option“ auf Seite 655	On, Off	On

Option	Werte	Standardwert
„truncate_timestamp_values-Option“ auf Seite 697	On, Off	Off

## SQL Remote-Optionen

Die folgenden Optionen steuern das SQL Remote-Replikationsverhalten.

Option	Werte	Standardwert
„blob_threshold-Option [SQL Remote]“ auf Seite 585	Ganzzahl (in kB)	256
„compression-Option [SQL Remote]“ auf Seite 592	Ganzzahl von -1 bis 9	6
„delete_old_logs-Option [SQL Remote]“ auf Seite 607	On, Off, Delay, <i>n</i> days	Off
„external_remote_options-Option [SQL Remote]“ auf Seite 611	On, Off	Off
„qualify_owners-Option [SQL Remote]“ auf Seite 658	On, Off	On
„quote_all_identifiers-Option [SQL Remote]“ auf Seite 659	On, Off	Aus
„replication_error-Option [SQL Remote]“ auf Seite 663	Name der gespeicherten Prozedur	(keine Prozedur)
„replication_error_piece-Option [SQL Remote]“ auf Seite 663	Name der gespeicherten Prozedur	(keine Prozedur)
„save_remote_passwords-Option [SQL Remote]“ auf Seite 668	On, Off	On
„sr_date_format-Option [SQL Remote]“ auf Seite 673	<i>Datumszeichenfolge</i>	yyyy/mm/dd
„sr_time_format-Option [SQL Remote]“ auf Seite 675	<i>Uhrzeit-Zeichenfolge</i>	hh:nn:ss.Ssssss
„sr_timestamp_format-Option [SQL Remote]“ auf Seite 676	<i>Zeitstempel-Zeichenfolge</i>	yyyy/mm/dd hh:nn:ss.Ssssss

Option	Werte	Standardwert
„sr_timestamp_with_time_zone_for- mat-Option [SQL Remote]“ auf Seite 677	<i>Zeitstempel-mit-Zeit- zonen-Zeichenfolge</i>	yyyy/mm/dd hh:nn:ss.Ssssss +hh:nn
„subscribe_by_remote-Option [SQL Remote]“ auf Seite 686	On, Off	On
„verify_all_columns-Option [SQL Remote]“ auf Seite 704	On, Off	Off
„verify_threshold-Option [SQL Remote]“ auf Seite 707	Ganzzahl (in Byte)	1000

## Bereich und Dauer von Datenbankoptionen

Sie können Optionen auf drei Ebenen setzen:

- PUBLIC
- Benutzer
- temporär

Temporäre Optionen haben Vorrang vor Benutzer- und PUBLIC-Einstellungen. Optionen auf Benutzerebene haben Vorrang vor PUBLIC-Einstellungen. Wenn Sie eine Option der Benutzerebene für den aktuellen Benutzer einstellen, wird die entsprechende temporäre Option ebenfalls gesetzt.

Einige Optionen (wie COMMIT-Verhalten) haben einen datenbankweiten Geltungsbereich. Das Setzen dieser Optionen erfordert bestimmte Privilegien. Andere Optionen (z.B. isolation\_level) können nur auf die aktuelle Verbindung angewendet werden und erfordern keine besonderen Privilegien.

Änderungen an Optionseinstellungen erfolgen je nach Option zu unterschiedlichen Zeitpunkten. Änderungen an einer globalen Option wie recovery\_time treten in Kraft, wenn die Datenbank das nächste Mal gestartet wird. Normalerweise werden nur Optionen sofort geändert, die die aktuelle Verbindung betreffen. Sie können Optionseinstellungen beispielsweise während einer Transaktion ändern.

### Vorsicht

Ändern Sie Optionswerte nicht, während ein Cursor geöffnet ist. Ein Ändern der Optionswerte bei geöffnetem Cursor kann zu inkonsistenten Ergebnissen in dem Cursor führen. Beispiel: Wenn Sie die date\_format-Option ändern, während ein Cursor geöffnet ist, kann dies dazu führen, dass einige Zeilen im alten Format zurückgegeben werden und einige Zeilen im neuen Format. Um sicherzustellen, dass die Zeilen in der Ergebnismenge konsistent mit dem neuen Optionswert berechnet werden, öffnen Sie den Cursor erst nach dem Ändern des Optionswerts.

## **PUBLIC-Optionen setzen**

Wenn der Wert einer Option für die PUBLIC-Rolle geändert wird, gilt dieser permanente Wert für alle Benutzer, für die kein eigener Wert festgelegt wurde. Ein Optionswert kann nur dann für eine einzelne Benutzer-ID gesetzt werden, wenn es für die betreffende Option bereits eine Einstellung für die PUBLIC-Rolle gibt.

Einige Optionen, die nur für die PUBLIC-Rolle gesetzt werden können, treten für bestehende Verbindungen sofort in Kraft, auch wenn die geänderte Einstellung für Benutzer über die CONNECTION\_PROPERTY-Funktion zunächst nicht sichtbar ist. Ein Beispiel für dieses Verhalten ist die global\_database\_id-Option. Aus diesem Grund sollten nur für PUBLIC geltende Optionen nicht geändert werden, während andere Benutzer mit der Datenbank verbunden sind.

## **Temporäre Optionen setzen**

Das Hinzufügen des Schlüsselworts TEMPORARY zur SET OPTION-Anweisung verändert die Dauer des Änderungsvorgangs. Normalerweise wird der Wert einer Option mit permanenter Wirkung geändert. Wenn die SET TEMPORARY OPTION-Anweisung ausgeführt wird, wirkt sich der neue Optionswert nur auf die aktuelle Verbindung und für die Dauer der Verbindung aus. Diese neue Einstellung wird nur im Serverspeicher gespeichert und wird in der Systemansicht SYSOPTION nicht reflektiert.

Wenn die SET TEMPORARY OPTION-Anweisung verwendet wird, um eine PUBLIC-Option zu setzen, bleibt der geänderte Wert für die Option bestehen, bis die Datenbank heruntergefahren wird. Dann werden die temporären Optionen für die PUBLIC-Rolle wieder auf ihre permanenten Werte zurückgesetzt.

Wenn Sie eine temporäre Option für die PUBLIC-Rolle setzen, bietet dies einen Sicherheitsvorteil. Wenn zum Beispiel die login\_mode-Option aktiviert ist, richtet sich die Datenbank nach der Login-Sicherheit des Systems, auf dem sie läuft. Bei Aktivierung dieser Option als temporäre Optionseinstellung ist eine Datenbank, die von der Sicherheit einer Windows-Domäne abhängig ist, nicht gefährdet, wenn sie heruntergefahren und auf einen lokalen Computer kopiert wird. In diesem Fall wird die login\_mode-Option auf ihren permanenten Wert zurückgesetzt. Dies könnte "Standard" sein, ein Modus, in dem eine integrierte Benutzerauthentifizierung nicht zulässig ist.

## **Optionen für eine SQL-Anweisung festlegen**

Die INSERT-, UPDATE-, DELETE-, SELECT-, UNION, EXCEPT- und INTERSECT-Anweisungen enthalten eine OPTION-Klausel, mit der Sie festlegen können, wie materialisierte Ansichten von der Anweisung verwendet werden und wie die Abfrage optimiert wird. Diese Klausel kann auch verwendet werden, um eine Optionseinstellung anzugeben, die nur für diese Anweisung Vorrang vor allen in Kraft befindlichen temporären und PUBLIC-Optionseinstellungen hat. Sie können die Einstellung der folgenden Optionen mit der OPTION-Klausel ändern:

- isolation\_level
- max\_query\_tasks
- optimization\_goal
- optimization\_level
- optimization\_workload
- user\_estimates

## Siehe auch

- „INSERT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UPDATE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DELETE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SELECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UNION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „EXCEPT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „INTERSECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „isolation\_level-Option“ auf Seite 619
- „max\_query\_tasks-Option“ auf Seite 633
- „optimization\_goal-Option“ auf Seite 647
- „optimization\_level-Option“ auf Seite 648
- „optimization\_workload-Option“ auf Seite 649
- „user\_estimates-Option“ auf Seite 702

## Datenbankoptionen mit der SET OPTION-Anweisung setzen

Setzen Sie Datenbankoptionen mit der SET OPTION-Anweisung. Sie hat folgende allgemeine Syntax:

```
SET [ EXISTING ] [ TEMPORARY ] OPTION  
[ userid. | PUBLIC. ] option-name = [ option-value ]
```

Sie können eine Benutzer-ID oder einen Rollennamen angeben, um die Option nur für diesen Benutzer oder für Berechtigungsempfänger dieser Rolle zu setzen. Sie können auch den Rollennamen PUBLIC angeben, mit dem die Optionen für Berechtigungsempfänger der PUBLIC-Rolle gesetzt werden. Standardmäßig wird neuen Benutzern die PUBLIC-Rolle erteilt. Wenn keine Benutzer-ID oder Rolle angegeben wurde, wird die Optionsänderung auf die derzeit angemeldete Benutzer-ID angewendet, die die SET OPTION-Anweisung ausgegeben hat.

Jede Option, ob benutzerdefiniert oder nicht, muss eine PUBLIC-Einstellung haben, bevor ein benutzerspezifischer Wert zugeordnet werden kann. Der Datenbankserver unterstützt bei benutzerdefinierten Optionen nicht das Setzen von TEMPORARY-Werten.

Wenn *option-value* nicht angegeben ist, wird der angegebene Optionswert auf den Wert dieser Option in der PUBLIC-Rolle zurückgesetzt. Durch Entfernen der TEMPORARY-Option wird der Optionswert auf die permanente Einstellung zurückgesetzt.

### Vorsicht

Ändern Sie Optionswerte nicht, während ein Cursor geöffnet ist. Ein Ändern der Optionswerte bei geöffnetem Cursor kann zu inkonsistenten Ergebnissen in dem Cursor führen. Beispiel: Wenn Sie die *date\_format*-Option ändern, während ein Cursor geöffnet ist, kann dies dazu führen, dass einige Zeilen im alten Format zurückgegeben werden und einige Zeilen im neuen Format. Um sicherzustellen, dass die Zeilen in der Ergebnismenge konsistent mit dem neuen Optionswert berechnet werden, öffnen Sie den Cursor erst nach dem Ändern des Optionswerts.

**Hinweis**

In Datenbanken, die eine türkische Kollation verwenden oder die Groß- und Kleinschreibung berücksichtigen, werden beim Ausführen einer Abfrage für die SYSOPTION-Systemansicht oder einer Abfrage wie der folgenden möglicherweise keine übereinstimmenden Zeilen gefunden, wenn der Optionsname in der falschen Schreibweise verwendet wird:

```
SELECT * FROM sa_conn_properties( ) WHERE propname = 'BLOCKING';
```

**Beispiel**

Mit der folgenden Anweisung wird eine Optionsänderung auf den Benutzer DBA angewendet, falls dieser Benutzer sie ausgegeben hat:

```
SET OPTION blocking_timeout = 3;
```

Mit der folgenden Anweisung wird eine Änderung auf die PUBLIC-Rolle angewendet. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um die login\_mode-Option setzen zu können.

```
SET OPTION PUBLIC.login_mode = 'Standard';
```

Die folgende Anweisung setzt zum Beispiel die ansi\_blanks-Option auf ihren Standardwert zurück.

```
SET OPTION ansi_blanks =;
```

**Siehe auch**

- „SET OPTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Alphabetische Liste der Datenbankoptionen“ auf Seite 572

## Datenbankoptionen anzeigen

**Systemdefinierte Optionswerte**

Mit einer der folgenden Methoden können Sie eine Liste aller systemdefinierten Optionswerte für Ihre eigene Verbindung abrufen. Um systemdefinierte Optionswerte für andere Verbindungen abzurufen, benötigen Sie das Systemprivileg SERVER OPERATOR, MONITOR oder DROP CONNECTION.

- **sa\_conn\_options-Systemprozedur** Um alle aktuellen systemdefinierten Optionseinstellungen aufzulisten, rufen Sie die sa\_conn\_options-Systemprozedur auf:

```
CALL sa_conn_options;
```

Führen Sie die folgende Anweisung aus, um diese Liste alphabetisch zu sortieren:

```
SELECT *
FROM sa_conn_options( )
ORDER BY OptionName;
```

Wenn Sie das Ergebnis filtern oder anders als nach Namen sortieren möchten, verwenden Sie eine WHERE-Klausel:

```
SELECT *
FROM sa_conn_options( )
```

```
WHERE OptionDescription LIKE '%date%'
ORDER BY PropNum;
```

- **sa\_conn\_properties-Systemprozedur** Aktuelle systemdefinierte Optionseinstellungen für Ihre Verbindung sind auch als Teilmenge von **Verbindungseigenschaften** verfügbar. Listen Sie mithilfe der sa\_conn\_properties-Systemprozedur alle Verbindungseigenschaften auf:

```
CALL sa_conn_properties;
```

Führen Sie die folgende Anweisung aus, um diese Liste alphabetisch zu sortieren:

```
SELECT *
FROM sa_conn_properties( )
ORDER BY PropName;
```

- **SET-Anweisung** Führen Sie in Interactive SQL die SET-Anweisung ohne Argumente aus, um die aktuellen Einstellungen der systemdefinierten Verbindungs-, Datenbank- und Interactive SQL-Optionen aufzulisten.

```
SET;
```

Sie können den aktuellen Wert für eine einzelne systemdefinierte Option abrufen, indem Sie die CONNECTION\_PROPERTY-Systemfunktion verwenden:

- **CONNECTION\_PROPERTY-Systemfunktion** Führen Sie die folgende Anweisung aus, um den Wert der Option ansi\_blanks abzurufen:

```
SELECT CONNECTION_PROPERTY ( 'ansi_blanks' );
```

Die CONNECTION\_PROPERTY-Systemfunktion kann nicht verwendet werden, um die Werte von benutzerdefinierten Optionen abzurufen.

In Embedded SQL-Programmen können Sie mit der GET OPTION-Anweisung den Wert einer (system- oder benutzerdefinierten) Option in Ihrer Embedded SQL-Anwendung abrufen.

### Benutzerdefinierte Optionswerte

Sie können die Werte von benutzerdefinierten Optionen abrufen, indem Sie die SYSOPTIONS-Systemansicht abfragen:

- **SYSOPTIONS-Systemansicht** Die Ergebnisse der Systemprozeduren sa\_conn\_options und sa\_conn\_properties umfassen Einstellungen auf Verbindungsebene für systemdefinierte Optionen, die Benutzer- oder PUBLIC-Einstellungen aufheben.

Die Werte von benutzerdefinierten Optionen werden nicht von den Systemprozeduren sa\_conn\_options oder sa\_conn\_properties zurückgegeben. Sie können auch die Katalogansicht SYSOPTION oder SYSOPTIONS direkt abfragen, um den Wert einer bestimmten benutzerdefinierten Option zu bestimmen. Die folgende Abfrage in der SYSOPTIONS-Systemansicht liefert alle Einstellungen auf PUBLIC-Ebene und auf Benutzerebene für alle system- und benutzerdefinierten Optionen, die permanent gesetzt wurden:

```
SELECT *
FROM SYSOPTIONS;
```

Wenn Sie mit der SET TEMPORARY OPTION-Anweisung eine temporäre serverdefinierte Option für eine bestimmte Verbindung setzen, führt dies nicht dazu, dass die Systemansicht SYSOPTION (oder SYSOPTIONS) aktualisiert wird. Temporäre Änderungen an Optionseinstellungen auf Verbindungsebene werden nur im Serverspeicher gespeichert.

### Alle Optionswerte

Sie können die Werte aller Optionen, außer der temporären Optionen, mit Sybase Central abrufen:

- **Sybase Central** Wählen Sie in Sybase Central eine Datenbank aus und klicken Sie dann auf **Datei » Optionen**.

### Siehe auch

- „sa\_conn\_options-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_conn\_properties-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SYSOPTION-Systemansicht“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CONNECTION\_PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GET OPTION-Anweisung [ESQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET-Anweisung [T-SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET REMOTE OPTION-Anweisung [SQL Remote]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Optionseinstellungen überwachen

Überwachen Sie Optionseinstellungen, indem Sie die sa\_server\_option-Systemprozedur mit der Eigenschaft OptionWatchList oder OptionWatchAction ausführen, um das Verhalten des Datenbankservers bei Änderungen an bestimmten Datenbankoptionswerten anzugeben.

### Voraussetzungen

Sie müssen das SERVER OPERATOR-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Rufen Sie die sa\_server\_option-Systemprozedur mit der Eigenschaft OptionWatchList oder OptionWatchAction auf.

Weisen Sie mithilfe der sa\_server\_option-Systemprozedur den Datenbankserver an, eine Nachricht zu senden oder eine Fehlermeldung zurückzugeben, wenn versucht wird, eine Datenbankoption zu setzen. Verwenden Sie die OptionWatchList-Eigenschaft, um eine Liste der zu überwachenden Optionen zu erstellen, und die OptionWatchAction-Eigenschaft, um die Aktion anzugeben, die der Datenserver ausführen soll, wenn versucht wird, eine überwachte Option zu setzen.

### Ergebnisse

Die Optionswerte werden überwacht.

### Beispiel

Weisen Sie mithilfe der folgenden gespeicherten Prozedur den Datenbankserver an, die Datenbankoptionen `automatic_timestamp`, `float_as_double` und `tsql_hex_constant` zu überwachen:

```
CALL dbo.sa_server_option(  
  'OptionWatchList', 'automatic_timestamp,float_as_double,tsql_hex_constant' );
```

Weisen Sie mithilfe der folgenden gespeicherten Prozedur den Datenbankserver an, einen Fehler zurückzugeben, wenn versucht wird, eine in der `OptionWatchList`-Eigenschaft angegebene Option einzustellen:

```
CALL dbo.sa_server_option( 'OptionWatchAction','ERROR' );
```

### Siehe auch

- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- [OptionWatchAction-Datenbankeigenschaft auf Seite 781](#)
- [OptionWatchList-Datenbankeigenschaft auf Seite 781](#)

## Datenbankoptionen ändern (Sybase Central)

Ändern Sie die Werte von Datenbankoptionen für eine Datenbank, einen Benutzer oder eine Rolle.

### Voraussetzungen

Jeder Benutzer kann seine eigenen Optionen setzen.

Um Datenbankoptionen für andere Benutzer oder Rollen, einschließlich der PUBLIC-Rolle, setzen zu können, benötigen Sie eines der folgenden Systemprivilegien, je nachdem, welches Privileg die betreffende Option erfordert:

- SET ANY SYSTEM OPTION
- SET ANY PUBLIC OPTION
- SET ANY SECURITY OPTION
- SET ANY USER DEFINED OPTION

### Kontext und Bemerkungen

Das Ändern der Optionen für die Datenbank entspricht dem Ändern der Optionen für die PUBLIC-Rolle.

Jede Option, ob benutzerdefiniert oder nicht, muss eine PUBLIC-Einstellung haben, bevor ein benutzerspezifischer Wert zugeordnet werden kann. Neue Optionen können Sie nur für die PUBLIC-Rolle erstellen.

Durch Ändern eines Optionswerts für die PUBLIC-Rolle ändert sich der Wert der Option für alle Benutzer außer denjenigen, die explizit Werte für diese Option gesetzt haben. Wenn Sie den Wert einer Option für einen Benutzer oder eine Rolle (außer der PUBLIC-Rolle) setzen, hebt der neue Wert den durch die PUBLIC-Rolle gesetzten Wert auf.

Wenn Sie eine Option aus einem Benutzer oder einer Rolle entfernen, wird die PUBLIC-Einstellung für die Option angewendet. Wenn Sie eine Option aus der PUBLIC-Rolle entfernen, wird die Option aus der

Datenbank entfernt. Alle Benutzereinstellungen für eine Option müssen entfernt werden, bevor die Option aus der PUBLIC-Rolle entfernt werden kann.

Sie können mit Sybase Central keine temporären Optionen setzen oder ändern. Verwenden Sie zum Setzen von temporären Optionen die SET OPTION-Anweisung.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Wählen Sie eine der folgenden Optionen:

Option	Aktion
Optionen für die PUBLIC-Rolle ändern	<ol style="list-style-type: none"> <li>a. Klicken Sie im linken Fensterausschnitt auf <b>Rollen</b>.</li> <li>b. Rechtsklicken Sie im rechten Fensterausschnitt auf <b>PUBLIC</b> und klicken Sie auf <b>Optionen</b>.</li> </ol>
Optionen für eine Rolle ändern	<ol style="list-style-type: none"> <li>a. Klicken Sie im linken Fensterausschnitt auf <b>Rollen</b>.</li> <li>b. Rechtsklicken Sie im rechten Fensterausschnitt auf die Rolle und klicken Sie auf <b>Optionen</b>.</li> </ol>
Optionen für einen Benutzer ändern	<ol style="list-style-type: none"> <li>a. Klicken Sie im linken Fensterausschnitt auf <b>Benutzer</b>.</li> <li>b. Rechtsklicken Sie im rechten Fensterausschnitt auf den Benutzer und klicken Sie auf <b>Optionen</b>.</li> </ol>

3. Konfigurieren Sie die Optionen für den Benutzer bzw. die Rolle. Die möglichen Werte, die Sie angeben können, werden im Feld **Wert** angezeigt. Wählen Sie eine der folgenden Optionen:

Option	Aktion
Option hinzufügen	Klicken Sie auf <b>Neu</b> und geben Sie Name und Wert für die Option an.
Option ändern	Ändern Sie den Optionswert im Feld <b>Wert</b> und klicken Sie dann auf <b>Jetzt permanent setzen</b> .
Option entfernen	Wählen Sie die Option aus und klicken Sie auf <b>Jetzt entfernen</b> .

4. Klicken Sie auf **Schließen**.

### Ergebnisse

Die Werte von Datenbankoptionen für die Datenbank, den Benutzer bzw. die Rolle werden geändert.

**Siehe auch**

- „Alphabetische Liste der Datenbankoptionen“ auf Seite 572
- „Datenbankoptionen mit der SET OPTION-Anweisung setzen“ auf Seite 566
- „Bereich und Dauer von Datenbankoptionen“ auf Seite 564
- „SET OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbankoptionseinstellungen für die Kommunikationsprotokolle TDS und Command Sequence

Verbindungen mit SQL Anywhere können über das TDS-Protokoll (Sybase Open Client- und jConnect JDBC-Verbindungen) oder über das Command Sequence-Protokoll (ODBC- und Embedded SQL-Verbindungen) hergestellt werden.

Wenn Sie mit Benutzern arbeiten, die sowohl TDS als auch Command Sequence (CmdSeq) verwenden, können Sie deren anfängliche Einstellungen mithilfe von gespeicherten Prozeduren konfigurieren. SQL Anywhere verwendet diese Methode, um Sybase Open Client-Verbindungen und jConnect-Verbindungen so einzustellen, dass sie dem Standardverhalten von Adaptive Server Enterprise entsprechen.

Die anfänglichen Einstellungen werden mit der login\_procedure-Option gesteuert. Diese Option benennt eine gespeicherte Prozedur, die bei der Verbindungsaufnahme durch einen Benutzer ausgeführt werden soll. Die Standardeinstellung ist die Verwendung der Systemprozedur sp\_login\_environment. Sie können dieses Verhalten ggf. ändern.

Die Prozedur sp\_login\_environment prüft, ob die Verbindung über TDS hergestellt wird. Wenn dies der Fall ist, ruft sie sp\_tsql\_environment auf, die bestimmte Optionen auf neue Standardwerte für die aktuelle Verbindung setzt.

**Siehe auch**

- „Kommunikationsprotokolle der Interface-Bibliothek“ [*SQL Anywhere 16 - Einführung*]
- „login\_procedure-Option“ auf Seite 625
- „sp\_login\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Alphabetische Liste der Datenbankoptionen

### allow\_nulls\_by\_default-Option

Steuert, ob neue Spalten, die ohne Festlegen von NULL oder NOT NULL erstellt wurden, NULL enthalten dürfen

**Zulässige Werte**

On, Off

**Standardwert**

On

Off für Sybase Open Client- und jConnect-Verbindungen

### Bemerkungen

Die allow\_nulls\_by\_default-Option ist für die Transact-SQL-Kompatibilität miteingeschlossen.

### Siehe auch

- „Optionen für die Transact-SQL-Kompatibilität“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- allow\_nulls\_by\_default-Verbindungseigenschaft auf Seite 711
- „Eigenschaften von Sybase Open Client- und jConnect-Verbindungen“ auf Seite 1571
- „CREATE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Optionen für die Transact-SQL-Kompatibilität“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Mit Transact-SQL kompatible Tabellen“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## allow\_read\_client\_file-Option

Damit wird gesteuert, ob das Lesen von Dateien auf einem Clientcomputer zugelassen ist.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Aktivieren Sie diese Option, damit aus Dateien auf einem Clientcomputer gelesen werden kann, z.B. mit der READ\_CLIENT\_FILE-Funktion.

### Siehe auch

- „Zugriff auf Daten auf Clientcomputern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „READ\_CLIENT\_FILE-Funktion“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „LOAD TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „isql\_allow\_read\_client\_file-Option [Interactive SQL]“ auf Seite 858
- „allow\_write\_client\_file-Option“ auf Seite 575
- „isql\_allow\_write\_client\_file-Option [Interactive SQL]“ auf Seite 859
- „Clientseitige Datensicherheit“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- allow\_read\_client\_file-Verbindungseigenschaft auf Seite 711

## allow\_snapshot\_isolation-Option

Steuert, ob die Snapshot-Isolation aktiviert oder deaktiviert ist

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Diese Option steuert, ob die Snapshot-Isolation für die Datenbank aktiviert ist. Wenn diese Option auf "On" gesetzt ist, beginnt der Datenbankserver, die Originalversionen der aktualisierten Zeilen in der temporären Datei aufzuzeichnen, falls eine Transaktion die Snapshot-Isolation verwendet.

Wenn Transaktionen ausgeführt werden, während die Einstellung der Option allow\_snapshot\_isolation geändert wird, wirkt sich die Änderung nicht unmittelbar aus. Transaktionen, die ausgeführt werden, während die Optionseinstellung von "Off" auf "On" geändert wird, müssen abgeschlossen sein, bevor Snapshots verwendet werden können. Wenn die Einstellung der Option von "On" auf "Off" geändert wird, werden ausstehende Snapshots abgeschlossen, bevor der Datenbankserver aufhört, Versionshinweisen zu sammeln, und neue Snapshots werden nicht eingeleitet.

Sie zeigen die aktuelle Einstellung der Snapshot-Isolation bei einer Datenbank an, indem Sie den Wert der Datenbankeigenschaft SnapshotIsolationState abfragen:

```
SELECT DB_PROPERTY ( 'SnapshotIsolationState' );
```

Die SnapshotIsolationState-Eigenschaft hat einen der folgenden Werte:

- **On** Snapshot-Isolation ist für die Datenbank aktiviert.
- **Off** Snapshot-Isolation ist für die Datenbank deaktiviert.
- **in\_transition\_to\_on** Snapshot-Isolation wird aktiviert, sobald die aktuellen Transaktionen abgeschlossen sind.
- **in\_transition\_to\_off** Snapshot-Isolation wird deaktiviert, sobald die aktuellen Transaktionen abgeschlossen sind.

**Siehe auch**

- „isolation\_level-Option“ auf Seite 619
- „updatable\_statement\_isolation-Option“ auf Seite 700
- „Snapshot-Isolation“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Isolationsstufen und Konsistenz“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „So aktivieren Sie die Snapshot-Isolation“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- allow\_snapshot\_isolation-Verbindungseigenschaft auf Seite 711

**Beispiel**

Die folgende Anweisung aktiviert die Snapshot-Isolation bei einer Datenbank:

```
SET OPTION PUBLIC.allow_snapshot_isolation = 'On';
```

**allow\_write\_client\_file-Option**

Damit wird gesteuert, ob das Schreiben von Dateien auf einen Clientcomputer zugelassen ist.

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Aktivieren Sie diese Option, damit Dateien auf einen Clientcomputer geschrieben werden können, z.B. mit der WRITE\_CLIENT\_FILE-Funktion.

**Siehe auch**

- „Zugriff auf Daten auf Clientcomputern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „WRITE\_CLIENT\_FILE-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „UNLOAD-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „isql\_allow\_write\_client\_file-Option [Interactive SQL]“ auf Seite 859
- „allow\_read\_client\_file-Option“ auf Seite 573
- „isql\_allow\_read\_client\_file-Option [Interactive SQL]“ auf Seite 858
- „Clientseitige Datensicherheit“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- allow\_write\_client\_file-Verbindungseigenschaft auf Seite 711

**ansi\_blanks-Option**

Steuert das Verhalten beim clientseitigen Kürzen von Zeichendaten

## Zulässige Werte

On, Off

## Standardwert

Off

## Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

## Bemerkungen

Die Option `ansi_blanks` hat keine Auswirkung, außer die Datenbank ignoriert bei Vergleichen nachgestellte Leerstellen und aufgefüllte Zeichenfolgen, die in Zeichen-Arrays abgerufen werden. Sie erzwingt einen Kürzungsfehler immer dann, wenn ein Wert vom Datentyp `CHAR(N)` in eine `"C char(M)"`-Variable bei Werten von  $N$  größer als oder gleich  $M$  eingelesen wird. Bei `ansi_blanks` auf "Off" tritt ein Kürzungsfehler nur dann auf, wenn mindestens ein nicht-leeres Zeichen gekürzt wird.

Wenn `ansi_blanks` in Embedded SQL auf "On" gesetzt ist, muss beim Angeben eines Wertes vom Datentyp `DT_STRING` das Feld `sqlen` auf die Länge des Puffers gesetzt werden, der den Wert enthält (zumindest die Länge des Werts einschließlich des Platzes für das abschließende Nullzeichen). Bei `ansi_blanks` auf "Off" wird die Länge nur durch die Position des NULL-Zeichens ermittelt. Der Wert der Option `ansi_blanks` wird bestimmt, wenn die Verbindung hergestellt wird. Ein Ändern der Option nach der Verbindungsherstellung wirkt sich nicht auf das Embedded SQL-Verhalten von `"sqlen"` aus.

Wenn eine Datenbank eine Leerzeichenfüllung hat, steuert diese Option Kürzungswarnungen an den Client, wenn der abgerufene Ausdruck `CHAR` oder `NCHAR` (nicht `VARCHAR` oder `NVARCHAR`) ist und in eine Hostvariable vom Typ `CHAR` bzw. `NCHAR` (nicht `VARCHAR` bzw. `NVARCHAR`) übertragen wird. Wenn diese Bedingungen zutreffen und die Hostvariable zu klein ist, um den abgerufenen Ausdruck aufzunehmen, wenn er mit Leerzeichen bis zur maximalen Länge des Ausdrucks aufgefüllt ist, wird eine Kürzungswarnung ausgegeben, und der Indikator enthält die Mindestanzahl von Bytes, die zur Aufnahme des abgerufenen Ausdrucks erforderlich sind, wenn er bis zu seiner maximalen Länge angefüllt wird. Wenn es sich um einen `CHAR(N)`- oder `NCHAR(N)`-Ausdruck handelt, kann der Indikator auf einen anderen Wert als  $N$  gesetzt werden, um die Zeichensatzkonvertierung des zurückgegebenen Werts und die Zeichenlänge-Semantik zu berücksichtigen.

## Siehe auch

- [„Kompatibilitätsoptionen“ auf Seite 559](#)
- [ansi\\_blanks-Verbindungseigenschaft auf Seite 712](#)
- [„Eigenschaften von Sybase Open Client- und jConnect-Verbindungen“ auf Seite 1571](#)
- [„sp\\_tsql\\_environment-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## ansi\_close\_cursors\_on\_rollback-Option

Steuert, ob mit `WITH HOLD` geöffnete Cursor beim Ausführen eines `ROLLBACK` geschlossen werden

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Der SQL/3 Standardentwurf erfordert, dass alle Cursor beim Zurücksetzen einer Transaktion geschlossen werden. Standardmäßig schließt SQL Anywhere beim Zurücksetzen nur die Cursor, die ohne die Klausel WITH HOLD geöffnet wurden. Mit dieser Option können Sie ein Schließen aller Cursor erzwingen.

Die Option close\_on\_endtrans setzt die Option ansi\_close\_cursors\_on\_rollback außer Kraft.

**Siehe auch**

- „close\_on\_endtrans-Option“ auf Seite 590
- „Kompatibilitätsoptionen“ auf Seite 559
- ansi\_close\_cursors\_on\_rollback-Verbindungseigenschaft auf Seite 712
- „Cursor und Transaktionen“ [*SQL Anywhere Server - Programmierung*]

## ansi\_permissions-Option

Steuert Privilegien durch Überprüfen auf DELETE- und UPDATE-Anweisungen.

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn ansi\_permissions auf "On" gesetzt ist, werden die für SQL/2008 erforderlichen Privilegien für DELETE- und UPDATE-Anweisungen überprüft. Der Standardwert in Adaptive Server Enterprise ist "Off". Die folgende Tabelle stellt die Unterschiede heraus.

SQL-Anweisung	Erforderliche Privilegien bei ansi_permissions-Einstellung "Off"	Erforderliche Privilegien bei ansi_permissions-Einstellung "On"
UPDATE	UPDATE-Privileg für die Spalten, in denen Werte gesetzt werden	UPDATE-Privileg für die Spalten, in denen Werte gesetzt werden  SELECT-Privileg für alle in der WHERE-Klausel enthaltenen Spalten  SELECT-Privileg für alle Spalten auf der rechten Seite der SET-Klausel
DELETE	DELETE-Privileg für die Tabelle	DELETE-Privileg für die Tabelle  SELECT-Privileg für alle in der WHERE-Klausel enthaltenen Spalten

**Siehe auch**

- „Kompatibilitätsoptionen“ auf Seite 559
- ansi\_permissions-Verbindungseigenschaft auf Seite 712
- „SET-Anweisung [T-SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## ansi\_substring-Option

Steuert das Verhalten der Funktion SUBSTRING (SUBSTR), wenn negative Werte für die Start- oder Längenparameter angegeben werden

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Wenn die Option ansi\_substring auf "On" gesetzt ist, entspricht das Verhalten der Funktion SUBSTRING dem ANSI/ISO SQL/2008-Verhalten. Ein negatives oder Null-Start-Offset wird behandelt, als ob die

Zeichenfolge links mit Nicht-Zeichen aufgefüllt ist, und gibt einen Fehler aus, wenn eine negative Länge angegeben ist.

Wenn diese Option auf "Off" gesetzt ist, ist das Verhalten der Funktion SUBSTRING dasselbe wie in früheren Versionen von SQL Anywhere: Ein negatives Start-Offset bedeutet ein Offset vom Ende der Zeichenfolge aus, und eine negative Länge bedeutet, dass die gewünschte Teilkette Länge-Zeichen links vom Start-Offset endet. Überdies entspricht ein Start-Offset von "0" einem Start-Offset von "1".

Die Einstellung dieser Option wirkt sich nicht auf das Verhalten der Funktion BYTE\_SUBSTR aus. Es wird empfohlen, dass Sie die Verwendung von nicht-positiven Start-Offsets oder negativen Längen mit der Funktion SUBSTRING vermeiden. Wo immer möglich sollten Sie stattdessen die Funktionen LEFT oder RIGHT verwenden.

### Siehe auch

- „SUBSTRING-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „LEFT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „RIGHT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsoptionen“ auf Seite 559
- ansi\_substring-Verbindungseigenschaft auf Seite 712

### Beispiel

Die folgenden Beispiele zeigen, basierend auf der Option ansi\_substring, die Unterschiede bei den von der Funktion SUBSTRING zurückgegebenen Werten.

```
SUBSTRING( 'abcdefgh',-2,4 );
ansi_substring = Off ==> 'gh' // substring starts at second-last character
ansi_substring = On  ==> 'a'  // takes the first 4 characters of
                               // ???abcdefgh and discards all ?

SUBSTRING( 'abcdefgh',4,-2 );
ansi_substring = Off ==> 'cd'
ansi_substring = On  ==> value -2 out of range for destination

SUBSTRING( 'abcdefgh',0,4 );
ansi_substring = Off ==> 'abcd'
ansi_substring = On  ==> 'abc'
```

## ansi\_update\_constraints-Option

Steuert den Bereich der Aktualisierungen, die zulässig sind

### Zulässige Werte

Off, Cursors, Strict

### Standardwert

Cursors

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

SQL Anywhere bietet mehrere Erweiterungen, die Aktualisierungen zulassen, die im ANSI SQL-Standard nicht zulässig sind. Diese Erweiterungen stellen effiziente Verfahren zur Durchführung von Aktualisierungen dar. Diese können jedoch zu unerwartetem Verhalten führen. Dieses Verhalten kann zu verlorenen Updates führen, wenn die Benutzeranwendung nicht mit dem Verhalten dieser Erweiterungen rechnet.

Die ansi\_update\_constraints-Option bestimmt, ob Aktualisierungen auf solche beschränkt werden, die beim SQL/2008-Standard zulässig sind.

Wenn die Option auf "Strict" gesetzt ist, werden die folgenden Aktualisierungen verhindert:

- Aktualisierungen von Cursors, die JOINS enthalten
- Aktualisierungen von Spalten, die in ORDER BY-Klauseln erscheinen
- Die FROM-Klausel ist in UPDATE-Anweisungen nicht zulässig

Wenn die Option auf "Cursors" gesetzt ist, gelten die gleichen Einschränkungen, aber nur für Cursor. Wenn kein Cursor mit FOR UPDATE oder FOR READ ONLY geöffnet ist, wählt der Datenbankserver einen Aktualisierungsgrad aus, der auf dem SQL/2008-Standard basiert. Wenn die ansi\_update\_constraints-Option auf "Cursors" oder "Strict" gesetzt ist, gelten Cursor, die eine ORDER BY-Klausel enthalten, standardmäßig als FOR READ ONLY, ansonsten gelten sie weiterhin standardmäßig als FOR UPDATE.

Für ODBC, JDBC, ADO.NET und OLE DB ist die Aktualisierbarkeit einer Anweisung explizit READ ONLY.

Für Embedded SQL ist die Aktualisierbarkeit einer Anweisung explizit READ ONLY, es sei denn, die SQL-Präprozessor-Option -m HISTORICAL ist angegeben.

Standardmäßig sind gespeicherte Prozedurcursoren nicht explizit FOR UPDATE oder READ ONLY.

### Siehe auch

- „UPDATE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Der SQL-Präprozessor“ [[SQL Anywhere Server - Programmierung](#)]
- „Kompatibilitätsoptionen“ auf Seite 559
- ansi\_update\_constraints-Verbindungseigenschaft auf Seite 712
- „Zeilenaktualisierungen und -löschungen durch einen Cursor“ [[SQL Anywhere Server - Programmierung](#)]

## ansinull-Option

Steuert die Interpretation von NULL

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Diese Option ist in erster Linie zur Kompatibilität mit Transact-SQL (Adaptive Server Enterprise) implementiert. Die Option ansinull beeinflusst das Ergebnis von Vergleichsprädikaten mit NULL-Konstanten und wirkt sich auf Warnungen aus, die für Gruppenabfragen über NULL ausgegeben werden.

Wenn die ansinull-Option auf "On" gesetzt ist, wird dreiwertige ANSI-Logik für alle Vergleichsprädikate in einer WHERE- oder HAVING-Klausel oder in einer On-Bedingung verwendet. Ein Vergleich mit NULL und = oder != wird als "unbekannt" ausgewertet.

Wenn die ansinull-Option auf "Off" gesetzt ist, benutzt SQL Anywhere zweiwertige Logik für die folgenden vier Bedingungen:

*expr* = NULL

*expr* != NULL

*expr* = @var // @var ist eine Prozedurvariable oder Hostvariable

*expr* != @var

In jedem Fall wird das Prädikat als TRUE oder FALSE bewertet, nie als UNKONWN. In diesen Vergleichen wird NULL als Sonderwert in jeder Domäne behandelt, und ein Gleichheitsvergleich (=) von zwei NULL-Werten wird als TRUE zurückgegeben. *expr* muss ein relativ einfacher Ausdruck sein, der nur Spalten, Variable und Literale referenziert. Unterabfragen und Funktionen sind nicht gestattet.

Wenn die ansinull-Option auf "On" gesetzt ist, generiert die Auswertung einer Aggregatfunktion mit Ausnahme von COUNT(\*) für einen Ausdruck, der mindestens ein NULL enthält, möglicherweise eine Warnung (SQLSTATE=01003). Siehe „Nullwert in Aggregatfunktion eliminiert“ [[Fehlermeldungen](#)].

Wenn die ansinull-Option auf "Off" gesetzt ist, wird diese Warnung nicht angezeigt.

### Hinweis

- Alle SQL-Anweisungen, die eine WHERE-, HAVING- oder ON-Klausel enthalten, werden durch die ansinull-Option beeinflusst. Außerdem wird jeder beliebige Ausdruck in einer solchen Anweisung durch die ansinull-Option beeinflusst.
- In Adaptive Server Enterprise 12.5 wurde für LIKE-Prädikate mit einer NULL-Musterzeichenfolge eine Änderung eingeführt, wenn die ansinull-Option auf "Off" gesetzt ist. In SQL Anywhere bleiben LIKE-Prädikate durch die Einstellung von "ansinull" unbeeinflusst.

### Siehe auch

- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET-Anweisung [T-SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- ansinull-Verbindungseigenschaft auf Seite 712
- „Eigenschaften von Sybase Open Client- und jConnect-Verbindungen“ auf Seite 1571

## auditing-Option

Aktiviert und deaktiviert Auditing in der Datenbank

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option schaltet Auditing ein und aus.

Beim Auditing handelt es sich um die Aufzeichnung detaillierter Informationen über zahlreiche Ereignisse in der Datenbank. Die Aufzeichnung erfolgt im Transaktionslog. Auditing bietet einige Sicherheitskomponenten, beeinträchtigt aber die Performance. Wenn Sie Auditing bei einer Datenbank aktivieren, müssen Sie das Transaktionslog weiterhin verwenden. Sie müssen Auditing deaktivieren, bevor Sie das Transaktionslog deaktivieren. Datenbanken mit aktiviertem Auditing können nicht im schreibgeschützten Modus gestartet werden.

Damit die auditing-Option funktioniert, müssen Sie sie auf "On" setzen und außerdem mithilfe der sa\_enable\_auditing\_type-Systemprozedur angeben, auf welche Arten von Informationen sich das Auditing beziehen soll. Das Auditing erfolgt nicht, wenn eine der folgenden Bedingungen zutrifft:

- Die auditing-Option ist auf "Off" gesetzt.
- Die Auditing-Optionen wurden deaktiviert.

Wenn Sie die auditing-Option auf "On" setzen und keine Auditing-Optionen eingeben, werden alle Arten von Audit-Daten registriert. Alternativ können Sie mithilfe der sa\_enable\_auditing\_type-Systemprozedur eine Kombination der folgenden Aktivitäten erfassen: Berechtigungsprüfungen, Verbindungsversuche, DDL-Anweisungen, PUBLIC-Optionen und Trigger.

### Siehe auch

- „Audits von Datenbankaktivitäten“ auf Seite 1416
- „sa\_audit\_string-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_enable\_auditing\_type-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_disable\_auditing\_type-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- auditing-Verbindungseigenschaft auf Seite 713

### Beispiel

Mit der folgenden Anweisung wird Auditing für die Datenbank aktiviert.

```
SET OPTION PUBLIC.auditing = 'On';
```

## auditing\_options-Option (für die Verwendung durch das System reserviert)

Diese Option ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.

## auto\_commit\_on\_create\_local\_temp\_index-Option

Steuert, ob der Datenbankserver eine COMMIT-Anweisung ausführt, bevor ein Index in einer lokalen temporären Tabelle erstellt wird.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

## Bemerkungen

Wenn diese Option auf "On" gesetzt ist, führt der Datenbankserver eine COMMIT-Anweisung aus, bevor ein Index in einer lokalen temporären Tabelle erstellt wird. Falls die COMMIT-Anweisung fehlschlägt, schlägt der Vorgang fehl oder wird zurückgesetzt. Wenn diese Option auf "Off" gesetzt ist (Standardwert), wird keine COMMIT-Anweisung ausgeführt, wodurch Prozeduren zugelassen werden, bei denen der Index als Teil eines atomaren Vorgangs benötigt wird (z.B. Trigger, UPDATE-Anweisung, INSERT-Anweisung, DELETE-Anweisung oder FROM-Klausel).

## Siehe auch

- „CREATE INDEX-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## background\_priority-Option [nicht mehr empfohlen]

Nicht mehr empfohlen. Begrenzt die Performance-Belastung anderer Verbindungen durch die aktuelle Verbindung

## Zulässige Werte

On, Off

## Standardwert

Off

## Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

Wenn Sie diese Option temporär setzen, gilt diese Einstellung nur für die aktuelle Verbindung. Unterschiedliche Verbindungen mit derselben Benutzer-ID haben unterschiedliche Einstellungen für diese Option.

Die abfrageinterne Parallelität wird nicht bei Verbindungen verwendet, für die background\_priority aktiviert ist.

## Bemerkungen

Wenn diese Option auf "On" gesetzt ist, werden Anforderungen auf der Prioritätsstufe "Hintergrund" ausgeführt. Wenn Sie diese Option auf Off setzen, werden Abfragen mit der Priorität ausgeführt, die mit der Option "Priority" festgelegt wird.

## Siehe auch

- „priority-Option“ auf Seite 656
- „max\_priority-Option“ auf Seite 632
- background\_priority-Verbindungseigenschaft auf Seite 713

## blob\_threshold-Option [SQL Remote]

Steuert die Größe des Wertes, den der Nachrichtenagent als langes Objekt ("Blob") behandelt

### Zulässige Werte

Ganzzahl, in Byte

### Standardwert

256

### Bemerkungen

Jeder Wert, der länger ist als blob\_threshold, wird als Blob repliziert. Das bedeutet, dass er in Stücke geteilt und in Abschnitten repliziert wird, bevor er unter Verwendung einer SQL-Variablen wieder zusammengefügt wird und die Stücke am Empfangsort verknüpft werden.

Jede SQL-Anweisung muss in eine Nachricht passen. Setzen Sie daher den Wert dieser Option nicht auf eine Größe, die größer ist als Ihre Nachrichtengröße (standardmäßig 50 kB).

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „BLOBs“ [[SQL Remote](#)]

## blocking-Option

Steuert das Antwortverhalten auf Sperrenkonflikte

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Wenn die blocking-Option auf "On" eingestellt ist, wartet jede Transaktion, die eine Sperre zu erwerben versucht, die mit einer vorhandenen, von einer anderen Transaktion gehaltenen Sperre kollidiert, bis alle kollidierenden Sperren freigegeben werden oder blocking\_timeout erreicht wird. Wenn die Sperre nicht innerhalb der in blocking\_timeout angegebenen Zeit freigegeben wurde, wird an die wartende Transaktion ein Fehlerstatus übermittelt. Wenn die blocking-Option auf "Off" eingestellt ist, erhält die Transaktion, die eine kollidierende Sperre zu erwerben versucht, einen Fehler.

Der Wert für die blockierende Verbindungseigenschaft kann während bestimmter Vorgänge (zum Beispiel beim Aktualisieren einer materialisierten Ansicht) vorübergehend auf "Off" gesetzt werden, was dann einen Fehler verursachen kann. Siehe „Benutzer '%1' hat die Zeile in '%2' gesperrt“ [[Fehlermeldungen](#)].

### Siehe auch

- „blocking\_timeout-Option“ auf Seite 587
- „Die Blocking-Option“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- blocking-Verbindungseigenschaft auf Seite 713

## blocking\_others\_timeout-Option

Legt fest, wie lange die Zeilen- und Tabellensperren der aktuellen Verbindung durch eine andere Verbindung blockiert werden, bevor die aktuelle Verbindung zurückgesetzt wird. So können Sie zum Beispiel vermeiden, dass eine Aufgabe mit niedriger Priorität andere Verbindungen länger als angegeben blockiert.

### Zulässige Werte

Ganzzahl, in Millisekunden

### Standardwert

0

### Bereich

Kann nur temporär, für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Wenn diese Option auf 0 gesetzt ist, können andere Verbindungen die aktuelle Verbindung für einen unbestimmten Zeitraum blockieren.

Falls eine andere Verbindung auf der aktuellen Verbindung für länger als die durch diese Option angegebene Anzahl von Millisekunden blockiert wird, wird die aktuelle Verbindung zurückgesetzt. Falls auf der aktuellen Verbindung zum gegebenen Zeitpunkt eine Anforderung ausgeführt wird, wird die Anforderung unterbrochen. Es wird ein Fehler zurückgegeben, wenn die Verbindung zurückgesetzt wurde. Der Fehler wird möglicherweise zwei Mal zurückgegeben, wenn eine Anforderung unterbrochen werden muss. Wenn die Verbindung inaktiv war, wird sie sofort zurückgesetzt. Die Anwendung muss bereit sein, fehlzuschlagen oder nach einer Wartezeit einen erneuten Versuch vorzunehmen, wenn sie zurückgesetzt wird.

#### Hinweis

Sperren, die mit der Anweisung `LOCK TABLE Tabellenname WITH HOLD` erstellt wurden, werden zurückgesetzt. Wenn eine Verbindung eine Fehlermeldung erhält, die besagt, dass ein Vorgang aufgrund eines blocking\_others\_timeout-Fehlers zurückgesetzt wurde, wird diese Fehlermeldung bei jeder Anforderung ausgegeben, bis die Verbindung getrennt wird.

**Siehe auch**

- [blocking\\_others\\_timeout](#)-Verbindungseigenschaft auf Seite 713
- „blocking\_timeout-Option“ auf Seite 587
- „Transaktion blockieren und Deadlock“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „LOAD TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**blocking\_timeout-Option**

Steuert, wie lange eine Transaktion auf die Zuweisung einer Sperre wartet.

**Zulässige Werte**

Ganzzahl, in Millisekunden

**Standardwert**

0

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn die Option blocking auf "On" gesetzt ist, wartet jede Transaktion, die eine bereits belegte Sperre angefordert hat, so viele Millieskunden, wie in blocking\_timeout angegeben, auf die Freigabe der Sperre. Wenn die Sperre nicht innerhalb der in blocking\_timeout angegebenen Zeit freigegeben wurde, wird an die wartende Transaktion ein Fehlerstatus übermittelt.

Wenn Sie diese Option auf "0" setzen, warten alle Transaktionen, die eine bereits belegte Sperre angefordert haben, bis alle konkurrierenden Transaktionen diese Sperre freigegeben haben.

**Siehe auch**

- „blocking-Option“ auf Seite 585
- [blocking\\_others\\_timeout](#)-Verbindungseigenschaft auf Seite 713
- „request\_timeout-Option“ auf Seite 664
- „Deadlocks“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- [blocking\\_timeout](#)-Verbindungseigenschaft auf Seite 714

**chained-Option**

Steuert den Transaktionsmodus beim Fehlen einer BEGIN TRANSACTION-Anweisung

**Zulässige Werte**

On, Off

### Standardwert

On

Off für Sybase Open Client- und jConnect-Verbindungen

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Steuert den Transact-SQL-Transaktionsmodus. Im unverketteten Modus (chained=Off) wird jede Anweisung individuell festgeschrieben, wenn nicht eine ausdrückliche BEGIN TRANSACTION-Anweisung zum Starten einer Transaktion ausgeführt wird. Im verketteten Modus (chained=On) wird eine Transaktion ausdrücklich vor jeder Anweisung zum Datenabruf oder zur Änderung gestartet.

### Siehe auch

- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Autocommit-Implementierung“ [*SQL Anywhere Server - Programmierung*]
- „Transaktionen“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- chained-Verbindungseigenschaft auf Seite 714

## checkpoint\_time-Option

Legt die maximale Anzahl von Minuten fest, für die der Datenbankserver läuft, ohne einen Checkpoint auszuführen.

### Zulässige Werte

Ganzzahl

### Standardwert

60

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Sie müssen den Datenbankserver herunterfahren und neu starten, damit sich die Änderung auswirkt.

### Bemerkungen

Diese Option wird mit der Option recovery\_time verwendet, mit deren Hilfe entschieden wird, wann Checkpoints gesetzt werden sollen.

**Siehe auch**

- „Checkpoint-Logs“ auf Seite 143
- „recovery\_time-Option“ auf Seite 661
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077
- „Datenbankserveroption -gc “ auf Seite 239
- „Datenbankserveroption -m “ auf Seite 265
- „CHECKPOINT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- checkpoint\_time-Verbindungseigenschaft auf Seite 715

## cis\_option-Option

Mit dieser Funktion wird gesteuert, ob die Informationen der TDS-Fehlersuche im Fenster der Datenbankservermeldungen angezeigt werden

**Zulässige Werte**

0, 7

**Standardwert**

0

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Mit dieser Option wird gesteuert, wie bei Fernzugriff Informationen über die Ausführung von Abfragen in einer entfernten Datenbank im Fenster der Datenbankservermeldungen erscheinen sollen. Setzen Sie diese Option auf "7", damit im Fenster der Datenbankservermeldungen Informationen über die Fehlersuche angezeigt werden. Wenn diese Option auf "0" (Standardwert) gesetzt wird, werden im Fenster der Datenbankservermeldungen keine Informationen zur Fehlersuche über den Ferndatenzugriff angezeigt.

Wenn Sie die Fernprotokollierung aktiviert haben, werden die Protokollierungsinformationen im Meldungsfenster des Datenbankservers angezeigt. Sie können diese Ausgabe in eine Datei schreiben, indem Sie die Serveroption -o verwenden, wenn Sie den Datenbankserver starten.

**Siehe auch**

- „Datenbankserveroption -o “ auf Seite 268
- „Systemanbindungstests“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- cis\_option-Verbindungseigenschaft auf Seite 715

## cis\_rowset\_size-Option

Setzt die Anzahl der Zeilen, die vom Fremdserver bei jedem Abruf zurückgegeben werden

### Zulässige Werte

Ganzzahl

### Standardwert

50

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wirkt sich aus, wenn eine neue Verbindung mit einem Fremdserver hergestellt wird.

### Bemerkungen

Diese Option setzt den ODBC-Wert FetchArraySize, wenn ODBC verwendet wird, um eine Verbindung mit einer entfernten Datenbank einzurichten.

### Siehe auch

- [cis\\_rowset\\_size-Verbindungseigenschaft auf Seite 715](#)

## close\_on\_endtrans-Option

Steuert das Schließen der Cursor am Ende einer Transaktion

### Zulässige Werte

On, Off

### Standardwert

On

Off bei jConnect-Verbindungen

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn close\_on\_endtrans auf "On" gesetzt ist, wird ein Cursor immer beim Festschreiben einer Transaktion geschlossen, sofern der Cursor nicht mit WITH HOLD geöffnet wurde. Das Verhalten beim Zurücksetzen einer Transaktion wird von der Option ansi\_close\_cursors\_on\_rollback bestimmt.

Wenn close\_on\_endtrans auf "Off" gesetzt ist, wird ein Cursor beim Festschreiben oder Zurücksetzen nicht geschlossen, unabhängig von der Einstellung der Option ansi\_close\_cursors\_on\_rollback und egal, ob der Cursor mit WITH HOLD geöffnet wurde oder nicht.

Wenn diese Option auf "Off" gesetzt wird, verhält sich SQL Anywhere kompatibel zu Adaptive Server Enterprise.

**Siehe auch**

- „ansi\_close\_cursors\_on\_rollback-Option“ auf Seite 576
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsoptionen“ auf Seite 559
- „SET-Anweisung [T-SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Eigenschaften von Sybase Open Client- und jConnect-Verbindungen“ auf Seite 1571
- close\_on\_endtrans-Verbindungseigenschaft auf Seite 716

**collect\_statistics\_on\_dml\_updates-Option**

Steuert das Sammeln von Statistiken während der Ausführung von Daten-ändernden DML-Anweisungen wie INSERT, DELETE und UPDATE

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Der Datenbankserver aktualisiert Statistiken während der normalen Anweisungsverarbeitung und verwendet die erfassten Statistiken zur automatischen Optimierung der Spaltenstatistiken. Setzen Sie die Option collect\_statistics\_on\_dml\_updates auf "Off", um das Aktualisieren von Statistiken während der Ausführung von Daten-ändernden DML-Anweisungen wie INSERT, DELETE und UPDATE zu deaktivieren.

Unter normalen Bedingungen muss diese Option nicht deaktiviert werden. In Umgebungen, in denen große Datenmengen häufig geändert werden, kann das Setzen dieser Option auf "Off" jedoch die Performance verbessern, sofern update\_statistics auf "On" gesetzt ist.

Der Unterschied zwischen der Option collect\_statistics\_on\_dml\_updates und der Option update\_statistics liegt darin, dass die Option update\_statistics die tatsächliche Anzahl der Zeilen, die das Prädikat erfüllen, mit der Anzahl der Zeilen vergleicht, bei denen eine Prädikaterfüllung geschätzt wird, und dann die Schätzung entsprechend aktualisiert. Die Option collect\_statistics\_on\_dml\_updates ändert die Spaltenstatistiken aufgrund der Werte der spezifischen Zeilen, die eingefügt, aktualisiert oder gelöscht werden.

**Siehe auch**

- „update\_statistics-Option“ auf Seite 701
- „Tipp: Spaltenstatistiken aktualisieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- collect\_statistics\_on\_dml\_updates-Verbindungseigenschaft auf Seite 716

## compression-Option [SQL Remote]

Legt den Grad der Komprimierung für SQL Remote-Nachrichten fest

### Zulässige Werte

Ganzzahl von -1 bis 9

### Standardwert

6

### Bemerkungen

Die Werte haben die folgende Bedeutung:

- **-1** Nachrichten im Version 5-Format versenden. Der Nachrichtenagent der Version 5 kann keine Nachrichten lesen, die vom Nachrichtenagenten der Version 6 oder höher gesendet werden. Achten Sie darauf, dass die compression-Option auf -1 eingestellt bleibt, bis alle Nachrichtenagenten in Ihrem System auf Version 6 oder höher umgestellt sind.
- **0** Keine Komprimierung
- **1 bis 9** Zunehmende Grade der Komprimierung. Das Erstellen von Nachrichten mit hoher Komprimierung kann länger als mit niedriger Komprimierung dauern.

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „Nachrichtengröße“ [[SQL Remote](#)]

## conn\_auditing-Option

Steuert, ob Auditing bei jeder Verbindung aktiviert oder deaktiviert ist, wenn die auditing-Option auf "On" gesetzt ist.

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Die Einstellung der conn\_auditing-Option wirkt sich nur aus, wenn sie in eine Login-Prozedur gesetzt ist (durch die login\_procedure-Datenbankoption angegeben). Das Setzen von conn\_auditing auf "On" schaltet Auditing bei der Verbindung ein. Es werden jedoch keine Audit-Daten aufgezeichnet, wenn die

auditing-Option nicht ebenfalls auf "On" gesetzt ist. Um zu bestimmen, ob einer Verbindung von der Audit-Funktion überprüft wird, führen Sie die folgende Anweisung aus:

```
SELECT CONNECTION_PROPERTY ( 'conn_auditing' );
```

### Siehe auch

- „Auditing konfigurieren (Sybase Central)“ auf Seite 1418
- „auditing-Option“ auf Seite 582
- „login\_procedure-Option“ auf Seite 625
- conn\_auditing-Verbindungseigenschaft auf Seite 717

## connection\_authentication-Option

Gibt eine Authentifizierungszeichenfolge an, mit der die Anwendungssignatur für authentifizierte Anwendungen anhand der Datenbanksignatur überprüft wird

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge

### Bereich

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Diese Option ist nur wirksam, wenn Sie die OEM Edition des SQL Anywhere-Datenbankservers verwenden.

Authentifizierte Anwendungen müssen die connection\_authentication-Datenbankoption bei jeder Verbindung unmittelbar nach der Herstellung der Verbindung setzen. Wenn die Signatur überprüft wird, ist die Verbindung authentifiziert und es gelten nur die Einschränkungen, die durch die SQL-Privilegien festgelegt sind. Wenn die Signatur nicht überprüft wird, ist die Verbindung auf die Aktionen beschränkt, die von nicht authentifizierten Anwendungen zugelassen werden.

Setzen Sie die connection\_authentication-Option mithilfe des Schlüsselworts TEMPORARY nur für die Dauer der aktuellen Verbindung. Die folgende SQL-Anweisung authentifiziert die Verbindung:

```
SET TEMPORARY OPTION connection_authentication =  
    'company = company-name;  
    application = application-name;  
    signature = application-signature';
```

Der *company-name* und der *application-name* müssen mit denjenigen in der Authentifizierungsanweisung für die Datenbank übereinstimmen. Die *application-signature* ist die Anwendungssignatur, die Sie von Sybase erhalten haben.

Wenn Ihr Firmenname Anführungszeichen, Apostrophe oder andere Sonderzeichen enthält, müssen Sie diese in der Zeichenfolge verdoppeln, damit der Name akzeptiert wird.

Weitere Hinweise zur Konfiguration und Verwendung der OEM Edition von SQL Anywhere finden Sie unter „[Authentifizierte SQL Anywhere-Anwendungen](#)“ auf [Seite 194](#).

### Siehe auch

- „[database\\_authentication-Option](#)“ auf [Seite 597](#)
- [connection\\_authentication-Verbindungseigenschaft](#) auf [Seite 717](#)

### Beispiel

Das folgende Beispiel verwendet eine Authentifizierungszeichenfolge, die Sonderzeichen enthält:

```
SET TEMPORARY OPTION connection_authentication=  
'Company = Joe''s Garage;  
Application = Joe''s Program;  
Signature = 0fa55157edb8e14d818e...';
```

## continue\_after\_raiserror-Option

Steuert Verhalten, das einer RAISERROR-Anweisung folgt

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Die Anweisung RAISERROR wird innerhalb von Prozeduren und Triggern verwendet, um einen Fehler zu erzeugen. Wenn die Option auf "Off" gesetzt ist, wird die Ausführung der Prozedur oder des Triggers gestoppt, sobald die Anweisung RAISERROR erkannt wird.

Diese Option wird innerhalb des TRY-Blocks einer BEGIN...END-Anweisung ignoriert.

Wenn Sie die Option `continue_after_raiserror` auf "On" setzen, signalisiert die Anweisung RAISERROR nicht länger einen Ausführen-Beenden-Fehler. Stattdessen werden der RAISERROR-Statuscode und die Meldung gespeichert, und der allerletzte "RAISERROR" beim Beenden der Prozedur zurückgegeben. Wenn die Prozedur, die RAISERROR verursacht hat, aus einer anderen Prozedur aufgerufen wurde, wird RAISERROR erst zurückgegeben, wenn die äußerste aufgerufene Prozedur beendet ist.

Dazwischenliegende RAISERROR-Statusangaben und -Codes gehen verloren, nachdem die Prozedur beendet ist. Falls in der Rückgabezeit ein Fehler im Zusammenhang mit RAISERROR auftritt, werden die

Informationen für den neuen Fehler zurückgegeben, und die RAISERROR-Informationen gehen verloren. Die Anwendung kann unmittelbar RAISERROR-Statistiken abfragen, indem sie die globale Variable @@error an verschiedenen Ausführungspunkten untersucht.

Die Einstellung der Option `continue_after_raiserror` wird benutzt, um das Verhalten nach einer RAISERROR-Anweisung nur dann zu steuern, wenn die Option `on_tsql_error` auf "Conditional" gesetzt ist (Standardwert). Wenn Sie die Option `on_tsql_error` auf "Stop" oder "Continue" setzen, hat die Einstellung `on_tsql_error` Vorrang vor der Einstellung `continue_after_raiserror`.

### Siehe auch

- „`on_tsql_error`-Option“ auf Seite 646
- „Kompatibilitätsoptionen“ auf Seite 559
- „RAISERROR-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `continue_after_raiserror`-Verbindungseigenschaft auf Seite 717
- „BEGIN-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## conversion\_error-Option

Steuert die Berichterstellung von Datentyp-Konvertierungsfehlern, indem sie Informationen aus der Datenbank abrufen

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option steuert, ob Datentyp-Konvertierungsfehler beim Abrufen oder Einfügen von Daten aus der oder in die Datenbank von der Datenbank als Fehler (`conversion_error` auf "On" gesetzt) oder als Warnung (`conversion_error` auf "Off" gesetzt) gemeldet werden.

Wenn `conversion_error` auf "On" gesetzt ist, wird der Fehler `SQLE_CONVERSION_ERROR` erzeugt. Wenn die Option auf "Off" gesetzt ist, wird die Warnung `SQLE_CANNOT_CONVERT` erzeugt.

Wenn Konvertierungsfehler nur als Warnung ausgegeben werden, wird NULL anstelle des Werts verwendet, der nicht konvertiert werden konnte. In Embedded SQL wird eine Indikatorvariable für die Spalten auf "-2" gesetzt, die den Fehler verursacht haben.

### Siehe auch

- „Indikatorvariablen: Konvertierungsfehler“ [[SQL Anywhere Server - Programmierung](#)]
- „Konvertierungsfehler beim Import“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Kompatibilitätsoptionen“ auf Seite 559
- `conversion_error`-Verbindungseigenschaft auf Seite 717

## cooperative\_commit\_timeout-Option

Bestimmt, wann ein COMMIT-Eintrag im Transaktionslog auf die Festplatte geschrieben wird

### Hinweis

Ab Version 11 wird diese Optionseinstellung ignoriert, da das Festschreibeverhalten automatisch abgestimmt wird.

### Zulässige Werte

Ganzzahl, in Millisekunden

### Standardwert

250

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option ist nur von Bedeutung, wenn `cooperative_commits` auf "On" gesetzt ist. Der Datenbankserver wartet die angegebene Zeit von Millisekunden vor dem Schreiben auf der Festplatte, bis andere Verbindungen eine Seite des Logs gefüllt haben. Die Standardeinstellung ist 250 Millisekunden.

### Siehe auch

- „`cooperative_commits`-Option“ auf Seite 596
- „`delayed_commit_timeout`-Option“ auf Seite 606
- „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `cooperative_commit_timeout`-Verbindungseigenschaft auf Seite 717

## cooperative\_commits-Option

Steuert, wann Festschreibungen auf die Festplatte geschrieben werden

### Hinweis

Ab Version 11 wird diese Optionseinstellung ignoriert, da das Festschreibeverhalten automatisch abgestimmt wird.

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn cooperative\_commits auf "Off" gesetzt ist, wird ein COMMIT nach dem Empfang vom Datenbankserver auf die Festplatte geschrieben und die Anwendung kann dann fortfahren.

Wenn cooperative\_commits auf "On" (Standardwert) gesetzt ist, schreibt der Datenbankserver den COMMIT nicht unmittelbar auf die Festplatte. Die Anwendung wartet stattdessen bis zur maximalen, mit der durch die Option cooperative\_commit\_timeout festlegten Dauer, um weitere Daten in die Seiten einzulesen, bevor die Seiten auf die Festplatte geschrieben werden.

Wenn Sie cooperative\_commits auf "On" setzen und die Einstellung cooperative\_commit\_timeout erhöhen, wird der gesamte Datenbankserver-Durchsatz verbessert, indem die Festplatten-I/O-Vorgänge aufgeteilt werden. Dies geht aber auf Kosten einer längeren Bearbeitungszeit für jede einzelne Verbindung.

Wenn sowohl cooperative\_commits als auch delayed\_commits auf gesetzt sind, und das Intervall COOPERATIVE\_COMMIT\_TIMEOUT verstreicht, ohne dass die Seiten geschrieben wurden, wird die Anwendung fortgesetzt (als ob das COMMIT ausgeführt worden wäre), und das restliche Intervall (delayed\_commit\_timeout - cooperative\_commit\_timeout) wird als delayed\_commits-Intervall verwendet. Die Seiten werden geschrieben, auch wenn sie nicht voll sind.

**Siehe auch**

- „delayed\_commits-Option“ auf Seite 606
- „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- cooperative\_commits-Verbindungseigenschaft auf Seite 717

## **database\_authentication-Option**

Legt die Authentifizierungszeichenfolge für eine Datenbank fest

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Leere Zeichenfolge

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Sie müssen die Datenbank neu starten, damit diese Option wirksam wird.

### Bemerkungen

Diese Option ist nur wirksam, wenn Sie die OEM Edition des SQL Anywhere-Datenbankservers verwenden.

Wenn eine Datenbank authentifiziert wird, können nur Verbindungen, für die die richtige Authentifizierungssignatur angegeben wird, Vorgänge in der Datenbank durchführen. Nicht authentifizierte Verbindungen arbeiten im schreibgeschützten Modus. Wenn Sie mit authentifizierten Datenbanken arbeiten möchten, verwenden Sie die OEM-Edition von SQL Anywhere.

Um eine Datenbank zu authentifizieren, geben Sie die `database_authentication`-Option für die Datenbank an:

```
SET OPTION PUBLIC.database_authentication =  
'company = company-name;  
application = application-name;  
signature = database-signature';
```

Die Argumente *company-name* und *application-name* sind die Werte, die Sie beim Erwerb Ihrer Signatur an Sybase übermittelt haben, und *database-signature* ist die Datenbanksignatur, die Sie von Sybase erhalten haben.

Wenn Ihr Firmenname Anführungszeichen, Apostrophe oder andere Sonderzeichen enthält, müssen Sie diese in der Zeichenfolge verdoppeln, damit der Name akzeptiert wird.

Wenn der Datenbankserver eine authentifizierte Datenbank lädt, wird eine Meldung im Meldungsfenster des Datenbankservers angezeigt, die die authentifizierte Firma und Anwendung enthält. Diese Meldung ist die Bestätigung dafür, dass die `database_authentication`-Option wirksam ist. Die Meldung hat folgende Form:

```
Diese Datenbank hat eine Lizenz für folgende Nutzung:  
Anwendung: Anwendungsname  
Firma: Firmenname
```

Sie können die Authentifizierungsanweisung in einem SQL-Skript speichern, um eine wiederholte Eingabe der langen Signatur zu vermeiden. Wenn Sie die Authentifizierungsanweisung in der Datei `%SQLANY16%\Scripts\authenticate.sql` speichern, wird sie jeweils verwendet, wenn Sie eine Datenbank erstellen, neu aufbauen oder ein Upgrade durchführen.

### Siehe auch

- „Authentifizierte SQL Anywhere-Anwendungen“ auf Seite 194
- „Upgrade von authentifizierten Datenbanken“ auf Seite 200
- „`connection_authentication`-Option“ auf Seite 593
- `database_authentication`-Verbindungseigenschaft auf Seite 718

### Beispiel

```
SET OPTION PUBLIC.database_authentication =  
'company = MyCompany';
```

```
application = MySQLAnywhereApp;  
signature = 0fa55157edb8e14d818e';
```

## date\_format-Option

Legt das Format für Datumsangaben fest, die aus der Datenbank abgerufen werden

### Zulässige Werte

Zeichenfolge

### Standardwert

YYYY-MM-DD

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig
MMM[m...]	Zeichenkurzform für Monate
D	Wochentag einstellig (1 = Sonntag, 7 = Samstag)
DD	Tag des Monats zweistellig
DDD[d...]	Zeichenkurzform für Wochentage
JJJ	Jahrestag von 1 bis 366

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Weitere Hinweise zur Steuerung der Interpretation von Datumsformaten finden Sie unter [„date\\_order-Option“ auf Seite 601](#).

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "mmm" gibt z.B. eine Länge von drei Zeichen für den Monat an.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.
- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein.  
Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.

**Hinweis**  
Wenn Sie die Einstellung für date\_format so ändern, dass das Datumsformat neu geordnet wird, achten Sie darauf, auch die date\_order-Option entsprechend zu ändern, und umgekehrt. Siehe „date\_order-Option“ auf Seite 601.

**Siehe auch**

- „Suchbedingungen, die Datumsangaben vergleichen“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „time\_format-Option“ auf Seite 690
- „timestamp\_format-Option“ auf Seite 692
- „timestamp\_with\_time\_zone\_format-Option“ auf Seite 694
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- date\_format-Verbindungseigenschaft auf Seite 718

**Beispiel**

Die folgende Tabelle verdeutlicht date\_format-Einstellungen anhand der Ausgabe folgender Anweisung, die am Montag, dem 14. April 2008 ausgeführt wurde.

```
SELECT CAST( CURRENT DATE AS VARCHAR );
```

date_format	CURRENT DATE
yyyy/mm/dd/ddd	2008/04/14/mon
yyyy/Mm/Dd/ddd	2008/4/14/mon

<b>date_format</b>	<b>CURRENT DATE</b>
jjj	105
mmm yyyy	apr 2008
Mmm yyyy	Apr 2008
mm-yyyy	04-2008

## date\_order-Option

Steuert die Interpretation von Datumsformaten

### Zulässige Werte

MDY, YMD, DMY

### Standardwert

YMD (dies entspricht den ISO-Datumsformat-Spezifikationen)

Für Sybase Open Client- und jConnect-Verbindungen ist der Standard MDY.

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Die Datenbankoption option date\_order wird verwendet, um zu bestimmen, ob 10/11/12 der 11. Okt. 1912, der 12. Nov. 1910 oder der 10. Nov. 1912 ist.

#### Hinweis

Wenn Sie die Einstellung für date\_order so ändern, dass das Datumsformat neu geordnet wird, achten Sie darauf, auch die Optionen date\_format und timestamp\_format entsprechend zu ändern, und umgekehrt. Siehe „date\_format-Option“ auf Seite 599 und „timestamp\_format-Option“ auf Seite 692.

### Siehe auch

- „Suchbedingungen, die Datumsangaben vergleichen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „sp\_tsql\_environment-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- date\_order-Verbindungseigenschaft auf Seite 718

## db\_publisher-Option

Speichert die Benutzer-ID für den Publikationseigentümer der Datenbank, falls vorhanden.

### Zulässige Werte

-1, NULL oder eine Benutzer-ID

### Standardwert

-1

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Wenn der Publikationseigentümer bereits festgelegt ist, müssen Sie diese Option auf -1 oder NULL setzen, bevor Sie sie auf eine andere Benutzer-ID setzen.

Durch das Ändern eines Publikationseigentümers wird der Wert für den CURRENT PUBLISHER-Spezialwert aktualisiert.

Sie können den db\_publisher-Wert auch mit den Anweisungen GRANT PUBLISH und REVOKE PUBLISH setzen bzw. zurücksetzen.

### Siehe auch

- „GRANT PUBLISH-Anweisung [SQL Remote]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „REVOKE PUBLISH-Anweisung [SQL Remote]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CURRENT PUBLISHER-Spezialwert“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „PUBLISH-Privileg“ [[SQL Remote](#)]

## debug\_messages-Option

Steuert, ob MESSAGE-Anweisungen ausgeführt werden, die eine DEBUG ONLY-Klausel enthalten.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Mit dieser Option können Sie das Verhalten von Meldungen während einer Fehlersuche in gespeicherten Prozeduren und Triggern steuern, die eine MESSAGE-Anweisung mit DEBUG ONLY-Klausel enthalten. Standardmäßig wird diese Option auf "Off" gesetzt und Meldungen werden während der Fehlersuche nicht angezeigt, wenn die Anweisung MESSAGE ausgeführt wird. Wenn Sie debug\_messages auf "On" setzen, können Sie die Meldungen während einer Fehlersuche für alle gespeicherten Prozeduren und Trigger aktivieren.

**Hinweis**

DEBUG ONLY-Meldungen sind kostengünstig, wenn die Option debug\_messages auf "Off" gesetzt wurde, sodass diese Anweisungen auf einem Produktionssystem normalerweise in gespeicherten Prozeduren belassen werden können. Verwenden Sie sie jedoch dort mit Vorsicht, wo sie häufig ausgeführt würden, da sie andernfalls zu Performance-Einbußen führen können.

**Siehe auch**

- „MESSAGE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- [debug\\_messages-Verbindungseigenschaft auf Seite 718](#)

**dedicated\_task-Option**

Weist eine Anforderungs-Handling-Task zu, um Anforderungen von einer einzelnen Verbindung abzuwickeln.

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung eingestellt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Wenn die Verbindungsoption dedicated\_task auf "On" gesetzt ist, wird exklusiv eine Anforderungs-Handling-Aufgabe zugewiesen, um die Anforderungen der Verbindung abzuwickeln. Indem Sie vorab eine Verbindung herstellen, bei der diese Option aktiviert ist, können Sie Informationen über den Status des Datenbankservers sammeln, falls er anderweitig nicht antwortet.

**Siehe auch**

- [dedicated\\_task-Verbindungseigenschaft auf Seite 718](#)

## default\_dbspace-Option

Ändert den Standard-DBSpace, in dem Tabellen erstellt werden

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Für jede Datenbank können Sie zusätzlich zum System-(Haupt-)DBSpace bis zu zwölf weitere DBSpaces erstellen. Wenn eine Tabelle ohne Angabe eines DBSpaces erstellt wird, wird der von dieser Optionseinstellung benannte DBSpace verwendet. Wenn diese Option nicht gesetzt, auf eine leere Zeichenfolge gesetzt oder auf "system" gesetzt ist, wird der System-DBSpace verwendet.

Wenn Sie temporäre Tabellen oder Indizes erstellen, werden sie immer im DBSpace TEMPORARY gespeichert, unbeschadet der Einstellung der Option default\_dbspace. Wenn Sie beim Erstellen einer Basistabelle die IN-Klausel angeben, wird der in der IN-Klausel angegebene DBSpace benutzt und nicht der mit der option default\_dbspace angegebene.

Wenn alle Tabellen in einem anderen DBSpace als dem System-DBSpace erstellt werden, wird der System-DBSpace nur für das Checkpoint-Log und die Systemtabellen verwendet. Dies ist nützlich, wenn Sie das Checkpoint-Log aus Performance-Gründen auf einer von den übrigen Datenbankobjekten separaten Festplatte platzieren möchten. Sie platzieren das Checkpoint-Log auf eine separate Festplatte, indem Sie alle CREATE TABLE-Anweisungen dahingehend ändern, dass sie den DBSpace angeben, oder indem Sie diese Option ändern, bevor Sie Tabellen erstellen.

### Siehe auch

- „Zusätzliche Hinweise zu DBSpaces“ auf Seite 128
- „Tipp: Verschiedene Dateien auf verschiedene Geräte platzieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „CREATE DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER DBSPACE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DBSpace-Erstellung“ auf Seite 130
- „Datenbankoption -ds “ auf Seite 325
- default\_dbspace-Verbindungseigenschaft auf Seite 718

### Beispiel

Im folgenden Beispiel wird ein neuer DBSpace mit dem Namen MyLibrary erstellt. Der Standard-DBSpace wird dann auf den DBSpace MyLibrary gesetzt und die Tabelle LibraryBooks wird im DBSpace MyLibrary und nicht im System-DBSpace gespeichert.

```
CREATE DBSPACE MyLibrary
AS 'c:\\dbfiles\\library.db';
SET OPTION default_dspace = 'MyLibrary';
CREATE TABLE LibraryBooks (
    title CHAR(100),
    author CHAR(50),
    isbn CHAR(30),
);
```

## default\_timestamp\_increment-Option

Gibt an, wie viele Mikrosekunden in einer Spalte mit dem Standardwert `TIMESTAMP` oder `UTC` `TIMESTAMP` addiert werden, um die Werte in der Spalte eindeutig zu halten, wenn eine Zeile, die die Spalte enthält, eingefügt oder aktualisiert wird.

### Zulässige Werte

Ganzzahl zwischen 1 und 1000000

### Standardwert

1

### Bereich

Kann für eine einzelne Verbindung oder für `PUBLIC` gesetzt werden. Sie müssen das `SET ANY PUBLIC` `OPTION`-Systemprivileg haben, um diese Option für `PUBLIC` oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Da ein `TIMESTAMP`-Wert in SQL Anywhere auf sechs Dezimalstellen genau ist, wird standardmäßig 1 Mikrosekunde (0,000001 Sekunden) addiert, um zwischen zwei identischen `TIMESTAMP`- bzw. `TIMESTAMP WITH TIME ZONE`-Werten unterscheiden zu können.

Wenn mehrere Zeilen, die eine Spalte mit dem Attribut `DEFAULT TIMESTAMP` oder `DEFAULT UTC` `TIMESTAMP` enthalten, aktualisiert werden und die Spalte selbst nicht explizit aktualisiert wird, erhält die Spalte einen eindeutigen Wert für jede aktualisierte Zeile. Beispiel: Drei Zeilen mit einer Spalte vom Typ `TIMESTAMP WITH TIME ZONE` mit dem `DEFAULT UTC` `TIMESTAMP`-Attribut werden aktualisiert. Die Zeilen werden um '2011-04-01 12: 47: 52.724000+00: 00' aktualisiert, aber jede Zeile enthält einen eindeutigen `UTC` `TIMESTAMP`-Wert.

```
2011-04-01 12:47:52.724000+00:00
2011-04-01 12:47:52.724001+00:00
2011-04-01 12:47:52.724002+00:00
```

Bestimmte Software, wie Microsoft Access, kürzt `TIMESTAMP`-Werte auf drei Dezimalstellen und macht dadurch gültige Vergleiche zum Problem. Sie können die Option `truncate_timestamp_values` auf "On" setzen, um die Anzahl der Dezimalstellen festzulegen, die SQL Anywhere zur Aufrechterhaltung der Systemverträglichkeit mit anderen Datenbanken berücksichtigt.

Wenn Sie diese Option bei der MobiLink-Synchronisation verwenden möchten, setzen Sie sie vor der Durchführung der ersten Synchronisation.

### Siehe auch

- „truncate\_timestamp\_values-Option“ auf Seite 697
- „TIMESTAMP-Spezialwert“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „UTC TIMESTAMP-Spezialwert“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- default\_timestamp\_increment-Verbindungseigenschaft auf Seite 718

## delayed\_commit\_timeout-Option

Gibt die maximale Verzögerung zwischen einer Anwendung an, die ein COMMIT ausführt und der COMMIT-Anweisung, die auf die Festplatte geschrieben wird, wenn die delayed\_commits-Option auf "On" gesetzt ist.

### Zulässige Werte

Ganzzahl, in Millisekunden

### Standardwert

500

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option ist nur von Bedeutung, wenn delayed\_commits auf "On" gesetzt ist. Sie legt fest, wann ein COMMIT-Eintrag im Transaktionslog auf die Festplatte geschrieben wird. Bei delayed\_commits auf "On" wartet der Datenbankserver vor dem Schreiben der aktuellen Seite auf die Festplatte die Zeitspanne in Millisekunden ab, die in der Option delayed\_commit\_timeout gesetzt wurde, bis andere Verbindungen eine Seite des Logs gefüllt haben.

### Siehe auch

- „delayed\_commits-Option“ auf Seite 606
- „cooperative\_commit\_timeout-Option“ auf Seite 596
- „cooperative\_commits-Option“ auf Seite 596
- „COMMIT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- delayed\_commit\_timeout-Verbindungseigenschaft auf Seite 718

## delayed\_commits-Option

Ermittelt, wann der Datenbankserver nach einem COMMIT die Kontrolle an eine Anwendung zurückgibt

### Zulässige Werte

On, Off

**Standardwert**

Off (dies entspricht dem Verhalten von ISO COMMIT)

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn die Option auf "On" gesetzt ist, antwortet der Datenbankserver auf eine COMMIT-Anweisung unmittelbar, anstatt zu warten, bis der Transaktionslogeintrag für COMMIT auf die Festplatte geschrieben wurde. Wenn die Option auf "Off" gesetzt ist, muss die Anwendung warten, bis die COMMIT-Anweisung auf die Festplatte geschrieben wurde.

Wenn die Option auf "On" gesetzt ist, wird das Log auf die Festplatte geschrieben, sobald die Logseite voll oder die Zeit gemäß der Optionseinstellung `delayed_commit_timeout` abgelaufen ist, je nachdem, was zuerst geschieht. Die Wahrscheinlichkeit ist gering, dass eine Transaktion während des Festschreibens verloren geht, falls ein Systemausfall auftritt, nachdem der Datenbankserver auf ein COMMIT geantwortet hat, aber bevor die Seite auf die Festplatte geschrieben wurde. Wenn `delayed_commits` auf "On" und die Option `delayed_commit_timeout` auf einen hohen Wert gesetzt ist, ergibt sich eine schnelle Antwortzeit, wobei es jedoch zum Verlust von festgeschriebenen Transaktionen während der Wiederherstellung kommen kann.

Falls sowohl `cooperative_commits` als auch `delayed_commits` auf "On" gesetzt ist und das `cooperative_commit_timeout`-Intervall verstreicht, ohne dass die Seiten geschrieben werden, wird die Anwendung fortgesetzt (als ob das COMMIT funktioniert hätte) und das restliche Intervall (`delayed_commit_timeout` - `cooperative_commit_timeout`) wird als `delayed_commits`-Intervall verwendet, nach dem die Seiten geschrieben wurden, auch wenn sie nicht voll sind.

**Siehe auch**

- „Tipp: Verzögerte Festschreibungen verwenden“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „`cooperative_commit_timeout`-Option“ auf Seite 596
- „`cooperative_commits`-Option“ auf Seite 596
- „`delayed_commit_timeout`-Option“ auf Seite 606
- „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `delayed_commits`-Verbindungseigenschaft auf Seite 718

**delete\_old\_logs-Option [SQL Remote]**

Steuert, ob Transaktionslogs gelöscht werden, nachdem ihre Transaktionen repliziert oder synchronisiert wurden

**Zulässige Werte**

On, Off, Delay, *n* days

### Standardwert

Off

### Bemerkungen

SQL Anywhere MobiLink-Clients und SQL Remote verwenden diese Option. Die Standardeinstellung ist "Off". Wenn sie auf "On" gesetzt ist, werden alte Transaktionslogs gelöscht, sobald alle Änderungen, die sie enthalten, erfolgreich repliziert und synchronisiert wurden. Wenn auf "DELAY" gesetzt, werden alte Transaktionslogs, deren Dateiname anzeigt, dass sie am gleichen Tag erstellt wurden, nicht gelöscht, sogar wenn alle Änderungen gesendet und bestätigt wurden. Wenn auf  $n$  Tage gesetzt, werden Logs gelöscht, die vor  $n$  Tagen erstellt wurden. Ein ungültiger Wert wird als "Off" interpretiert und es wird weder ein Fehler noch eine Warnung gemeldet.

Weitere Hinweise dazu, wie Sie die delete\_old\_logs-Option in Verbindung mit der BACKUP-Anweisung zum Löschen alter Kopien von Transaktionslogs verwenden können, finden Sie unter [„BACKUP-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#).

### Siehe auch

- „Transaktionslog-Verwaltung“ auf Seite 1070
- „SQL Anywhere-Clientlogs“ [[MobiLink - Clientadministration](#)]
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998
- MobiLink: „Erweiterte Option MirrorLogDirectory (mld)“ [[MobiLink - Clientadministration](#)]
- SQL Remote: „Transaktionslogs für entfernte Datenbanken verwalten“ [[SQL Remote](#)]
- „SQL Remote-Optionen“ [[SQL Remote](#)]

### Beispiel

Wenn Sie am 18. Januar dbmsync in einer entfernten Datenbank ausführen, bei der die delete\_old\_logs-Option auf zehn Tage eingestellt ist, löscht dbmsync alle Offline-Transaktionslogs, die am oder vor dem 7. Januar erstellt wurden. Die entfernte Datenbank würde die Option folgendermaßen setzen:

```
SET OPTION delete_old_logs = '10 days';
```

## disk\_sandbox-Option

Steuert, ob die Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt werden, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Die Einstellung tritt sofort in Kraft.

**Bemerkungen**

Wenn Sie diese Option auf "On" setzen, werden die Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse. Die Einstellung bleibt über Sitzungen hinweg bestehen.

**Siehe auch**

- „Sandboxing“ auf Seite 1411
- „Datenbankserveroption -sbx “ auf Seite 279
- „Datenbankoption -sbx “ auf Seite 330
- „START DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_db\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**divide\_by\_zero\_error-Option**

Steuert die Berichterstellung bei einem Nullteilungsfehler

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Diese Option zeigt an, ob eine Teilung durch Null als Fehler berichtet wird. Wenn die Option auf "On" gesetzt ist, ergibt eine Teilung durch Null einen Fehler mit SQLSTATE 22012.

Wenn die Option auf "Off" gesetzt ist, ergibt die Teilung durch Null keinen Fehler. Es wird stattdessen NULL zurückgegeben.

**Siehe auch**

- [divide\\_by\\_zero\\_error-Verbindungseigenschaft](#) auf Seite 719
- „Einschränkungen für materialisierte Ansichten“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

**escape\_character-Option**

Diese Option ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.

## exclude\_operators-Option

Diese Option ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.

## extended\_join\_syntax-Option

Steuert, ob Abfragen in einer Syntax mit mehrfachen Korrelationsnamen für Mehrtabellen-Joins zulässig sind oder als Fehler gemeldet werden

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn diese Option auf "On" gesetzt ist, lässt SQL Anywhere zu, dass auf der Nullwert-liefernden Seite von Outer-Joins dieselben Korrelationsnamen doppelt oder mehrfach verwendet werden. Alle mit einem identischen Korrelationsnamen definierten Tabellen oder Ansichten werden als ein und dieselbe Instanz der Tabelle oder Ansicht interpretiert.

Die nachstehende FROM-Klausel zeigt die Interpretation eines Joins mit doppelt vorkommenden Korrelationsnamen durch SQL Anywhere, wobei C1 und C2 Suchbedingungen sind:

```
( R left outer join T on ( C1 ), T join S on ( C2 ) )
```

Wenn diese Option auf "On" gesetzt ist, wird der Join wie folgt interpretiert:

```
( R left outer join T on ( C1 ) ) join S on ( C2 )
```

Wenn die Option auf "Off" gesetzt ist, wird SQLCODE -137 generiert. Siehe „Tabelle '%1' erfordert einen eindeutigen Korrelationsnamen“ [[Fehlermeldungen](#)].

#### Hinweis

Wenn Sie sich das Ergebnis der Eliminierung von doppelten Korrelationsnamen ansehen wollen, können Sie die mit der REWRITE-Funktion umgeschriebene Anweisung mit dem zweiten Argument ANSI anzeigen.

**Siehe auch**

- „REWRITE-Funktion [Verschiedene]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Doppelte Korrelationsnamen in Joins (Stern-Joins)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- `extended_join_syntax`-Verbindungseigenschaft auf Seite 720

## **extern\_login\_credentials-Option**

Steuert, ob Verbindungen mit entfernten Datenbanken mithilfe der externen Anmeldeinformationen des angemeldeten Benutzers oder der externen Anmeldeinformationen des effektiven Benutzers hergestellt werden.

**Zulässige Werte**

Login\_user, Effective\_user

**Standardwert**

Effective\_user

**Bereich**

Kann nur für die PUBLIC-Rolle gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Diese Option legt fest, ob Verbindungen für den Ferndatenzugriff mithilfe der externen Anmeldeinformationen des angemeldeten Benutzers oder der externen Anmeldeinformationen des effektiven Benutzers hergestellt werden.

- **Login\_user** Wenn Login\_user angegeben wurde, verwendet der Datenbankserver immer die externen Anmeldeinformationen des angemeldeten Benutzers, um Verbindungen für den Ferndatenzugriff herzustellen, und zwar unabhängig vom aktuellen effektiven Benutzer.
- **Effective\_user** Wenn Effective\_user angegeben wurde, beachtet der Datenbankserver die Einstellung des aktuellen effektiven Benutzers. Verbindungen für den Ferndatenzugriff werden auf Basis der externen Anmeldeinformationen des aktuellen effektiven Benutzers hergestellt, statt immer die externen Anmeldeinformationen des angemeldeten Benutzers zu verwenden. Die Angabe von Effective\_user kann dazu führen, dass für dieselbe lokale Verbindung mehrere Verbindungen mit entfernten Datenbanken hergestellt werden (eine pro effektivem Benutzer).

**Siehe auch**

- „CREATE PROCEDURE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## **external\_remote\_options-Option [SQL Remote]**

Gibt an, wo die Nachrichtenverbindungsparameter gespeichert werden sollen

### Zulässige Werte

On, Off

### Standardwert

Off

### Bemerkungen

SQL Remote verwendet diese Option, um anzuzeigen, ob die Nachrichtenverbindungsparameter in der Datenbank (Off) oder extern (On) gespeichert werden.

### Siehe auch

- [„Festlegen von Steuerungsparametern für den entfernten Nachrichtentyp“ \[SQL Remote\]](#)

## fire\_triggers-Option

Steuert, ob Trigger in der Datenbank ausgelöst werden

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Wenn die Option auf "On" gesetzt ist, werden Trigger ausgelöst. Wenn die Option auf "Off" gesetzt ist, werden keine Trigger ausgelöst, auch keine Trigger zur Aufrechterhaltung der referenziellen Integrität (wie kaskadierendes Aktualisieren und Löschen). Die Option wird durch die Option -gf aufgehoben, die unabhängig von der fire\_triggers-Einstellung alle Triggerauslösungen deaktiviert.

Diese Option ist beim Replizieren von Daten von Adaptive Server Enterprise zu SQL Anywhere von Bedeutung, da alle Aktionen, einschließlich Aktionen, die von Triggern ausgeführt werden, von Adaptive Server Enterprise über Transaktionslogs zu SQL Anywhere repliziert werden.

### Siehe auch

- [„Datenbankserveroption -gf“ auf Seite 241](#)
- [„Trigger“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„Kompatibilitätsoptionen“ auf Seite 559](#)
- [fire\\_triggers-Verbindungseigenschaft auf Seite 720](#)

## first\_day\_of\_week-Option

Stellt die Nummerierung der Wochentage ein

### Zulässige Werte

1, 2, 3, 4, 5, 6, 7

### Standardwert

7 (Sonntag ist der erste Wochentag)

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Die Werte haben folgende Bedeutung:

Wert	Bedeutung
1	Montag
2	Dienstag
3	Mittwoch
4	Donnerstag
5	Freitag
6	Samstag
7	Sonntag

Der von dieser Option angegebene Wert wirkt sich auf die Ergebnisse der DATEPART-Funktion aus, wenn ein Wochentagwert bezogen wird. Sie können den ersten Wochentag mithilfe der Option DATEFIRST der SET-Anweisung ändern.

Der von dieser Option angegebene Wert wirkt sich nicht auf das Ergebnis der DOW-Funktion aus. Beispiel: Selbst wenn der erste Wochentag auf Montag gesetzt ist, gibt die DOW-Funktion eine 2 für Montag zurück.

### Siehe auch

- „DATEPART-Funktion [Datum und Uhrzeit]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DOW-Funktion [Datum und Uhrzeit]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET-Anweisung [T-SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- first\_day\_of\_week-Verbindungseigenschaft auf Seite 721

## for\_xml\_null\_treatment-Option

Steuert die Behandlung von NULL in Abfragen, die die FOR XML-Klausel verwenden

### Zulässige Werte

Empty, Omit

### Standardwert

Omit

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn Sie eine Abfrage ausführen, die die FOR XML-Klausel enthält, legt die Option for\_xml\_null\_treatment fest, wie NULL behandelt wird. Standardmäßig werden Elemente und Attribute, die NULL enthalten, aus dem Ergebnis ausgeklammert. Wenn Sie diese Option auf "Empty" setzen, werden leere Elemente oder Attribute erstellt, wenn der Wert NULL ist.

### Siehe auch

- „Abrufen von Abfrageergebnissen als XML mit der FOR XML-Klausel“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SELECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- for\_xml\_null\_treatment-Verbindungseigenschaft auf Seite 721

## force\_view\_creation-Option

Diese Option ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.

### Vorsicht

Die Option force\_view\_creation darf nur innerhalb eines *reload.sql*-Skripten verwendet werden. Diese Option wird vom Dienstprogramm zum Entladen (dbunload) verwendet und darf nicht explizit gesetzt werden.

## global\_database\_id-Option

Steuert den Wertebereich bei Spalten, die mit DEFAULT GLOBAL AUTOINCREMENT erstellt wurden. Wird verwendet, um eindeutige Primärschlüssel in einer Replikationsumgebung zu generieren.

### Zulässige Werte

Nicht-negative Ganzzahl

**Standardwert**

2147483647

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Der Wert, den Sie für diese Option angeben, ist der Startwert. Wenn bei mit DEFAULT GLOBAL AUTOINCREMENT erstellten Spalten eine Zeile in die Tabelle eingefügt wird, die keinen Wert für die DEFAULT GLOBAL AUTOINCREMENT-Spalte enthält, generiert der Datenbankserver einen Wert für die Spalte. Der Wert wird durch den Wert global\_database\_id value und die Partitionsgröße für die Spalte festgelegt.

Der Standardwert von global\_database\_id zeigt an, dass DEFAULT GLOBAL AUTOINCREMENT deaktiviert ist. In diesem Fall wird als Standard NULL generiert.

Sie können den Wert der Option in der aktuellen Datenbank herausfinden, indem Sie die folgende Anweisung verwenden:

```
SELECT DB_PROPERTY( 'GlobalDBID' );
```

Diese Funktion ist vor allem in Replikationsumgebungen nützlich, um eindeutige Primärschlüssel sicherzustellen.

**Siehe auch**

- „CREATE TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Der Standardwert GLOBAL AUTOINCREMENT“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- Neuladen von Tabellen mit AUTOINCREMENT-Spalten [[SQL Anywhere 16 - Änderungen und Upgrades](#)]
- global\_database\_id-Verbindungseigenschaft auf Seite 721
- MobiLink: „Globale Datenbank-IDs“ [[MobiLink - Serveradministration](#)]
- SQL Remote: „Mehrfach vorhandene Primärschlüssel“ [[SQL Remote](#)]

**Beispiel**

Das folgende Beispiel setzt die Datenbank-Identifizierungsnummer auf 100.

```
SET OPTION PUBLIC.global_database_id = '100';
```

**http\_connection\_pool\_basesize-Option**

Gibt die nominale Schwellenwertgröße von Datenbankverbindungen an.

**Zulässige Werte**

Ganzzahl zwischen 0 und 1000 (inklusive)

### Standardwert

10

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Das Ändern dieser Option wird innerhalb von fünf Sekunden beim nächsten Bereinigungszyklus wirksam. Nicht verwendete Datenbankverbindungen, die `http_connection_pool_timeout` innerhalb des `http_connection_pool_basesize`-Schwellenwerts überschritten haben, werden gelöscht. Wenn die Größe eines Verbindungspools den `http_connection_pool_basesize`-Schwellenwert überschreitet, werden Verbindungen wesentlich schneller gelöscht.

Wenn Sie einen Wert von 0 angeben, werden die HTTP-Verbindungspools innerhalb von fünf Sekunden nach dem Setzen der Option bereinigt und das HTTP-Verbindungspooling wird deaktiviert.

Nicht verwendete überzählige Verbindungen werden innerhalb der Hälfte des Zeitüberschreitungsintervalls entfernt. Die Hälfte der verbleibenden Verbindungen wird gelöscht, wenn diese Verbindungen innerhalb eines Viertels des Zeitüberschreitungsintervalls nicht verwendet werden, und so weiter. Die folgenden Datenbankeigenschaften wurden zur Ermittlung der Effizienz der Verbindungspools in einer Datenbank hinzugefügt:

- `Http_Conn_Pool_Cached_Count`
- `Http_Conn_Pool_Hits`
- `Http_Conn_Pool_Misses`
- `Http_Conn_Pool_Steals`

### Siehe auch

- „`http_connection_pool_timeout`-Option“ auf Seite 616
- `http_connection_pool_timeout`-Verbindungseigenschaft auf Seite 722
- `http_connection_pool_basesize`-Verbindungseigenschaft auf Seite 721
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „HTTP-Webdienste“ [*SQL Anywhere Server - Programmierung*]

## `http_connection_pool_timeout`-Option

Gibt die maximale Dauer an, über die eine nicht verwendete Verbindung im Verbindungspool aufrecht erhalten werden kann.

### Zulässige Werte

Ganzzahl zwischen 1 und 86400 (inklusive)

### Standardwert

60

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Überzählige Verbindungen werden mit einer ansteigenden Rate basierend auf diesem Wert gelöscht, wenn die Poolgröße den Wert von `http_connection_pool_basesize` überschreitet.

Das Ändern dieser Option wird innerhalb von fünf Sekunden beim nächsten Bereinigungszyklus wirksam. Nicht verwendete Datenbankverbindungen, die `http_connection_pool_timeout` innerhalb des `http_connection_pool_basesize`-Schwellenwerts überschritten haben, werden gelöscht. Wenn die Größe eines Verbindungspools den `http_connection_pool_basesize`-Schwellenwert überschreitet, werden Verbindungen wesentlich schneller gelöscht.

Nicht verwendete überzählige Verbindungen werden innerhalb der Hälfte des Zeitüberschreitungsintervalls entfernt. Die Hälfte der verbleibenden Verbindungen wird gelöscht, wenn diese Verbindungen innerhalb eines Viertels des Zeitüberschreitungsintervalls nicht verwendet werden, und so weiter. Die folgenden Datenbankeigenschaften wurden zur Ermittlung der Effizienz der Verbindungspools in einer Datenbank hinzugefügt:

- `Http_Conn_Pool_Cached_Count`
- `Http_Conn_Pool_Hits`
- `Http_Conn_Pool_Misses`
- `Http_Conn_Pool_Steals`

**Siehe auch**

- „[http\\_connection\\_pool\\_basesize-Option](#)“ auf Seite 615
- [http\\_connection\\_pool\\_basesize-Verbindungseigenschaft](#) auf Seite 721
- [http\\_connection\\_pool\\_timeout-Verbindungseigenschaft](#) auf Seite 722
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „[HTTP-Webdienste](#)“ [*SQL Anywhere Server - Programmierung*]

## **http\_session\_timeout**

Gibt den Standardwert für das Timeout in Minuten an, über das die HTTP-Sitzung bei Inaktivität bestehen bleibt.

**Zulässige Werte**

Ganzzahl (1 bis 525600)

**Standardwert**

30

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn Sie diese Datenbankoption auf einen anderen Wert setzen, legen Sie damit einen neuen Standardwert für die Zeitüberschreitung bei Sitzungen fest, der auf alle nachfolgenden HTTP-Sitzungen angewendet wird. Eine HTTP-Sitzung kann diesen Standardwert überschreiben, indem sie die Systemprozedur `sa_set_http_option` zur Einstellung des SessionTimeout-Werts innerhalb einer bestimmten HTTP-Sitzung aufruft.

### Siehe auch

- „sa\_set\_http\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „HTTP-Sitzungsverwaltung auf einem HTTP-Server“ [[SQL Anywhere Server - Programmierung](#)]
- SessionCreateTime-Verbindungseigenschaft auf Seite 736
- SessionTimeout-Verbindungseigenschaft auf Seite 736
- http\_session\_timeout-Verbindungseigenschaft auf Seite 722
- „HTTP-Webdienste“ [[SQL Anywhere Server - Programmierung](#)]

## integrated\_server\_name-Option

Gibt den Namen des Domain Controller-Servers an, der bei integrierter Benutzerauthentifizierung (integrierten Logins) zum Suchen nach Windows-Benutzergruppenmitgliedschaften verwendet wird.

### Zulässige Werte

Zeichenfolge

### Standardwert

NULL

### Bereich

Diese Option ermöglicht es einem Benutzer mit SET ANY SECURITY OPTION-Systemprivileg, den Namen des Domain Controller-Servers anzugeben, über den nach Gruppenmitgliedschaften gesucht wird, wenn bei integrierten Logins Windows-Benutzergruppen verwendet werden. Standardmäßig wird der Computer, auf dem SQL Anywhere läuft, zur Verifizierung der Gruppenmitgliedschaft verwendet.

### Bemerkungen

Diese Option ermöglicht es einem Benutzer mit den entsprechenden Privilegien, den Namen des Domain Controller-Servers anzugeben, über den nach Gruppenmitgliedschaften gesucht wird, wenn bei integrierten Logins Windows-Benutzergruppen verwendet werden. Standardmäßig wird der Computer, auf dem SQL Anywhere läuft, zur Verifizierung der Gruppenmitgliedschaft verwendet.

**Siehe auch**

- „Integrierte Logins für Windows-Benutzergruppen“ auf Seite 58
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `integrated_server_name`-Verbindungseigenschaft auf Seite 722

**Beispiel**

Das folgende Beispiel gibt an, dass die Gruppenmitgliedschaft auf dem Computer "server-1" verifiziert wird.

```
SET OPTION PUBLIC.integrated_server_name = '\\\\server-1';
```

## isolation\_level-Option

Steuert die Isolationsstufe für Sperren

**Zulässige Werte**

0, 1, 2, 3, Snapshot, Statement-snapshot, Readonly-statement-snapshot

**Standardwert**

0

1 für Sybase Open Client-, jConnect- und TDS-Verbindungen

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Diese Option steuert die Sperren-Isolationsstufe folgendermaßen:

- **0** Lässt Dirty Reads, nicht wiederholbare Lesevorgänge und Phantomzeilen zu
- **1** Verhindert Dirty Reads. Lässt nicht wiederholbare Lesevorgänge und Phantomzeilen zu.
- **2** Verhindert Dirty Reads und nicht wiederholbare Lesevorgänge. Lässt Phantomzeilen zu.
- **3** Serialisierbar. Verhindert Dirty Reads, nicht wiederholbare Lesevorgänge und Phantomzeilen.
- **Snapshot** Verwendet einen Snapshot von festgeschriebenen Daten ab dem Zeitpunkt, an dem die erste Zeile von einer Transaktion gelesen oder aktualisiert wird
- **Statement-snapshot** Verwendet bei jeder Anweisung einen Snapshot von festgeschriebenen Daten ab dem Zeitpunkt, an dem die erste Zeile aus der Datenbank gelesen wird. Nicht wiederholbare Zeilen und Phantomzeilen können innerhalb einer Transaktion, aber nicht in einer einzelnen Anweisung vorkommen.

- **Readonly-statement-snapshot** Verwendet bei schreibgeschützten Anweisungen einen Snapshot von festgeschriebenen Daten ab dem Zeitpunkt, an dem die erste Zeile aus der Datenbank gelesen wird. Nicht wiederholbare Zeilen und Phantomzeilen können innerhalb einer Transaktion, aber nicht in einer einzelnen Anweisung vorkommen. Bei aktualisierbaren Anweisungen wird die Isolationsstufe verwendet, die durch die Option `updatable_statement_isolation` angegeben ist (kann 0 (Standardwert), 1, 2 oder 3 sein).

Setzen Sie die `allow_snapshot_isolation`-Option auf "On", um die Einstellungen Snapshot, Statement-snapshot oder Readonly-statement-snapshot verwenden zu können.

Wenn Sie den SQL Anywhere JDBC-Treiber verwenden, ist die Standard-Isolationsstufe 0.

Abfragen, die auf Snapshot-Isolationsstufe Snapshot, Statement-snapshot oder Readonly-statement-snapshot ausgeführt werden, erhalten einen Snapshot eines festgeschriebenen Status der Datenbank.

Sie können temporäre oder PUBLIC-Einstellungen für diese Option in einzelnen INSERT-, UPDATE-, DELETE-, SELECT-, UNION-, EXCEPT- und INTERSECT-Anweisungen aufheben, indem Sie eine OPTION-Klausel in die Anweisung aufnehmen.

### Siehe auch

- „Isolationsstufen und Konsistenz“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „`sp_tsql_environment`-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`allow_snapshot_isolation`-Option“ auf Seite 574
- „`updatable_statement_isolation`-Option“ auf Seite 700
- „Snapshot-Isolation“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Richtlinien zum Auswählen der Isolationsstufen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Kompatibilitätsoptionen“ auf Seite 559
- „BEGIN TRANSACTION-Anweisung [T-SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `isolation_level`-Verbindungseigenschaft auf Seite 722

## java\_class\_path-Option

Gibt eine zusätzliche Reihe von Verzeichnissen oder JAR-Dateien an, in denen nach Klassen gesucht werden soll.

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

## Bemerkungen

Es wird empfohlen, alle Klassen- und JAR-Dateien, die mit Java in der Datenbank verwendet werden, in der Datenbank zu installieren. Wenn Sie die Klassen und JAR-Dateien in der Datenbank speichern, kann die Datenbank problemlos auf einen anderen Computer oder ein anderes Betriebssystem verschoben werden. Ein anderer Vorteil der Installation von Klassen und JAR-Dateien in der Datenbank besteht darin, dass der Datenbankserver-Klassenlader die Klassen und Ressourcen aus der Datenbank abrufen kann, sodass jede Verbindung, die Java in der Datenbank verwendet, ihre eigene Instanz dieser Klassen und ihre eigene Kopie statischer Variablen in diesen Klassen besitzt.

Wenn eine Klasse oder eine JAR-Datei vom Systemklassenlader geladen werden muss, kann die Option mit der Datenbankoption `java_class_path` oder der `dbeng16/dbsrv16-Serveroption -cp` angegeben werden. Beide Optionen fügen Klassen und JAR-Dateien dem Klassenpfad hinzu, den der Datenbankserver zum Start der Java VM aufbaut. Die `java_class_path`-Datenbankoption ist nützlich, wenn auf dem Server mehrere Datenbanken laufen und jede Datenbank eine eigene Gruppe von JAR-Dateien und Verzeichnissen hat, die vom Systemklassenlader geladen werden müssen. Die Datenbankserveroption `-cp` ist nützlich, wenn alle Datenbanken auf dem Server dieselben Klassen oder JAR-Dateien erfordern.

## Siehe auch

- „Datenbankserveroption `-cp`“ auf Seite 225
- „Java in der Datenbank“ [[SQL Anywhere Server - Programmierung](#)]
- „Eigene Java-Klassen in Datenbanken verwenden“ [[SQL Anywhere Server - Programmierung](#)]
- „`java_class_path`-Option“ auf Seite 620

## java\_location-Option

Gibt den Pfad der Java VM für die Datenbank an

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

## Bemerkungen

Standardmäßig enthält diese Option eine leere Zeichenfolge. In diesem Fall durchsucht der Datenbankserver die `JAVA_HOME`-Umgebungsvariable, den Pfad und andere Standorte nach der Java VM. Mit der `JavaVM`-Datenbankeigenschaft können Sie abfragen, welche Java VM der Datenbankserver verwendet, wenn die `java_location`-Option nicht gesetzt ist.

### Siehe auch

- „java\_vm\_options-Option“ auf Seite 622
- „Lektion 2: Auswählen einer Java VM“ [*SQL Anywhere Server - Programmierung*]
- JavaVM-Datenbankeigenschaft auf Seite 778
- java\_location-Verbindungseigenschaft auf Seite 723

## java\_main\_userid-Option (nicht mehr empfohlen)

Diese Option wird nicht mehr empfohlen.

## java\_vm\_options-Option

Legt fest, welche Befehlszeilenoptionen der Datenbankserver beim Starten der Java VM verwendet.

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Mit dieser Option können Sie Optionen angeben, die der Datenbankserver beim Starten der Java VM verwendet, wie in der Option java\_location angegeben. Diese zusätzlichen Optionen können verwendet werden, um die Java VM für die Fehlersuche oder zum Ausführen als Dienst auf Unix-Plattformen einzurichten. In manchen Fällen sind zusätzliche Optionen erforderlich, um die Java VM im 64-Bit-Modus anstelle des 32-Bit-Modus auszuführen.

### Siehe auch

- „java\_location-Option“ auf Seite 621
- „Lektion 2: Auswählen einer Java VM“ [*SQL Anywhere Server - Programmierung*]
- java\_vm\_options-Verbindungseigenschaft auf Seite 723

### Beispiel

Im folgenden Beispiel wird die java\_vm\_options-Option verwendet, damit die Java VM unter Unix weiterläuft, wenn der Datenbankserver als Dienst gestartet wurde und der Benutzer sich abmelden muss:

```
SET OPTION PUBLIC.java_vm_options = '-Xrs';
```

Das folgende Beispiel teilt der Java VM mit, den 64-Bit-Modus unter HP-UX zu verwenden:

```
SET OPTION PUBLIC.java_vm_options = '-d64';
```

## log\_deadlocks-Option

Steuert, ob die Meldung von Deadlocks ein- oder ausgeschaltet ist

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Wenn diese Option auf "On" eingestellt ist, protokolliert der Datenbankserver in einem internen Puffer Informationen über Deadlocks. Die Größe des Puffers ist mit 10000 Byte festgelegt. Sie können die Deadlock-Informationen anzeigen, indem Sie die gespeicherte Prozedur sa\_report\_deadlocks verwenden. Der Inhalt des Puffers wird beibehalten, wenn diese Option auf "Off" gesetzt wird.

Wenn ein Deadlock auftritt, werden Informationen nur für jene Verbindungen protokolliert, die vom Deadlock betroffen sind. Die Reihenfolge, in der Verbindungen gemeldet werden, hängt davon ab, welche Verbindung auf welche Zeile wartet. Bei Thread-Deadlocks werden Informationen über alle Verbindungen gemeldet.

Wenn die Option zur Meldung von Deadlocks aktiviert ist, können Sie auch das Systemereignis "Deadlock" verwenden, um Maßnahmen für den Eintritt eines Deadlocks festzulegen. Siehe [„Systemereignisse“ auf Seite 1091](#).

Sie können auch die Einstellung für diese Option ändern, indem Sie die DeadlockLogging-Eigenschaft mit der Systemprozedur sa\_server\_option verwenden.

### Siehe auch

- „sa\_report\_deadlocks-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Wie Sie ermitteln, was in einem Deadlock blockiert ist“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Praktische Einführung: Deadlocks diagnostizieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- [log\\_deadlocks-Verbindungseigenschaft auf Seite 724](#)

## login\_mode-Option

Steuert die Verwendung von Standard-, integrierter, Kerberos- und LDAP-Benutzerauthentifizierung für die Datenbank.

### Zulässige Werte

Einer oder mehrere der folgenden Werte: Standard, Integrated, Kerberos, CloudAdmin, Mixed (nicht mehr empfohlen)

### Standardwert

Standard

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option legt fest, ob Standard-, integrierte, Kerberos-, LDAP- und CloudAdmin-Benutzerauthentifizierung zulässig sind. Ein oder mehrere der folgenden Login-Modi werden akzeptiert (Groß-/Kleinschreibung wird nicht berücksichtigt):

- **Standard** Standard-Benutzerauthentifizierung ist zulässig. Dieser Wert ist die Standardeinstellung. Verbindungen mit Standard-Benutzerauthentifizierung enthalten eine Benutzer-ID und ein Kennwort und verwenden nicht den Verbindungsparameter Integrated oder Kerberos.
- **Integrated** Integrierte Benutzerauthentifizierung ist zulässig.
- **Kerberos** Kerberos-Benutzerauthentifizierung ist zulässig.
- **LDAPUA** LDAP-Benutzerauthentifizierung ist zulässig. Verbindungen mit LDAP-Benutzerauthentifizierung enthalten eine Benutzer-ID und ein Kennwort und verwenden nicht den Verbindungsparameter Integrated oder Kerberos.
- **CloudAdmin** Dieser Login-Modus ist für die interne Verwendung in der Cloud vorgesehen.
- **Mixed (nicht mehr empfohlen)** Dies entspricht der Angabe von "Standard,Integrated".

Wenn Sie mehrere Login-Modi angeben, lässt der Datenbankserver alle angegebenen Logins zu.

#### Vorsicht

Wenn die login\_mode-Datenbankoption keine Standard-Benutzerauthentifizierung zulässt, sind Verbindungen ausschließlich auf Benutzer beschränkt, denen eine integrierte, Kerberos- oder LDAP-Login-Zuordnung erteilt wurde. Der Versuch, eine Standard-Verbindung mithilfe von Datenbankbenutzer-ID und Kennwort herzustellen, führt zu einem Fehler. Die einzige Ausnahme hiervon sind Benutzer mit allen DBA-Privilegien.

Sie können mehrere Werte in einer Liste mit Trennkommas angeben. Die Liste darf keine Leerstellen enthalten. Die folgende Einstellung z.B. lässt Standard- und integrierte Logins zu:

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

Wenn eine Datenbankdatei nicht gesichert ist und von nicht autorisierten Benutzern kopiert werden kann, sollte die temporäre login\_mode-Option für PUBLIC verwendet werden (bei integrierter und Kerberos-

Benutzerauthentifizierung). Auf diese Weise werden integrierte und Kerberos-Logins nicht standardmäßig unterstützt, wenn die Datei kopiert wird.

### Siehe auch

- „Integrierte Windows-Logins“ auf Seite 52
- „Kerberos-Authentifizierung“ auf Seite 63
- „LDAP-Benutzerauthentifizierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -al“ auf Seite 216
- „Hinweise zur Sicherheit: Benutzer-IDs“ auf Seite 1409
- „Sicherheitsprobleme: Kopierte Datenbankdateien“ auf Seite 76
- login\_mode-Verbindungseigenschaft auf Seite 724

### Beispiel

Aktivieren Sie nur die integrierte Benutzerauthentifizierung (sodass Standard-, Kerberos- und LDAP-Benutzerauthentifizierung fehlschlagen):

```
SET OPTION PUBLIC.login_mode = 'Integrated';
```

Aktivieren Sie Standard- und Kerberos-Benutzerauthentifizierung (sodass integrierte und LDAP-Benutzerauthentifizierung fehlschlagen):

```
SET OPTION PUBLIC.login_mode = 'Standard,Kerberos';
```

Aktivieren Sie Standard-, integrierte, Kerberos- und LDAP-Benutzerauthentifizierung:

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated,Kerberos,LDAPUA';
```

## login\_procedure-Option

Gibt eine Login-Prozedur an, die beim Start Optionen für die Verbindungskompatibilität setzt.

### Zulässige Werte

Zeichenfolge

### Standardwert

sp\_login\_environment-Systemprozedur

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Diese Login-Prozedur ruft die Prozedur "sp\_login\_environment" zur Laufzeit auf, um die Verbindungseinstellungen für die Datenbank festzulegen. Die Login-Prozedur wird aufgerufen, nachdem alle Überprüfungen, ob die Verbindung eine gültige ist, durchgeführt wurden. Die durch die Option login\_procedure angegebene Prozedur wird bei Ereignisverbindungen nicht ausgeführt, sie wird jedoch für Webdienstverbindungen ausgeführt.

Sie können die Optionseinstellungen der Standarddatenbank anpassen, indem Sie eine neue Prozedur erstellen, und die Prozedur `login_procedure` die neue Prozedur aufrufen lassen. Diese angepasste Prozedur muss entweder `sp_login_environment` aufrufen oder feststellen, wann eine TDS-Verbindung auftritt (siehe den `sp_login_environment`-Standardcode), und `sp_tsql_environment` direkt aufrufen. Anderenfalls können TDS-basierte Verbindungen unterbrochen werden. Bearbeiten Sie weder `sp_login_environment` noch `sp_tsql_environment`.

Eine Fehlermeldung über ein abgelaufenes Kennwort mit SQLSTATE 08WA0 kann durch eine benutzerdefinierte Login-Prozedur signalisiert werden, um einem Benutzer mitzuteilen, dass sein Kennwort abgelaufen ist. Durch die Signalisierung des Fehlers können Anwendungen den Fehler prüfen und abgelaufene Kennwörter verarbeiten. Es wird empfohlen, eine Login-Richtlinie zu verwenden, um den Kennwortablauf zu implementieren, und nicht eine Login-Prozedur, die die Fehlermeldung über das abgelaufene Kennwort übermittelt.

Wenn Sie den Verbindungsparameter `NewPassword=*` verwenden, ist die Signalisierung dieses Fehlers erforderlich, damit die Clientbibliothek zur Eingabe eines neuen Kennwort auffordern kann. Wenn die Prozedur den SQLSTATE 28000 (Benutzer-ID oder Kennwort ungültig) oder SQLSTATE 08WA0 (Kennwort abgelaufen) übergibt, oder die Prozedur mit `RAISERROR` einen Fehler ausgibt, schlägt das Login fehl und der Benutzer erhält eine Fehlermeldung. Wenn Sie einen anderen Fehler signalisieren oder ein anderer Fehler auftritt, ist die Benutzeranmeldung erfolgreich und eine Meldung wird in das Log des Datenbankservers geschrieben.

### Siehe auch

- „`post_login_procedure`-Option“ auf Seite 651
- „`sp_login_environment`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_tsql_environment`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Hinweise zur Sicherheit: Kennwörter“ auf Seite 1410
- „Verbindungsparameter `NewPassword (NEWPWD)`“ auf Seite 372
- „`CREATE PROCEDURE`-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `login_procedure`-Verbindungseigenschaft auf Seite 724
- „Login-Richtlinien“ auf Seite 535

### Beispiel

Im folgenden Beispiel wird gezeigt, wie Sie eine Verbindung untersagen, indem der Fehler `INVALID_LOGON` angezeigt wird.

```
CREATE PROCEDURE DBA.login_check( )
BEGIN
    DECLARE INVALID_LOGON EXCEPTION FOR SQLSTATE '28000';
    // Allow a maximum of 3 concurrent connections
    IF( DB_PROPERTY( 'ConnCount' ) > 3 ) THEN
        SIGNAL INVALID_LOGON;
    ELSE
        CALL sp_login_environment;
    END IF;
END
go

GRANT EXECUTE ON DBA.login_check TO PUBLIC
go
```

```
SET OPTION PUBLIC.login_procedure='DBA.login_check'
go
```

Weitere Informationen zu einer anderen Methode zum Sperren von Verbindungen finden Sie unter „RAISERROR-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Das folgende Beispiel zeigt, wie Sie Verbindungsversuche blockieren können, wenn die Anzahl der fehlgeschlagenen Verbindungen für einen Benutzer innerhalb eines Zeitraums von 30 Minuten 3 überschreitet. Bei jedem Verbindungsversuch innerhalb der Blockierungsperiode wird der Fehler "ungültiges Kennwort" gemeldet, die Verbindungsversuche werden als fehlgeschlagen protokolliert. Das Log wird lange genug aufbewahrt, damit es von einem DBA inspiziert werden kann.

```
CREATE TABLE DBA.ConnectionFailure(
    pk INT PRIMARY KEY DEFAULT AUTOINCREMENT,
    user_name CHAR(128) NOT NULL,
    tm TIMESTAMP NOT NULL DEFAULT CURRENT_TIMESTAMP
)
go

CREATE INDEX ConnFailTime ON DBA.ConnectionFailure(
    user_name, tm )
go

CREATE EVENT ConnFail TYPE ConnectFailed
HANDLER
BEGIN
    DECLARE usr CHAR(128);
    SET usr = event_parameter( 'User' );

    // Put a limit on the number of failures logged.
    IF (SELECT COUNT(*) FROM DBA.ConnectionFailure
        WHERE user_name = usr
        AND tm >= DATEADD( minute, -30,
            CURRENT_TIMESTAMP )) < 20 THEN
        INSERT INTO DBA.ConnectionFailure( user_name )
            VALUES( usr );
        COMMIT;
        // Delete failures older than 7 days.
        DELETE DBA.ConnectionFailure
        WHERE user_name = usr
        AND tm < dateadd( day, -7, CURRENT_TIMESTAMP );
        COMMIT;
    END IF;
END
go

CREATE PROCEDURE DBA.login_check( )
BEGIN
    DECLARE usr CHAR(128);
    DECLARE INVALID_LOGON EXCEPTION FOR SQLSTATE '28000';
    SET usr = CONNECTION_PROPERTY( 'Userid' );
    // Block connection attempts from this user
    // if 3 or more failed connection attempts have occurred
    // within the past 30 minutes.
    IF ( SELECT COUNT( * ) FROM DBA.ConnectionFailure
        WHERE user_name = usr
        AND tm >= DATEADD( minute, -30,
            CURRENT_TIMESTAMP ) ) >= 3 THEN
        SIGNAL INVALID_LOGON;
    ELSE
        CALL sp_login_environment;
```

```
        END IF;
    END
    go

    GRANT EXECUTE ON DBA.login_check TO PUBLIC
    go

    SET OPTION PUBLIC.login_procedure='DBA.login_check'
    go
```

Das folgende Beispiel zeigt, wie Sie einen Fehler mit der Meldung signalisieren können, dass das Kennwort eines Benutzers abgelaufen ist. Es wird empfohlen, eine Login-Richtlinie zu verwenden, um die Benachrichtigung über abgelaufene Kennwörter zu implementieren.

```
CREATE PROCEDURE DBA.check_expired_login( )
BEGIN
    DECLARE PASSWORD_EXPIRED EXCEPTION FOR SQLSTATE '08WA0';

    IF( condition-to-check-for-expired-password ) THEN
        SIGNAL PASSWORD_EXPIRED;
    ELSE
        CALL sp_login_environment;
    END IF;
END;
```

## materialized\_view\_optimization-Option

Steuert, wie materialisierte Ansichten vom Optimierer verwendet werden, um Abfragen effizient zu beantworten

### Zulässige Werte

**Disabled, Fresh, Stale,  $N$  { Minute[s] | Hour[s] | Day[s] | Week[s] | Month[s] }**

### Standardwert

Stale

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Mit der Option materialized\_view\_optimization können Sie die Umstände festlegen, unter denen der Optimierer veraltete materialisierte Ansichten verwenden kann.

Daten in einer materialisierten Ansicht sind veraltet, sobald eine der von der materialisierten Ansicht referenzierten Basistabellen aktualisiert wird. Berücksichtigen Sie beim Festlegen der Aktualisierungshäufigkeit für die materialisierte Ansicht das akzeptable Ausmaß an Datenveralterung ebenso wie die Zeit, die das Aktualisieren der Ansicht dauert, da die Ansicht während des Aktualisierungsprozesses nicht für Abfragen verfügbar ist. Erwägen Sie außerdem, ob es für den Datenbankserver akzeptabel ist, Ergebnisse zurückzugeben, die möglicherweise nicht den aktuellen

Zustand der Datenbank widerspiegeln. Sie können unter den folgenden Einstellungen für diese Option wählen:

- **Disabled** Keine materialisierten Ansichten bei der Abfrageoptimierung verwenden
- **Fresh** Eine materialisierte Ansicht nur verwenden, wenn sie neu ist (Daten in den Basistabellen wurden seit der letzten Aktualisierung nicht geändert)
- **Stale** Materialisierte Ansichten verwenden, auch wenn sie veraltet sind. Dieser Wert ist die Standardeinstellung.
- **N { Minute[s] | Hour[s] | Day[s] | Week[s] | Month[s] }** Neue und veraltete materialisierte Ansichten verwenden, solange die veralteten materialisierten Ansichten innerhalb der angegebenen Zeitspanne aktualisiert wurden. In Minuten angegebene Werte müssen weniger als 2<sup>31</sup> Minuten betragen. Der Datenbankserver behandelt eine Woche wie 7 Tage und einen Monat wie 30 Tage.

Wenn eine Abfrage eine materialisierte Ansicht direkt referenziert, wird die Ansicht unabhängig von ihrer Aktualisierung verwendet. In diesem Fall hat die Option `materialized_view_optimization` keine Auswirkung.

#### Siehe auch

- „Materialisierte Ansichten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Fortgeschrittene Aufgaben: Einstellungen zum Steuern der Datenveraltung in materialisierten Ansichten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- `materialized_view_optimization`-Verbindungseigenschaft auf Seite 725

## max\_client\_statements\_cached-Option

Steuert die Anzahl der Anweisungen, die vom Client im Cache gehalten werden

#### Zulässige Werte

Ganzzahl, 0 bis 100

#### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

#### Standardwert

10

#### Bemerkungen

Das clientseitige Caching von Anweisungen verringert Datenbankanforderungen und Anweisungsvorbereitungen, wenn identische SQL-Anweisungen mehrfach vorbereitet werden. Wenn derselbe SQL-Text wiederholt vorbereitet und gelöscht wird, legt der Client die Anweisung im Cache ab, wodurch sie vorbereitet auf dem Datenbankserver verbleibt, selbst nachdem sie von der Anwendung gelöscht wurde. Das Caching der Anweisung erspart dem Datenbankserver den zusätzlichen Aufwand, die

Anweisung zu löschen und erneut vorzubereiten. Bei einer Änderung des Schemas bzw. der Einstellung einer Datenbankoption oder bei Ausführung einer DROP VARIABLE-Anweisung wird die vorbereitete Anweisung automatisch gelöscht und bei der nächsten Ausführung der SQL-Anweisung wieder vorbereitet. Dadurch wird sichergestellt, dass eine zwischengespeicherte Anweisung, die ein falsches Verhalten bewirken könnte, nicht wieder verwendet wird.

Diese Option legt die maximale Anzahl von Anweisungen fest, die vorbereitet (im Cache) verbleiben können. Anweisungen im Cache werden vom Ressourcen-Gouverneur max\_statement\_count nicht mitgezählt.

Die Einstellung dieser Option gilt für Verbindungen, die unter Verwendung von SQL, ODBC, OLE DB, ADO.NET und des SQL Anywhere JDBC-Treibers erstellt werden. Sie gilt nicht für Sybase Open Client-, jConnect- oder HTTP-Verbindungen.

Wenn diese Option auf 0 gesetzt wird, ist das clientseitige Caching von Anweisungen deaktiviert. Eine Erhöhung dieses Werts kann die Performance verbessern, wenn die Anwendung dieselbe SQL-Anweisung mehr als zehnmal vorbereitet und löscht. Wenn eine Anwendung beispielsweise eine Schleife mit fünfundzwanzig SQL-Anweisungen durchführt und diese bei jeder Wiederholung der Schleife vorbereitet und löscht sowie die einzelnen SQL-Anweisungen in jeder Wiederholung denselben Text haben, können Sie die Performance möglicherweise verbessern, indem Sie diese Option auf 25 setzen.

Eine Erhöhung des Werts dieser Option erhöht den Speicherbedarf auf dem Client und verstärkt den Cachedruck auf dem Datenbankserver. Wenn eine signifikante Anzahl von zwischengespeicherten Anweisungen aufgrund von Schemaänderungen oder Optionseinstellungen nicht wieder verwendet werden kann, wird die Caching von Anweisungen bei dieser Verbindung automatisch deaktiviert. Wenn das Caching von Anweisungen automatisch deaktiviert wird, schaltet der Client das Caching von Anweisungen periodisch wieder ein, um die Entscheidung zu überprüfen und um zu ermitteln, ob eine erneute Aktivierung des Cachings von Anweisungen von Nutzen wäre.

Das Caching von Clientanweisungen im Cache könnte in folgenden Situationen zu unerwarteten Ergebnissen führen:

1. Eine Anweisung wird vorbereitet und beschrieben, ihr Describe gibt aber zurück, dass die Anweisung kein Ergebnis hat.

```
CREATE OR REPLACE FUNCTION test() RETURNS INT BEGIN RETURN 1;
END;
CALL test();
```

2. Eine DDL-Anweisung führt dazu, dass derselbe Anweisungstext (in diesem Beispiel die CALL-Anweisung) jetzt eine Ergebnismenge auf derselben Verbindung zurückgibt. Zum Beispiel:

```
CREATE OR REPLACE PROCEDURE test() BEGIN SELECT 2;
END;
CALL test();
```

Wenn das clientseitige Caching von Anweisungen aktiviert ist, wird die zweite CALL test()-Anweisung falsch beschrieben.

Wenn das Log mit dem Perl-Skript *tracetime.pl* analysiert wird, sollte die `max_client_statements_cached`-Option auf 0 gesetzt werden, damit das clientseitige Caching von Anweisungen deaktiviert wird, während die Anforderungsprotokollierung erfasst wird.

#### Siehe auch

- „`max_statement_count`-Option“ auf Seite 635
- `ClientStmtCacheHits`-Verbindungseigenschaft auf Seite 715
- `ClientStmtCacheMisses`-Verbindungseigenschaft auf Seite 716
- `ClientStmtCacheHits`-Servereigenschaft auf Seite 747
- `ClientStmtCacheMisses`-Servereigenschaft auf Seite 747
- `max_client_statements_cached`-Verbindungseigenschaft auf Seite 725

## max\_cursor\_count-Option

Steuert einen Ressourcenwächter, der die maximale Anzahl von Cursors begrenzt, die eine Verbindung gleichzeitig verwenden kann

#### Zulässige Werte

Ganzzahl

#### Standardwert

50

#### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für eine Verbindung setzen zu können. Wird sofort wirksam.

#### Bemerkungen

Dieser Ressourcenwächter ermöglicht einem DBA, die Anzahl der Cursor pro Verbindung zu begrenzen, die ein Benutzer verwenden kann. Falls ein Vorgang die Grenze für eine Verbindung überschreitet, wird ein Fehler erzeugt, der anzeigt, dass die Ressourcengrenze überschritten wurde.

Wenn eine Verbindung eine gespeicherte Prozedur ausführt, wird diese gespeicherte Prozedur mit den Privilegien des Prozedureigentümers ausgeführt. Die von der Prozedur verwendeten Ressourcen werden jedoch der aktuellen Verbindung zugeordnet.

Sie können Ressourcengrenzen entfernen, indem Sie die Option auf "0" (Null) setzen.

#### Siehe auch

- „Tipp: Ressourcenwächter verwenden“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- `max_cursor_count`-Verbindungseigenschaft auf Seite 725

## max\_plans\_cached-Option

Gibt die maximale Anzahl der Ausführungspläne an, die in einem Cache gespeichert werden können

### Zulässige Werte

Ganzzahl

### Standardwert

20

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option definiert die maximale Anzahl von Plänen, die für jede Verbindung im Cache gehalten werden können. Der Optimierer setzt den Ausführungsplan für Abfragen, INSERT-, UPDATE- und DELETE-Anweisungen, die in gespeicherten Prozeduren, Funktionen oder Triggern ausgeführt werden. Nachdem eine Anweisung in einer gespeicherten Prozedur, einer gespeicherten Funktion oder einem Trigger von einer Verbindung einige Male ausgeführt wurde, erstellt der Optimierer einen wiederverwendbaren Plan für die Anweisung.

Wiederverwendbare Pläne benutzen nicht die Werte der Hostvariablen für die Selektivitätsschätzung oder die Neuschreibungsoptimierung. Daher erzeugt der wiederverwendbare Plan unter Umständen höheren Aufwand, als wenn die Anweisung erneut optimiert würde. Wenn der Aufwand für den wiederverwendbaren Plan nahe beim günstigsten beobachteten Aufwand für eine Anweisung liegt, fügt der Optimierer den Plan dem Plancache hinzu.

Der Cache wird geleert, wenn Sie Anweisungen wie CREATE TABLE und DROP TABLE durchführen, die das Tabellenschema ändern können. Anweisungen, die deklarierte temporäre Tabellen referenzieren, werden nicht im Cache gespeichert.

Wenn diese Option auf "0" gesetzt wird, ist das Caching von Plänen deaktiviert.

### Siehe auch

- „Plan-Caching“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- [max\\_plans\\_cached-Verbindungseigenschaft auf Seite 725](#)

## max\_priority-Option

Steuert die maximale Prioritätsstufe für Verbindungen.

### Zulässige Werte

Critical, High, Above Normal, Normal, Below normal, Low, Background

**Standardwert**

Normal

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

Wenn Sie diese Option temporär setzen, gilt diese Einstellung nur für die aktuelle Verbindung. Unterschiedliche Verbindungen mit derselben Benutzer-ID haben unterschiedliche Einstellungen für diese Option.

**Bemerkungen**

Die Abfolgeplanung mit unterschiedlichen Prioritätsstufen ermöglicht es, dass alle Abfragen eine gewisse CPU-Zeit erhalten, unabhängig von der Prioritätsstufe der Abfrage. Abfragen mit höherer Priorität erhalten mehr Zeiteinheiten als solche mit niedrigerer Priorität.

**Siehe auch**

- [„background\\_priority-Option \[nicht mehr empfohlen\]“ auf Seite 584](#)
- [„priority-Option“ auf Seite 656](#)
- [max\\_priority-Verbindungseigenschaft auf Seite 725](#)
- [„Tipp: Ressourcenwächter verwenden“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)

## max\_query\_tasks-Option

Gibt die maximale Anzahl von Serveraufgaben an, die der Datenbankserver zur parallelen Verarbeitung einer Abfrage verwenden kann

**Zulässige Werte**

Ganzzahl

**Standardwert**

0

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Die Option max\_query\_tasks legt den maximalen Parallelitätsgrad fest, der bei einer SQL-Anweisung verwendet werden kann. Diese Option legt die Anzahl der Serveraufgaben fest, die zur parallelen Verarbeitung einer Abfrage verwendet werden können. Der Standardwert ist "0", was es dem Datenbankserver ermöglicht, beliebig viele Aufgaben zu verwenden. Jeder andere Wert für die Option max\_query\_tasks legt die maximale Anzahl von in der Abfrage zulässigen Aufgaben fest. Wenn Sie die

Option `max_query_tasks` auf 1 setzen, wird die abfrageinterne Parallelität (Intra-Query-Parallelität) deaktiviert.

Weitere Informationen zu Serveraufgaben, zu Threads und zur Abfrageausführung finden Sie unter „[SQL Anywhere-Threading](#)“ auf Seite 171 und „[Datenbankserverkonfiguration der Multiprogramming-Stufe](#)“ auf Seite 175.

Die Anzahl der Aufgaben, die der Datenbankserver bei allen Anforderungen verwenden kann, wird durch den Schwellenwert begrenzt, der gesetzt wird, indem beim Start die Option `-gn` verwendet wird. Diese Anzahl ist ein globales Maximum für alle Datenbanken und Verbindungen, die von diesem Server betrieben werden. Die Anzahl der Aufgaben, die bei einer Anforderung ausgeführt werden können, wird auch durch die Anzahl der logischen Prozessoren beschränkt, die dem Datenbankserver verfügbar sind. Das Einstellen der Prozessoren-Parallelität auf "1", mit der Option `-gtc` beispielsweise, deaktiviert die abfrageinterne Parallelität.

Wenn die abfrageinterne Parallelität aktiviert ist, wird sie verwendet, um `SELECT`-Anweisungen zu verarbeiten, die bestimmten Qualifikationen entsprechen. Das Vorhandensein eines `Exchange-Operators` im Zugriffsplan für die Abfrage zeigt an, dass die abfrageinterne Parallelität verwendet wurde.

Sie können temporäre oder `PUBLIC`-Einstellungen für diese Option in einzelnen `INSERT`-, `UPDATE`-, `DELETE`-, `SELECT`-, `UNION`-, `EXCEPT`- und `INTERSECT`-Anweisungen aufheben, indem Sie eine `OPTION`-Klausel in die Anweisung aufnehmen.

### Siehe auch

- „[Datenbankserveroption -gn](#)“ auf Seite 244
- „[Datenbankserveroption -gt](#)“ auf Seite 251
- „[Datenbankserveroption -gtc](#)“ auf Seite 253
- `max_query_tasks`-Verbindungseigenschaft auf Seite 725

## max\_recursive\_iterations-Option

Begrenzt die maximale Anzahl von Iterationen eines rekursiven allgemeinen Tabellenausdrucks

### Zulässige Werte

Ganzzahl

### Standardwert

100

### Bereich

Kann für eine einzelne Verbindung oder für `PUBLIC` gesetzt werden. Sie müssen das `SET ANY PUBLIC` `OPTION`-Systemprivileg haben, um diese Option für `PUBLIC` oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Die Berechnung eines rekursiven allgemeinen Tabellenausdrucks wird mit Fehlermeldung abgebrochen, wenn sie nicht innerhalb einer angegebenen Anzahl von Wiederholungen beendet werden kann.

Rekursive Unterabfragen bewirken oft einen geometrisch zunehmenden Bedarf an Ressourcen für jede zusätzliche Iteration. Begrenzen Sie durch das Setzen dieser Option den Verbrauch von Zeit und Ressourcen, bevor eine unendliche Rekursion erkannt wird, und lassen Sie gleichzeitig zu, dass Ihre rekursiven gemeinsamen Tabellenausdrücke wie vorgesehen funktionieren.

Wenn diese Option auf "0" gesetzt wird, werden rekursive allgemeine Tabellenausdrücke deaktiviert.

#### Siehe auch

- „Rekursive allgemeine Tabellenausdrücke“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- `max_recursive_iterations`-Verbindungseigenschaft auf Seite 725

## max\_statement\_count-Option

Steuert einen Ressourcenwächter, der die maximale Anzahl von vorbereiteten Anweisungen begrenzt, die eine Verbindung gleichzeitig verwenden kann

#### Zulässige Werte

Ganzzahl

#### Standardwert

50

#### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

#### Bemerkungen

Anwendungen, die vorbereitete Anweisungen verwenden, können den Fehler "Ressourcenwächter hat Grenze für 'vorbereitete Anweisungen' überschritten" erhalten, wenn die vorbereiteten Anweisungen nicht explizit gelöscht werden, sobald sie nicht mehr benötigt werden. Die Datenbankoption `max_statement_count` ist ein Ressourcenwächter, der es dem DBA ermöglicht, die Anzahl der vorbereiteten Anweisungen pro Verbindung zu begrenzen. Falls ein Vorgang die Grenze für eine Verbindung überschreitet, wird ein Fehler erzeugt, der anzeigt, dass die Ressourcengrenze überschritten wurde.

Wenn eine Verbindung eine gespeicherte Prozedur ausführt, wird diese gespeicherte Prozedur mit den Privilegien des Prozedureigentümers ausgeführt. Die von der Prozedur verwendeten Ressourcen werden jedoch der aktuellen Verbindung zugeordnet.

Der Datenbankserver hält Datenstrukturen für jede vorbereitete Anweisung aufrecht, die eine Verbindung erstellt. Diese Strukturen werden erst freigegeben, wenn die Anwendung dem Datenbankserver signalisiert, dass die vorbereiteten Anweisungen nicht mehr benötigt werden, oder wenn die Verbindung getrennt wird. Um die Anzahl der Anweisungen bei einer Verbindung zu vermindern, müssen Sie das Äquivalent einer DROP STATEMENT-Anforderung ausführen. Die folgende Tabelle enthält die Befehle, die Sie bei den von SQL Anywhere unterstützten APIs ausführen können:

Schnittstelle	Anweisung
ADO	RecordSet.Close
ADO.NET	SADataReader.Close oder SADataReader.Dispose
Embedded SQL	DROP STATEMENT
Java	resultSet.Close, Statement.Close
ODBC	SQLFreeStmt( hstmt, SQL_DROP ) oder SQLFreeHandle( SQL_HANDLE_STMT, hstmt )

#### Hinweis

In Java and .NET wird empfohlen, dass Sie Anweisungen explizit löschen. Verlassen Sie sich bei dieser Bereinigung nicht auf die Abfalldatensammlung, weil die Sprachroutinen keine Serveraufrufe ausgeben, um die Anweisungsressourcen freizugeben. Außerdem gibt es keine Garantie, wann die Routinen zur Abfalldatensammlung ausgeführt werden.

Wenn ein Server mehr als die Standardanzahl von vorbereiteten Anweisungen jeweils für eine Verbindung unterstützen muss, sollte die Einstellung max\_statement\_count auf einen höheren Wert gesetzt werden. Beachten Sie allerdings, dass eine größere Anzahl von aktiven vorbereiteten Anweisungen zusätzlichen Serverspeicher verbraucht. Sie können den Ressourcenwächter für vorbereitete Anweisungen ganz ausschalten, indem Sie die Option max\_statement\_count auf "0" (Null) setzen, aber das ist nicht empfehlenswert. Wenn Sie es tun, wird der Datenbankserver für eine Beendigung aufgrund einer Speichermangel-Bedingung bei solchen Anwendungen anfällig, die vorbereitete Anweisungen nicht korrekt freigeben.

#### Siehe auch

- „Vorbereitete Anweisungen“ [[SQL Anywhere Server - Programmierung](#)]
- „DROP STATEMENT-Anweisung [ESQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- max\_statement\_count-Verbindungseigenschaft auf Seite 725
- „Tipp: Ressourcenwächter verwenden“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## max\_temp\_space-Option

Steuert die Höchstmenge an Speicher für temporäre Dateien, die eine Verbindung verwenden kann

#### Zulässige Werte

Integer [ k | m | g | p ]

#### Standardwert

0

## Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option für PUBLIC setzen zu können. Wird sofort wirksam.

Wenn Sie diese Option temporär setzen, gilt diese Einstellung nur für die aktuelle Verbindung. Unterschiedliche Verbindungen mit derselben Benutzer-ID haben unterschiedliche Einstellungen für diese Option.

## Bemerkungen

Mit dieser Option können Sie die Höchstmenge an Speicher für temporäre Dateien angeben, die eine Verbindung verwenden kann, bevor die Anforderung fehlschlägt, weil die Begrenzung des Speichers für temporäre Dateien überschritten wird. Die Option `temp_space_limit_check` muss auf "On" gesetzt sein (der Standardwert), damit die Option `max_temp_space` wirksam werden kann.

Der Standardwert "0" zeigt an, dass es keine feste Begrenzung für die Höchstmenge an Speicher für temporäre Dateien gibt, die eine Verbindung anfordern kann. Jeder andere Wert gibt die Anzahl der Bytes des Speichers für temporäre Dateien an, die eine Verbindung verwenden kann. Sie können **k**, **m** oder **g** verwenden, um die Einheit in kB, MB bzw. GB anzugeben. Wenn Sie **p** verwenden, ist das Argument ein Prozentsatz des gesamten verfügbaren Speichers für temporäre Dateien.

Bei Verbindungen, die Speicherplatz für temporäre Dateien anfordern, überprüft der Datenbankserver die Begrenzung anhand der Einstellung der `max_temp_space`-Option, um zu gewährleisten, dass die Anforderung unterhalb der Maximalgröße liegt. Wenn die Verbindung mehr Speicher für temporäre Dateien als zulässig anfordert, schlägt die Anforderung fehl und der Fehler `SQLSTATE_TEMP_SPACE_LIMIT` wird generiert.

## Siehe auch

- „`temp_space_limit_check`-Option“ auf Seite 689
- „`sa_disk_free_space`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `max_temp_space`-Verbindungseigenschaft auf Seite 726

## Beispiel

Legen Sie eine Grenze von 1 GB für eine Verbindung fest:

```
SET OPTION PUBLIC.max_temp_space = '1g';
```

Mit beiden folgenden Anweisungen wird eine Grenze von 1 MB für eine Verbindung festgelegt:

```
SET OPTION PUBLIC.max_temp_space = 1048576;
```

```
SET OPTION PUBLIC.max_temp_space = '1m';
```

Fünf Prozent des gesamten verfügbaren temporären Speichers verwenden:

```
SET OPTION PUBLIC.max_temp_space = '5p';
```

## min\_password\_length-Option

Setzt die Mindestlänge für neue Kennwörter in der Datenbank

## Zulässige Werte

Ganzzahl

Der Wert wird in Byte angegeben. Für Einbyte-Zeichensätze entspricht dieser Wert der Anzahl der Zeichen.

## Standardwert

3 Zeichen

## Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

## Bemerkungen

Mit dieser Option kann der Datenbankadministrator eine Mindestlänge für alle Kennwörter erzwingen, um die Sicherheit zu erhöhen. Bestehende Kennwörter sind nicht betroffen. Kennwörter haben eine maximale Länge von 255 Byte und beachten die Groß/Kleinschreibung.

## Siehe auch

- [„verify\\_password\\_function-Option“ auf Seite 704](#)
- [„Hinweise zur Sicherheit: Kennwörter“ auf Seite 1410](#)
- [min\\_password\\_length-Verbindungseigenschaft auf Seite 726](#)

## Beispiel

Setzt die Mindestlänge für neue Kennwörter auf 6 Byte

```
SET OPTION PUBLIC.min_password_length = 6;
```

## min\_role\_admins-Option

Legt die minimale Anzahl von Administratoren fest, die für eine Rolle erforderlich ist.

## Zulässige Werte

Ganzzahl zwischen 1 und 10.

## Standardwert

1

## Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Die Mindestanzahl von Administratoren wird überprüft, wenn Rollen erstellt, gelöscht oder entzogen werden, wenn Benutzer manuell gesperrt werden oder wenn ein Benutzer wegen Überschreitung des Werts für die `max_days_since_login`-Option automatisch gesperrt wird.

Außerdem wird die Mindestanzahl von Administratoren überprüft, wenn ein Benutzerkennwort auf NULL geändert wird.

Benutzer, die kein NULL-Kennwort haben, werden als Administratoren gezählt. Änderungen am Wert dieser Option sind nur zulässig, wenn jede Rolle mindestens die angegebene Anzahl von Administratoren aufweist. Wenn beim Entziehen einer Rolle die Anzahl von Administratoren unter den Wert der `min_role_admins`-Option fällt, gibt die Anweisung einen Fehler zurück. Gesperrte Konten werden im Hinblick auf die Anzahl von Administratoren nicht berücksichtigt. Administratoren mit abgelaufenem Kennwort werden jedoch weiterhin mitgezählt.

**Siehe auch**

- „Rollen“ auf Seite 1271

**Beispiel**

Im folgenden Beispiel wird die `min_role_admins`-Option auf 2 gesetzt:

```
SET OPTION PUBLIC.MIN_ROLE_ADMINS = 2;
```

## **ml\_remote\_id-Option**

Legt die entfernte ID für eine entfernte Datenbank in einem MobiLink-Synchronisationssystem fest.

**Zulässige Werte**

Ein beliebiger Wert, der die Datenbank für die MobiLink-Synchronisation eindeutig kennzeichnet

**Standardwert**

NULL

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY USER DEFINED OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Diese Option ordnet eine entfernte ID für eine entfernte Datenbank in einem MobiLink-Synchronisationssystem zu. Die entfernte ID muss innerhalb des Synchronisationssystems eindeutig sein.

Wenn Sie die entfernte ID manuell festlegen und danach die entfernte Datenbank neu erstellen, müssen Sie entweder der neu erstellten entfernten Datenbank einen anderen Namen geben oder die Prozedur `ml_reset_sync_state` verwenden, um die Statusinformationen für die entfernte Datenbank in der konsolidierten Datenbank zurückzusetzen.

### Vorsicht

Der sicherste Zeitpunkt zum Ändern der entfernten ID ist vor der ersten Synchronisation. Falls Sie die entfernte ID später ändern, müssen Sie direkt vor dieser Änderung eine vollständige, erfolgreiche Synchronisation durchgeführt haben. Andernfalls könnten Sie Daten verlieren und die Datenbank könnte inkonsistent werden.

### Siehe auch

- „Entfernte IDs“ [*MobiLink - Clientadministration*]
- „Name der entfernten MobiLink-ID“ [*MobiLink - Clientadministration*]
- „Entfernte IDs und MobiLink-Benutzernamen in Skripten“ [*MobiLink - Clientadministration*]
- „ml\_reset\_sync\_state-Systemprozedur“ [*MobiLink - Serveradministration*]

### Beispiel

Die folgende SQL-Anweisung setzt die entfernte ID auf den Wert 'HR001':

```
SET OPTION PUBLIC.ml_remote_id = 'HR001'
```

## nearest\_century-Option

Steuert die Interpretation von zweistelligen Jahresangaben bei Konvertierungen von Zeichenfolgen in Datumsangaben

### Zulässige Werte

Ganzzahl zwischen 0 und 100

### Standardwert

50

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option steuert die Behandlung von zweistelligen Jahresangaben bei der Konvertierung von Zeichenfolgen in Datumsangaben oder Zeitstempeln.

Die Einstellung nearest\_century ist ein numerischer Wert, der als Überschreitungslimit fungiert. Zweistellige Jahre unterhalb des Werts werden in 20JJ konvertiert, während Jahre größer oder gleich dem Wert in 19JJ konvertiert werden.

Früher verhielt sich SQL Anywhere so, dass er 1900 zum Jahr hinzugefügt hat. Adaptive Server Enterprise verhält sich so, dass er das nächste Jahrhundert verwendet und so bei jedem Jahrwert yy, der kleiner als 50 ist, das Jahr auf 20yy setzt.

**Siehe auch**

- „Kompatibilitätsoptionen“ auf Seite 559
- `nearest_century`-Verbindungseigenschaft auf Seite 728

## **non\_keywords-Option**

Schaltet individuelle Schlüsselwörter aus und ermöglicht ihre Verwendung als Bezeichner

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Leere Zeichenfolge

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Diese Option deaktiviert einzelne Schlüsselwörter. Mit dieser Option kann sichergestellt werden, dass mit älteren Produktversionen erstellte Anwendungen durch neue Schlüsselwörter nicht gestört werden. Falls Sie einen Bezeichner in Ihrer Datenbank haben, der nun ein Schlüsselwort ist, können Sie den Bezeichner entweder in allen Anwendungen oder Skripten mit Anführungszeichen umgeben oder das Schlüsselwort mithilfe der Option `non_keywords` ausschalten.

Es ist nicht möglich, die Schlüsselwörter `set`, `option` und `options` zu deaktivieren. Ob ein Wort als Schlüsselwort identifiziert wird, hängt von folgenden Faktoren ab (in der genannten Reihenfolge):

- Es ist in der SQL Anywhere-Liste der reservierten Wörter enthalten.
- Es wurde mit der `reserved_keywords`-Option aktiviert.
- Es wurde mithilfe der `non_keywords`-Option deaktiviert.

Die folgende Anweisung verhindert, dass `TRUNCATE` und `SYNCHRONIZE` als Schlüsselwörter erkannt werden:

```
SET OPTION non_keywords = 'TRUNCATE, SYNCHRONIZE';
```

Jede neue Einstellung dieser Option ersetzt die frühere Einstellung. Die folgende Anweisung löscht alle früheren Einstellungen.

```
SET OPTION non_keywords =;
```

Ein Nebeneffekt dieser Option ist, dass SQL-Anweisungen, die ein deaktiviertes Schlüsselwort verwenden, nicht angewendet werden können. Sie erzeugen einen Syntaxfehler.

Sie können mit der `reserved_keywords`-Option individuelle Schlüsselwörter aktivieren.

### Siehe auch

- „reserved\_keywords-Option“ auf Seite 665
- „Schlüsselwörter“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsoptionen“ auf Seite 559
- non\_keywords-Verbindungseigenschaft auf Seite 728
- „reserved\_keywords-Option“ auf Seite 665

## odbc\_describe\_binary\_as\_varbinary

Steuert, wie der SQL Anywhere ODBC-Treiber die BINARY-Spalten beschreibt

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Mit dieser Option können Sie wählen, ob alle BINARY- und VARBINARY-Spalten für Ihre Anwendung als BINARY oder VARBINARY beschrieben werden sollen. Standardmäßig beschreibt der SQL Anywhere ODBC-Treiber sowohl BINARY- als auch VARBINARY-Spalten als SQL\_BINARY. Wenn diese Option auf "On" eingestellt ist, beschreibt der ODBC-Treiber BINARY- und VARBINARY-Spalten als SQL\_VARBINARY. Unabhängig von der Einstellung dieser Option ist es nicht möglich, zwischen BINARY- und VARBINARY-Spalten zu unterscheiden.

Es kann nützlich sein, diese Option auf "On" zu setzen, wenn Sie Delphi-Anwendungen verwenden, bei denen BINARY-Spalten immer mit Nullen aufgefüllt werden, VARBINARY-Spalten hingegen nicht. Sie können die Performance von Delphi-Anwendungen steigern, indem Sie diese Option auf "On" setzen, damit alle Spalten als Datentypen mit variabler Länge behandelt werden.

### Siehe auch

- „BINARY-Datentyp“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „VARBINARY-Datentyp“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- odbc\_describe\_binary\_as\_varbinary-Verbindungseigenschaft auf Seite 728

## odbc\_distinguish\_char\_and\_varchar-Option

Steuert, wie der SQL Anywhere ODBC-Treiber die CHAR-Spalten beschreibt

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Wenn eine Verbindung geöffnet wird, benutzt der SQL Anywhere ODBC-Treiber die Einstellungen dieser Option, um festzulegen, wie CHAR-Spalten beschrieben werden. Wenn diese Option auf "Off" gesetzt ist (Standardwert), werden CHAR-Spalten als SQL\_VARCHAR beschrieben. Wenn diese Option auf "On" gesetzt ist, werden CHAR-Spalten als SQL\_CHAR beschrieben. VARCHAR-Spalten werden immer als SQL\_VARCHAR beschrieben.

**Siehe auch**

- „CHAR-Datentyp“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „VARCHAR-Datentyp“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `odbc_distinguish_char_and_varchar`-Verbindungseigenschaft auf Seite 728

## **oem\_string-Option**

Speichert benutzerdefinierte Informationen in der Titelseite der Datenbankdatei

**Zulässige Werte**

Zeichenfolge (bis zu 128 Byte)

**Standardwert**

Leere Zeichenfolge

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Sie können Informationen in der Titelseite der Datenbankdatei speichern und sie später extrahieren, indem Sie die Datei direkt von Ihrer Anwendung aus lesen. Diese Seite ist im System-DBSpace "file header" (Dateititel) gespeichert. Wenn Sie für die OEM-Zeichenfolge einen längeren Wert als 128 Byte angeben, wird ein Fehler zurückgegeben.

Es kann nützlich sein, Informationen wie Schemaversionen, den Anwendungsnamen, die Anwendungsversion etc. zu speichern. Alternativ könnte eine Anwendung, ohne die Datenbank zu starten,

die OEM-Zeichenfolge verwenden, um zu ermitteln, ob die Datenbankdatei der Anwendung zugeordnet ist, oder Sie können Ihre Anwendung so planen, dass sie die Informationen verwendet, um zu validieren, dass die Datenbankdatei für Ihre Anwendung bestimmt ist. Dies geschieht, indem eine Zeichenfolge gespeichert wird, die die Anwendung für Validierungszwecke liest, bevor die Datenbankdatei verwendet wird. Sie könnten auch Metadaten extrahieren, um sie Benutzern anzuzeigen.

Um `oem_string` im System-DBSpace "file header" zu setzen, führen Sie die folgende Anweisung aus:

```
SET OPTION PUBLIC.oem_string=user-specified-string;
```

Der *user-specified-string*-Wert wird sowohl in der Systemtabelle `ISYSOPTION` als auch im Datei-Header des System-DBSpace gespeichert. Sie müssen die Zeichenfolge im erforderlichen Zeichensatz definieren, bevor Sie sie in einer `SET OPTION`-Anweisung angeben können, weil keine Konvertierung der Zeichenfolge stattfindet, wenn sie an die `SET OPTION`-Anweisung übergeben wird. Sie können die `CSCONVERT`-Funktion verwenden, um die Zeichenfolge in den erforderlichen Zeichensatz zu konvertieren.

Sie können den Wert von `oem_string` auf folgende Arten abrufen:

- Unter Verwendung der Verbindungseigenschaft `oem_string`:

```
SELECT CONNECTION_PROPERTY( 'oem_string' );
```

- Unter Verwendung der `SYSOPTION`-Systemansicht:

```
SELECT setting FROM SYSOPTION WHERE "option" = 'oem_string';
```

SQL Anywhere stellt zwei Beispielprogramme im *oem\_string*-Verzeichnis zur Verfügung:

- *dboem.cpp* ist ein C-Programm, das illustriert, wie die OEM-Zeichenfolge extrahiert und im Fenster der Datenbankservermeldungen angezeigt wird.
- *dboem.pl* illustriert, wie die OEM-Zeichenfolge extrahiert und im "stdout" innerhalb eines PERL-Skripten angezeigt wird.

### Vorsicht

Anwendungen dürfen die OEM-Zeichenfolge in der Datenbank nicht direkt beschreiben, weil dies die Datenbank-Titelseite beschädigt.

Unter Windows können Anwendungen die Datei nicht direkt lesen, wenn ein Server die Datenbankdatei geladen hat. Der Datenbankserver hat eine Exklusivsperrung auf der Datei. Auf einer unterstützten Unix-Plattform hingegen können Anwendungen mit Leseberechtigung die Datei jederzeit direkt lesen. Allerdings werden Änderungen an der OEM-Zeichenfolge möglicherweise nicht sofort angezeigt. Das Ausgeben eines Checkpoints bewirkt, dass der Datenbankserver Seite 0 auf die Festplatte leert und den aktuellen OEM-Zeichenfolgenwert widerspiegelt.

Sollte der Datenbankserver zwischen der Änderung der OEM-Zeichenfolge und dem nächsten Checkpoint ausfallen, spiegelt der Header der Datei möglicherweise nicht den neuen OEM-Zeichenfolgenwert wider. Der neue OEM-Zeichenfolgenwert wird nach einer Wiederherstellung der Datenbank korrekt gesetzt.

**Siehe auch**

- „CSCONVERT-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- oem\_string-Verbindungseigenschaft auf Seite 728

**Beispiel**

Das folgende Beispiel verschlüsselt die OEM-Zeichenfolge, die Informationen über die Datenbankdatei enthält, und speichert sie in der Datenbank-Titeldatei:

```
BEGIN
  DECLARE @v VARCHAR(100);
  SET @v = BASE64_ENCODE( ENCRYPT( 'database version 10', 'abc' ) );
  EXECUTE IMMEDIATE 'SET OPTION PUBLIC.oem_string = '' | | @v | | ''';
END;
```

Sie können den Wert der OEM-Zeichenfolge abrufen, indem Sie die folgende Anweisung ausführen:

```
SELECT DECRYPT(
  BASE64_DECODE(
    CONNECTION_PROPERTY( 'oem_string' ) ), 'abc' )
```

**on\_charset\_conversion\_failure-Option**

Legt fest, was geschieht, wenn während der Zeichensatzübersetzung ein Fehler auftritt

**Zulässige Werte**

Ignore, Warning, Error

**Standardwert**

Ignore

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Legt fest, was geschieht, wenn während der Zeichensatzübersetzung ein Fehler auftritt. Folgende Möglichkeiten bestehen:

- **Ignore** Fehler und Warnung erscheinen nicht.
- **Warning** Ersetzungen und unzulässige Zeichen werden als Warnungen ausgegeben. Ungültige Zeichen werden nicht übersetzt.
- **Error** Ersetzungen und unzulässige Zeichen werden als Fehler ausgegeben.

Wenn eine Zeichensatzkonvertierung zwischen dem Client und der Datenbank erforderlich ist und ungültige Zeichen erkannt werden bzw. wenn Zeichenersetzung verwendet wird, steuert diese Option, ob der Vorgang ignoriert oder eine Warnung bzw. ein Fehler zurückgegeben wird.

Übersetzer für die Konvertierung von Einbyte-Zeichen in Einbyte-Zeichen können weder Ersetzungen noch unzulässige Zeichen melden und müssen daher auf "Ignore" gesetzt werden.

Diese Option steuert nicht das Verhalten, wenn verlustreiche Konvertierungen auf dem Client stattfinden. Beispiel: SQL-Anweisungen vom Client müssen im CHAR-Datenbank-Zeichensatz sein bzw. in ihn konvertiert werden. Nehmen wir an, eine Unicode-Clientanwendung bereitet eine SQL-Anweisung vor und diese Anweisung enthält Zeichen, die nicht im CHAR-Datenbank-Zeichensatz dargestellt werden können. Stattdessen werden Ersatzzeichen verwendet. Da die verlustreiche Konvertierung allerdings auf dem Client stattgefunden hat, bemerkt sie der Datenbankserver nicht.

### Siehe auch

- „Vergleiche zwischen CHAR und NCHAR“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Konvertierungen von NCHAR in CHAR“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Verlustreiche Konvertierung und Ersetzungszeichen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- [on\\_charset\\_conversion\\_failure](#)-Verbindungseigenschaft auf Seite 728

## on\_tsql\_error-Option

Steuert die Fehlerbehandlung in gespeicherten Prozeduren

### Zulässige Werte

- **Stopp** Nach Erkennung eines Fehlers soll die Ausführung sofort gestoppt werden.
- **Conditional** Die Verarbeitung wird fortgesetzt, wenn die Prozedur ON EXCEPTION RESUME verwendet und die dem Fehler folgende Anweisung den Fehler verarbeitet, andernfalls wird die Verarbeitung beendet.
- **Continue** Die Ausführung wird ohne Rücksicht auf die Art der folgenden Anweisung fortgesetzt. Wenn mehrere Fehler auftreten, wird nach Abschluss der gespeicherten Prozedur der erste Fehler zurückgegeben, der in der Prozedur aufgetreten ist.

### Standardwert

Conditional

Continue bei jConnect-Verbindungen

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option steuert die Fehlerbehandlung in gespeicherten Prozeduren und Transact-SQL-Batches. Innerhalb des TRY-Blocks einer BEGIN...END-Anweisung hat diese Option keine Wirkung und die Fehlerbehandlung verhält sich gemäß der Definition innerhalb des TRY-Blocks.

Die Einstellungen "Conditional" und "Continue" für `on_tsq_error` werden für die Kompatibilität mit Adaptive Server Enterprise benutzt, wobei "Continue" das Verhalten von Adaptive Server Enterprise am genauesten nachbildet. Wenn Fehler früher gemeldet werden sollen, benutzen Sie die Einstellung "Conditional" beim Erstellen neuer gespeicherter Transact-SQL-Prozeduren.

Wenn diese Option auf "Stop" oder "Continue" gesetzt ist, hat sie Vorrang vor den Einstellungen der `continue_after_raisererror`-Option. Ist die Option hingegen auf "Conditional" (Standard) gesetzt, wird das Verhalten nach der RAISERROR-Anweisung durch die Einstellung der Option `continue_after_raisererror` bestimmt.

**Siehe auch**

- „Transact-SQL-Prozedursprache“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „`continue_after_raisererror`-Option“ auf Seite 594
- „Kompatibilitätsoptionen“ auf Seite 559
- „`sp_tsq_environment`-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `on_tsq_error`-Verbindungseigenschaft auf Seite 728

## optimization\_goal-Option

Legt fest, ob die Abfrageverarbeitung dahingehend optimiert wird, die erste Zeile schnell zurückzugeben, oder ob die Kosten für die Ausgabe der vollständigen Ergebnismenge minimiert werden sollen.

**Zulässige Werte**

First-row, All-rows

**Standardwert**

All-rows

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Mit der Option `optimization_goal` wird festgelegt, ob SQL Anywhere SQL-Anweisungen in Datenmanipulationssprache (DML - Data Manipulation Language) auf Antwortzeiten oder Ressourcenverbrauch optimiert.

Wenn die Option auf "All-rows" (Standardwert) gesetzt ist, optimiert SQL Anywhere eine Abfrage, indem ein Zugriffsplan mit der geschätzten Mindestabruflzeit benutzt wird. Die Einstellung "All-rows" für "optimization\_goal" ist in der Regel für Anwendungen sinnvoll, die die komplette Ergebnismenge verarbeiten sollen, wie z.B. Sybase PowerBuilder DataWindow-Anwendungen. Die Einstellung "All-rows" ist auch für unempfindliche Cursor (ODBC-statisch) geeignet, da die komplette Ergebnismenge beim Öffnen des Cursors initialisiert wird. Außerdem ist die Einstellung auch für abrollende Cursor (ODBC-Keyset-gesteuert) geeignet, weil der Zweck eines solchen Cursors darin besteht, das Scrollen durch die Ergebnismenge zu ermöglichen.

Wenn die Option auf First-row gesetzt ist, wählt SQL Anywhere einen Zugriffsplan, der die Zeitspanne zum Abruf der ersten Zeile der Ergebnismenge reduzieren soll, worunter möglicherweise die Gesamtabrufzeit leidet. Insbesondere vermeidet der SQL Anywhere-Optimierer nach Möglichkeit Zugriffspläne, die die Materialisierung von Ergebnissen erfordern, um die Zeitspanne bis zum Zurückgeben der ersten Zeile zu verkürzen. Mit dieser Einstellung bevorzugt der Optimierer Zugriffspläne, die für die ORDER BY-Klausel einer Abfrage einen Index benutzen, anstelle von Zugriffsplänen, die einen expliziten Sortiervorgang benötigen.

Sie können den Tabellen-Hint FASTFIRSTROW in der FROM-Klausel einer Abfrage verwenden, um das Optimierungsziel für eine bestimmte Abfrage auf "First-row" zu setzen, ohne die Einstellung von optimization\_goal ändern zu müssen.

Weitere Hinweise zum Tabellen-Hint FASTFIRSTROW finden Sie unter „FROM-Klausel“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Sie können temporäre oder PUBLIC-Einstellungen für diese Option in einzelnen INSERT-, UPDATE-, DELETE-, SELECT-, UNION-, EXCEPT- und INTERSECT-Anweisungen aufheben, indem Sie eine OPTION-Klausel in die Anweisung aufnehmen.

### Siehe auch

- [optimization\\_goal-Verbindungseigenschaft auf Seite 728](#)

## optimization\_level-Option

Steuert den Aufwand, den der SQL Anywhere-Abfrageoptimierer betreibt, um einen Zugriffsplan für eine SQL-Anweisung zu finden.

### Zulässige Werte

0-15

### Standardwert

9

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Die optimization\_level-Option steuert die Menge des Aufwands, den der SQL Anywhere-Optimierer zur Optimierung von SQL-Datenmanipulationssprachen-Anweisungen (DML - Data Manipulation Language) einsetzt. Diese Option steuert die maximale Anzahl von alternativen Join-Strategien, die der Optimierer bei jedem SELECT-Block berücksichtigt. Je höher die Einstellung von optimization\_level ist, desto größer ist die maximale Anzahl von alternativen Join-Strategien, die der Optimierer berücksichtigt.

Wenn die Option auf "0" eingestellt ist, wählt der SQL Anywhere-Optimierer den ersten Zugriffsplan aus, der in Betracht kommt, wodurch alle Kosten-basierende Vergleiche von alternativen Plänen vermieden

werden. Zusätzlich werden bei Stufe 0 einige semantische Optimierungen von verschachtelten Abfragen deaktiviert. Wenn diese Option auf einen höheren Wert als 0 eingestellt ist, evaluiert der Optimierer verschiedene Strategien und wählt jene mit den geringsten zu erwartenden Kosten aus. Wenn diese Option auf einen höheren Wert als der Standardwert (9) eingestellt ist, ist der Optimierer aggressiver bei der Suche nach alternativen Strategien, was möglicherweise zu einem größeren Zeitaufwand während der Optimierungsphase führt.

In der Regel wird diese Option temporär auf niedrigere Stufen (0, 1 oder 2) gesetzt, wenn die Anwendung kürzere OPEN-Zeiten für eine DML-Anweisung benötigt. Es ist bekannt, dass auch bei komplexen Anweisungen die Ausführungszeit für die Abfrage sehr kurz sein kann und der vom Optimierer ausgewählte spezifische Zugriffsplan weniger wichtig ist. Es ist nicht empfehlenswert, einen anderen als den Standardwert für die PUBLIC-Einstellung von `optimization_level` zu verwenden.

Die Auswirkung der Einstellung der `optimization_level`-Option ist unabhängig von den Einstellungen der `optimization_goal`- und `optimization_workload`-Optionen.

Einfache DML-Anweisungen (Einzel-Block- und Einzel-Tabellen-Anweisungen, die Gleichheitsbedingungen in der WHERE-Klausel enthalten, die eine bestimmte Zeile eindeutig identifizieren) werden heuristisch optimiert und umgehen den Kosten-basierten Optimierer zur Gänze. Die Optimierung von einfachen DML-Anweisungen wird nicht durch die Einstellung der `optimization_level`-Option beeinflusst. Die Zählung der Anzahl von Anforderungen, die durch den Bypass-Mechanismus des Optimierers optimiert wurden, steht als die QueryBypassed-Verbindungseigenschaft zur Verfügung.

Weitere Hinweise zur QueryBypassed-Verbindungseigenschaft finden Sie im Abschnitt „[Liste der Verbindungseigenschaften](#)“ auf Seite 711.

Sie können temporäre oder PUBLIC-Einstellungen für diese Option in einzelnen INSERT-, UPDATE-, DELETE-, SELECT-, UNION-, EXCEPT- und INTERSECT-Anweisungen aufheben, indem Sie eine OPTION-Klausel in die Anweisung aufnehmen.

#### Siehe auch

- „So funktioniert der Optimierer“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- `optimization_level`-Verbindungseigenschaft auf Seite 729

## `optimization_workload`-Option

Legt fest, ob die Abfrageverarbeitung für eine Arbeitslast optimiert wird, die aus einer Mischung von Aktualisierungen und Lesevorgängen besteht, oder für eine Arbeitslast, die hauptsächlich auf Lesevorgängen basiert.

#### Zulässige Werte

Mixed, OLAP

#### Standardwert

Mixed

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Die Option `optimization_workload` steuert, ob SQL Anywhere Abfragen für eine Verarbeitungslast aus gemischten Aktualisierungen und Lesevorgängen oder aus fast reinen Lesevorgängen optimiert.

Wenn die Option auf "Mixed" gesetzt ist (Standard), wählt SQL Anywhere Algorithmen zur Abfrageoptimierung für die Verarbeitungslast, die als Mischung aus kurzen Einfügungen, Aktualisierungen, Löschungen und längeren Leseabfragen definiert wird.

Wenn die Option auf "OLAP" gesetzt ist, wählt SQL Anywhere Algorithmen zur Abfrageoptimierung für die Verarbeitungslast, die aus längeren Leseabfragen und Aktualisierungen von Batches besteht. Der Optimierer kann sich insbesondere dafür entscheiden, den Ausführungsalgorithmus Clustered Hash Group By zu verwenden.

Wenn die Option auf "OLAP" gesetzt ist, wird der Abfrageausführungsalgorithmus Clustered Hash Group By aktiviert. Wenn die Option auf "Mixed" gesetzt ist (Standardwert), ist er deaktiviert.

Sie können temporäre oder PUBLIC-Einstellungen für diese Option in einzelnen INSERT-, UPDATE-, DELETE-, SELECT-, UNION-, EXCEPT- und INTERSECT-Anweisungen aufheben, indem Sie eine OPTION-Klausel in die Anweisung aufnehmen.

### Siehe auch

- [„optimization\\_level-Option“ auf Seite 648](#)
- [optimization\\_workload-Verbindungseigenschaft auf Seite 729](#)

## pinned\_cursor\_percent\_of\_cache-Option

Gibt an, wie viel Cache für die Bereithaltung von Cursors benutzt werden kann

### Zulässige Werte

Ganzzahl zwischen 0 und 100

### Standardwert

10

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

### Bemerkungen

Der Datenbankserver benutzt Seiten des virtuellen Speichers für die Datenstrukturen, die für die Verarbeitung von Cursors erforderlich sind. Diese Seiten werden im Speicher zwischen Fetch-Anforderungen gesperrt, damit sie sofort bereit sind, wenn die nächste Fetch-Anforderung eintrifft.

Um zu verhindern, dass diese Seiten auf Systemen mit geringem Speicher zu viel Cachespeicher belegen, wird ein Grenzwert für den Prozentsatz des Caches festgelegt, der für die Bereithaltung von Cursors verwendet werden darf. Sie können die Option `pinned_cursor_percent_of_cache` verwenden, um das Limit festzulegen.

Der Prozentwert wird mit 0 bis 100 angegeben, Standard ist 10. Wenn die Option auf "0" gesetzt wird, werden zwischen Fetch-Anforderungen keine Cursorseiten im Cache bereitgehalten.

**Siehe auch**

- [pinned\\_cursor\\_percent\\_of\\_cache-Verbindungseigenschaft auf Seite 730](#)

## post\_login\_procedure-Option

Gibt eine Prozedur an, deren Ergebnismenge Meldungen enthält, die von Anwendungen angezeigt werden sollen, wenn ein Benutzer eine Verbindung herstellt.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

sa\_post\_login\_procedure-Systemprozedur

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Wenn die Option `post_login_procedure` auf etwas Anderes als eine leere Zeichenfolge gesetzt ist, können Anwendungen die Prozedur aufrufen, die von der Option als Teil des Verbindungsprozesses angegeben ist, um zu bestimmen, welche Meldungen ggf. dem Benutzer angezeigt werden. Die Option sollte im Format *Eigentümer.Funktionsname* sein, um zu verhindern, dass Benutzer die Funktion außer Kraft setzen.

Das SQL Anywhere 16-Plug-In für Sybase Central und Interactive SQL rufen die Prozedur auf, wenn diese Option gesetzt ist, und zeigen von der Prozedur zurückgegebene Meldungen in einem Fenster an. Andere Anwendungen, die nicht in SQL Anywhere enthalten sind, sollten angepasst werden, um die von dieser Option verfügbar gemachte Prozedur aufzurufen und Meldungen anzuzeigen, falls Sie diese Funktionalität benötigen.

Ein Fall, bei dem eine Anwendung möglicherweise eine Meldung bei Verbindungsherstellung anzeigen muss, wäre die Benachrichtigung an Benutzer, deren Kennwort abzulaufen droht, falls ein Kennwortablaufdatum implementiert ist. Diese Funktionalität kann verwendet werden, um den Benutzer bei jeder Verbindungsherstellung zu benachrichtigen, falls das Kennwort in den nächsten Tagen ablaufen wird, und dies, bevor es tatsächlich abläuft.

Die von dieser Option angegebene Prozedur muss eine Ergebnismenge mit einer oder mehreren Zeilen und zwei Spalten zurückgeben. Die erste Spalte vom Typ VARCHAR(255) gibt den Text der Meldung

oder NULL zurück, wenn es keine Meldung gibt. Die zweite Spalte vom Typ INT gibt den Aktionstyp zurück. Folgende Werte für Aktionen sind zulässig:

- **0** Die Meldung anzeigen (falls vorhanden)
- **1** Die Meldung anzeigen und den Benutzer zu einer Kennwortänderung auffordern
- **2-99** Reserviert
- **100 und höher** Benutzerdefiniert

Das SQL Anywhere 16-Plug-In und Interactive SQL (dbisql) zeigen alle Meldungen an, die nicht NULL sind, unabhängig vom Aktionswert. Wenn die Aktion auf 1 gesetzt ist, fordern diese Tools den Benutzer zur Änderung des Kennworts und zum Einstellen des neuen Kennworts auf den benutzerdefinierten Wert auf.

Ein Beispiel, das `post_login_procedure` verwendet und erweiterte Kennwortregeln enthält sowie ein Kennwortablaufdatum implementiert, finden Sie unter "Eine Kennwort-Überprüfungsfunktion verwenden".

### Siehe auch

- [„login\\_procedure-Option“ auf Seite 625](#)
- [„verify\\_password\\_function-Option“ auf Seite 704](#)
- [„Hinweise zur Sicherheit: Kennwörter“ auf Seite 1410](#)
- [„Verbindungsparameter NewPassword \(NEWPWD\)“ auf Seite 372](#)
- [„sa\\_post\\_login\\_procedure-Systemprozedur“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [post\\_login\\_procedure-Verbindungseigenschaft auf Seite 730](#)

### Beispiel

Das folgende Beispiel verwendet eine Prozedur mit Namen `p_post_login_check`, die Benutzer warnt, dass ihr Kennwort abzulaufen droht, und sie auffordert, das Kennwort zu ändern.

```
CREATE PROCEDURE DBA.p_post_login_check( )
RESULT( message_text VARCHAR(255), message_action INT )
BEGIN
    DECLARE message_text      CHAR(255);
    DECLARE message_action    INT;

    -- assume the password_about_to_expire variable was
    -- set by the login procedure
    IF password_about_to_expire = 1 THEN
        SET message_text = 'Your password is about to expire';
        SET message_action = 1;
    ELSE
        SET message_text = NULL;
        SET message_action = 0;
    END IF;
    -- return message (if any) through this result set
    SELECT message_text, message_action;
END;

GRANT EXECUTE ON DBA.p_post_login_check TO PUBLIC;

SET OPTION PUBLIC.post_login_procedure = 'DBA.p_post_login_check';
```

## precision-Option

Legt die maximale Anzahl von Stellen im Ergebnis aller dezimalen Berechnungen fest

### Zulässige Werte

Ganzzahl zwischen 1 und 127 (inklusive)

### Standardwert

30

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Gesamtstellen ist die Gesamtzahl aller Stellen links und rechts vom Dezimalzeichen. Die scale-Option legt die minimale Anzahl der Stellen nach dem Dezimalzeichen fest, wenn ein arithmetisches Ergebnis auf die maximalen Gesamtstellen gekürzt wird.

Multiplikation, Division, Addition, Subtraktion und Aggregatfunktionen können jeweils Ergebnisse haben, die die maximale Gesamtstellenzahl übersteigen.

Wenn zum Beispiel DECIMAL(8,2) mit DECIMAL(9,2) multipliziert wird, könnte das Ergebnis DECIMAL(17,4) erfordern. Wenn die Anzahl der Gesamtstellen (PRECISION) 15 ist, werden nur 15 Stellen im Ergebnis gehalten. Wenn die Dezimalstellenzahl (SCALE) 4 ist, lautet das Ergebnis DECIMAL(15,4). Wenn die Dezimalstellenzahl (SCALE) 2 ist, lautet das Ergebnis DECIMAL(15,2). In beiden Fällen ist ein Überlauf möglich.

### Siehe auch

- „scale-Option“ auf Seite 668
- „DECIMAL-Datentyp“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „NUMERIC-Datentyp“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- precision-Verbindungseigenschaft auf Seite 730
- scale-Verbindungseigenschaft auf Seite 735

## prefetch-Option

Steuert, ob Zeilen clientseitig abgerufen werden, bevor sie der Clientanwendung zur Verfügung gestellt werden.

### Zulässige Werte

Off, Conditional, Always

### Standardwert

Conditional

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Diese Option steuert, ob Zeilen clientseitig abgerufen werden, bevor sie Clientanwendungen zur Verfügung gestellt werden. Durch gleichzeitiges Abrufen mehrerer Zeilen, auch wenn die Zeilen von der Clientanwendung einzeln angefordert werden (wenn zum Beispiel die Zeilen eines Cursors in einer Schleife durchlaufen werden), können die Antwortzeiten verkürzt und der allgemeine Durchsatz verbessert werden, indem die Anzahl der Anforderungen an die Datenbank verringert wird.

- "Off" bedeutet, dass kein Prefetch-Vorgang ausgeführt wird.
- "Conditional" (Standardwert) bewirkt, dass ein Prefetch durchgeführt wird, es sei denn, der Cursortyp ist "SENSITIVE" oder die Abfrage enthält eine Proxytabelle.
- "Always" bedeutet, dass ein Prefetch-Vorgang auch bei sensitiven Cursortypen und für Cursor durchgeführt wird, die eine Proxytabelle betreffen.

Der Always-Wert muss mit Vorsicht verwendet werden, weil er sich auf einige Cursor-Semantiken auswirkt. So bewirkt er z.B., dass sensitive Corsoren asensitiv werden. Alte Werte werden möglicherweise abgerufen, wenn der Wert zwischen dem Prefetch und der Abrufanforderung der Anwendung aktualisiert wurde. Zusätzlich kann das Anwenden eines Prefetch mit einem Cursor, der einer Proxytabelle betrifft, den Fehler -668 ("Cursor ist beschränkt auf FETCH NEXT") bewirken, wenn der Client versucht, Prefetch-Zeilen erneut abzurufen. Ein Client versucht möglicherweise, Prefetch-Zeilen nach einer Zurücksetzung oder einem Abruf relativ 0 erneut abzurufen, wenn eine Abrufspalte erneut oder zum ersten Mal nach dem ersten Abruf gebunden wird, oder auch, wenn GET DATA verwendet wird.

Die wertempfindlichen Cursortypen umfassen die ESQL SENSITIVE - und SCROLL-Cursortypen, sowie die ODBC-, OLE DB DYNAMIC- und KEYSET-Cursortypen.

Die Einstellung der prefetch-Option wird von Sybase Open Client- und jConnect-Verbindungen ignoriert.

Wenn der DisableMultiRowFetch-Verbindungsparameter auf YES eingestellt ist, wird die prefetch-Datenbankoption ignoriert und kein Prefetch durchgeführt.

Diese Option hat früher den Wert "On" angenommen. Dieser Wert ist jetzt ein Aliasname für "Conditional".

### Siehe auch

- „Prefetch“ [[SQL Anywhere Server - Programmierung](#)]
- „Verbindungsparameter DisableMultiRowFetch (DMRF)“ auf Seite 357
- prefetch-Verbindungseigenschaft auf Seite 730

## preserve\_source\_format-Option

Steuert, ob die Original-Quellendefinition von Prozeduren, Triggern, Ansichten und Event-Handlern in Systemdateien gespeichert werden. Beim Speichern wird sie in der Spalte "source" in SYSTAB, SYSPROCEDURE, SYSTRIGGER und SYSEVENT registriert.

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Wenn preserve\_source\_format auf "On" gesetzt wurde, speichert der Datenbankserver die formatierte Quelle von CREATE- und ALTER-Anweisungen auf Prozeduren, Ansichten, Triggern und Events, und platziert sie in die source-Spalte der entsprechenden Systemansicht.

Unformatierter Quelltext wird in denselben Systemtabellen gespeichert, und zwar in den Spalten proc\_defn, trigger\_defn und view\_defn. Allerdings sind diese Definitionen in Sybase Central nicht einfach zu lesen. In der formatierten source-Spalte können Sie die Definitionen mit den von Ihnen gewünschten Leerstellen, Kommentaren und Groß-/Kleinschreibung prüfen.

Diese Option kann ausgeschaltet werden, um den Platzbedarf zum Speichern von Objektdefinitionen in der Datenbank zu vermindern. Die Option kann nur für die PUBLIC-Rolle gesetzt werden.

### Siehe auch

- [preserve\\_source\\_format-Verbindungseigenschaft auf Seite 730](#)

## prevent\_article\_pkey\_update-Option

Verwaltet die Updates von Primärschlüsselspalten der Tabellen, die in MobiLink-Publikationen einbezogen sind.

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn Sie diesen Parameter auf "On" setzen, werden keine Updates auf Primärschlüsselspalten von Tabellen erlaubt, die Teil einer Publikation sind. Dadurch wird die Einhaltung der Datenintegrität gewährleistet, vor allem in einer Replikations- und Synchronisationsumgebung.

#### Vorsicht

Es wird dringend empfohlen, dass Sie diese Option in einer Synchronisations- oder Replikationsumgebung nicht auf "Off" setzen.

### Siehe auch

- [prevent\\_article\\_pkey\\_update-Verbindungseigenschaft auf Seite 730](#)

## priority-Option

Legt die Prioritätsstufe fest, in der Anforderungen einer Verbindung ausgeführt werden.

### Zulässige Werte

Critical, High, Above Normal, Normal, Below Normal, Low, Background

### Standardwert

Normal

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

Wenn Sie diese Option temporär setzen, gilt die Einstellung nur für die aktuelle Verbindung. Unterschiedliche Verbindungen mit derselben Benutzer-ID haben unterschiedliche Einstellungen für diese Option.

### Bemerkungen

Der Wert dieser Option kann nicht höher als der Wert der Option max\_priority eingestellt werden.

### Siehe auch

- [„max\\_priority-Option“ auf Seite 632](#)
- [priority-Verbindungseigenschaft auf Seite 730](#)
- [„Tipp: Ressourcenwächter verwenden“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)

## progress\_messages-Option

Diese Option steuert, ob Meldungen zum Verarbeitungsfortschritt vom Datenbankserver zum Client gesendet werden.

### Zulässige Werte

- **Off** Meldungen zum Verarbeitungsfortschritt werden nicht an den Client gesendet.
- **RAW** Wenn RAW (unformatiert) ausgewählt ist, wird folgendes Format für Meldungen zum Verarbeitungsfortschritt verwendet:

```
43;9728;22230;pages;5025;6138
```

Unformatierte Meldungen zum Verarbeitungsfortschritt haben sechs durch Semikola getrennte Felder, die wie folgt definiert sind:

- **Feld 1** Der Prozentsatz der ausgeführten Anweisung.
- **Feld 2** Die Anzahl der abgeschlossenen Seiten, Zeilen oder Byte.
- **Feld 3** Die Anzahl der zu verarbeitenden Seiten, Zeilen oder Byte.
- **Feld 4** Gegenstand der Verarbeitung: Seiten, Zeilen oder Byte.
- **Feld 5** Die aktuell verstrichene Zeit, angezeigt in Millisekunden.
- **Feld 6** Die geschätzte verbleibende Zeit für den Abschluss der Ausführung der Anweisung in Millisekunden.
- **Formatted** Wenn "Formatted" ausgewählt ist, wird folgendes Format für Meldungen zum Verarbeitungsfortschritt verwendet:

```
43 % (9728 von 22230 Seiten) fertig nach 00:00:05; geschätzte 00:00:06  
verbleiben
```

Formatierte Meldungen zum Verarbeitungsfortschritt werden lokalisiert und das Zeitformat ist HH:MM:SS. Einheiten unter 100 KB werden in Byte, Einheiten unter 100 MB in Kilobyte und Einheiten über 100 MB in MByte angezeigt.

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Meldungen zum Verarbeitungsfortschritt werden in Intervallen gesendet, die 5% der geschätzten Gesamtdauer für die Ausführung der Anweisung betragen. In der Regel wird die Schätzung eingehalten

und die erste Meldung zum Verarbeitungsfortschritt wird innerhalb von 10 Sekunden gesendet. Weitere Meldungen zum Verarbeitungsfortschritt werden in Intervallen von 30 Sekunden bis 5 Minuten gesendet. Wenn der Prozentwert für den Verarbeitungsfortschritt mit dem in einer vorherigen Meldung gesendeten Wert identisch ist, wird eine aktualisierte Fortschrittsmeldung erst nach Verstreichen von mehr als 5 Minuten seit dem Senden der letzten Meldung gesendet. Meldungen zum Verarbeitungsfortschritt werden für Anweisungen, die weniger als 30 Sekunden für die Ausführung benötigen, nicht gesendet.

Die Schätzungen werden ständig neu berechnet. Die Genauigkeit der Schätzung für die verbleibende Zeit steigt mit Fortschreiten des Vorgangs. Während Ereignissen wie etwa Sicherungen wird während der Anweisungsausführung die Gesamtzahl der Seiten möglicherweise angepasst, sodass sich der Prozentwert für den Verarbeitungsfortschritt und die Schätzungen für die verbleibende Zeit ändern können. Bei Anweisungen wie BACKUP ... WITH CHECKPOINT COPY oder UNLOAD SELECT ist die Gesamtzahl der betroffenen Seiten oder Zeilen unbekannt und es ist möglich, dass der Prozentwert für den Verarbeitungsfortschritt mit über 100 % angegeben wird. Dies führt dazu, dass die geschätzte verbleibende Zeit nicht berechnet werden kann und in der Meldung zum Verarbeitungsfortschritt nicht angegeben wird.

Die folgenden Anweisungen und Prozeduren unterstützen Meldungen zum Verarbeitungsfortschritt:

- BACKUP DATABASE (sowohl Bild als auch Archiv)
- LOAD TABLE (nur USING FILE und USING CLIENT FILE)
- MESSAGE
- REORGANIZE TABLE
- RESTORE DATABASE
- UNLOAD (alle Typen)
- sa\_table\_page\_usage-Systemprozedur

Sie können die progress\_messages-Option setzen, indem Sie die SET TEMPORARY OPTION-Anweisung verwenden, wenn Sie mit der Dienstprogrammdatenbank verbunden sind. Siehe „[SET OPTION-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*] und [Zulässige Anweisungen für die Dienstprogrammdatenbank auf Seite 146](#).

Sie können die progress\_messages-Option auch in Interactive SQL setzen, indem Sie auf **Extras » Optionen » SQL Anywhere » Befehle** und anschließend auf **Fortschrittsmeldungen anzeigen** klicken. Wenn die Option **Fortschrittsmeldungen anzeigen** aktiviert ist, wird die progress\_messages-Option auf "Formatted" eingestellt.

### Siehe auch

- „[Sicherungsdienstprogramm \(dbbackup\)](#)“ auf Seite 886
- [Progress-Verbindungseigenschaft](#) auf Seite 731
- „[sa\\_table\\_page\\_usage-Systemprozedur](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## qualify\_owners-Option [SQL Remote]

Steuert, ob SQL-Anweisungen, die von SQL Remote repliziert werden, als Objektnamen qualifiziert werden sollen.

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bemerkungen**

Wenn in SQL Anywhere-Installationen keine Qualifikation erforderlich ist und diese Option auf "Off" gesetzt wird, sind Nachrichten etwas kleiner.

**Siehe auch**

- „SQL Remote-Optionen“ [[SQL Remote](#)]

## query\_mem\_timeout-Option

Legt in Millisekunden die Zeitspanne fest, die eine Abfrage maximal auf Speicherzuteilung abwartet.

**Zulässige Werte**

-1, 0, positive Ganzzahl

**Standardwert**

-1

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Wenn diese Option auf -1 (Standardwert) oder einen Wert unter 0 eingestellt ist, wartet die Abfrage bis zu 50 mal die für die Abfrage geschätzte Ausführungszeit auf die Speicherzuteilung. Wenn diese Option auf 0 eingestellt ist, wartet die Abfrage ewig auf Speicherzuteilung. Sonst ist der Wert die Anzahl der Millisekunden, die eine Abfrage maximal auf Speicherzuteilung wartet.

**Siehe auch**

- „Cache und der Speichernutzungswächter“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- [query\\_mem\\_timeout-Verbindungseigenschaft](#) auf Seite 731

## quote\_all\_identifiers-Option [SQL Remote]

Steuert, ob SQL-Anweisungen, die von SQL Remote repliziert werden, Bezeichner zwischen Anführungszeichen stellen sollen.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bemerkungen

Wenn diese Option ausgeschaltet ist, setzt dbremote Bezeichner in Anführungszeichen, wenn SQL Anywhere Anführungszeichen verlangt (so wie dies bisher der Fall war).

Wenn die Option aktiviert ist, werden alle Bezeichner in Anführungszeichen gesetzt.

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]

## quoted\_identifier-Option

Steuert die Interpretation von Zeichenfolgen, die in Anführungszeichen eingeschlossen sind

### Zulässige Werte

On, Off

### Standardwert

On

Off für Sybase Open Client- und jConnect-Verbindungen

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option steuert, ob in Anführungszeichen eingeschlossene Zeichenfolgen als Bezeichner (On) oder als Literal-Zeichenfolgen (Off) interpretiert werden. Die quoted\_identifier-Option ist für die Transact-SQL-Kompatibilität miteingeschlossen.

Siehe „Optionen für die Transact-SQL-Kompatibilität“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].

### Siehe auch

- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET-Anweisung [T-SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- quoted\_identifier-Verbindungseigenschaft auf Seite 732

## read\_past\_deleted-Option

Steuert das Verhalten des Datenbankservers bei nicht festgeschriebenen Löschungen auf Isolationsstufe 1 und 2.

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn read\_past\_deleted auf "On" gesetzt ist (Standard), überspringen sequenzielle Scans auf Isolationsstufe 1 und 2 nicht festgeschriebene gelöschte Zeilen. Wenn "Off" gesetzt wurde, blockieren sequenzielle Scans bei nicht festgeschriebenen gelöschten Zeilen auf Isolationsstufe 1 und 2 (bis die löschende Transaktionen festgeschrieben oder zurückgesetzt wird). Diese Option ändert das Serververhalten auf Isolationsstufe 1 und 2.

Für die meisten Zwecke muss diese Option auf "On" gesetzt bleiben. Wenn die Option auf "Off" gesetzt ist, hängt das Blockierungsverhalten vom Plan ab, den der Optimierer gewählt hat (wenn ein Index vorhanden ist, der eventuell verwendet werden könnte).

### Siehe auch

- „Isolationsstufen und Konsistenz“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- [read\\_past\\_deleted-Verbindungseigenschaft auf Seite 733](#)

## recovery\_time-Option

Legt die maximale Zeitdauer in Minuten fest, die dem Datenbankserver zum Wiederherstellen nach einem Systemausfall zur Verfügung steht

### Zulässige Werte

Ganzzahl in Minuten

### Standardwert

2

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Tritt in Kraft, wenn der Datenbankserver neu gestartet wird.

### Bemerkungen

Diese Option wird mit der Option `checkpoint_time` verwendet, mit deren Hilfe entschieden wird, wann Checkpoints gesetzt werden sollen.

SQL Anywhere verwendet zum Ermitteln der Wiederherstellungszeit eine Heuristik, die auf den seit dem letzten Checkpoint ausgeführten Vorgängen basiert. Der Wert enthält sowohl die geschätzte Wiederherstellungszeit als auch die geschätzte Checkpoint-Zeit der Datenbank. Deshalb ist die Wiederherstellungszeit ungenau.

### Siehe auch

- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „`checkpoint_time`-Option“ auf Seite 588
- „Datenbankserveroption -gr“ auf Seite 249
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077
- `recovery_time`-Verbindungseigenschaft auf Seite 733

## remote\_idle\_timeout-Option

Steuert, wie viele Inaktivitätssekunden von Webdienst-Clientprozeduren und -funktionen toleriert werden.

### Zulässige Werte

Ganzzahl in Sekunden

### Standardwert

15

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option wirkt sich auf Webdienst-Clientprozeduren und -funktionen aus. Wenn mehr Zeit als die angegebene Anzahl von Sekunden ohne Aktivität verstreicht, tritt für die Prozedur oder Funktion eine Zeitüberschreitung ein.

### Siehe auch

- „Webclient-Anwendungsentwicklung“ [*SQL Anywhere Server - Programmierung*]
- `remote_idle_timeout`-Verbindungseigenschaft auf Seite 733
- „CREATE PROCEDURE-Anweisung [Webdienste]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE FUNCTION-Anweisung [Webdienst]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## replication\_error-Option [SQL Remote]

Ermöglicht es Ihnen, eine gespeicherte Prozedur anzugeben, die vom Nachrichtenagenten beim Auftreten eines SQL-Fehlers aufgerufen wird.

### Zulässige Werte

Name der gespeicherten Prozedur

### Standardwert

(Keine Prozedur)

### Bemerkungen

Bei SQL Remote ermöglicht Ihnen die Option `replication_error` die Angabe einer gespeicherten Prozedur, die vom Nachrichtenagenten beim Auftreten eines SQL-Fehlers aufgerufen wird. Standardmäßig wird keine Prozedur aufgerufen.

Die Prozedur muss ein einzelnes Argument vom Typ `CHAR`, `VARCHAR` oder `LONG VARCHAR` enthalten. Die Prozedur wird einmal mit der SQL-Fehlernachricht und ein zweites Mal mit der SQL-Anweisung aufgerufen, die den Fehler bewirkt. Unter bestimmten Umständen (wie Fremdschlüsselverstöße) ist die SQL-Anweisung, die den Fehler verursachte, nicht verfügbar, wodurch die gespeicherte Prozedur nur einmal aufgerufen werden kann.

Obwohl Sie mit der Option `SQL-Fehler` in Replikationen verfolgen und überwachen können, müssen Sie die Fehler trotzdem aus Ihrem Setup entfernen. Diese Option kann solche Fehler nicht beseitigen.

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „`replication_error_piece`-Option [SQL Remote]“ auf Seite 663
- „Fehlerbehandlungsprozeduren für die Replikation“ [[SQL Remote](#)]

## replication\_error\_piece-Option [SQL Remote]

Ermöglicht es Ihnen zusammen mit der `replication_error`-Option, eine gespeicherte `LONG VARCHAR`-Prozedur anzugeben, die vom Nachrichtenagenten aufgerufen wird, wenn während der SQL Remote-Replikation ein SQL-Fehler auftritt.

### Zulässige Werte

Name der gespeicherten Prozedur

### Standardwert

(Keine Prozedur)

### Bemerkungen

Wenn ein Fehler auftritt und `replication_error` definiert ist, wird die `replication_error`-Prozedur mit dem kompletten Fehlertext aufgerufen.

Wenn `replication_error` und `replication_error_piece` definiert sind, wird der Fehler in VARCHAR-Teile aufgeteilt. `replication_error` wird mit dem ersten Teil aufgerufen und `replication_error_piece` wird wiederholt mit den verbleibenden Teilen aufgerufen.

### Siehe auch

- „`replication_error`-Option [SQL Remote]“ auf Seite 663
- „SQL Remote-Optionen“ [SQL Remote]

## request\_timeout-Option

Steuert die maximale Zeit, die eine einzelne Anforderung benötigen darf. Diese Option kann verhindern, dass eine Verbindung eine signifikante Menge an Serverressourcen über eine längere Zeitspanne hinweg verbraucht.

### Zulässige Werte

Ganzzahl von 0 bis 86400 (ein Tag), in Sekunden

### Standardwert

0

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn diese Option auf "0" gesetzt ist, gibt es kein Zeitlimit.

Eine Anforderung, die länger als ungefähr `request_timeout`-Sekunden (Uhrzeit, nicht CPU-Zeit) dauert, wird unterbrochen, und ein Fehler wird an den Benutzer zurückgegeben. Der zurückgegebene Fehler ist `SQL*REQUEST_TIMEOUT`: "Anforderung wegen Zeitüberschreitung unterbrochen". Wenn eine Anforderung blockiert und die Option `blocking_timeout` auf "0" gesetzt ist, kann die Anforderung bis zu einem Maximum von `request_timeout`-Sekunden blockiert bleiben, bis ein Blockierungsfehler zurückgegeben wird (z.B. `SQL*LOCKED`: "Benutzer '%1' hat die Zeilen in '%2' gesperrt").

Werte im Bereich von 1 bis 14 können nicht als Benutzeroption oder PUBLIC-Option, jedoch als temporäre Option angegeben werden. Dies verhindert, dass Benutzer keinen Zugriff auf den Datenbankserver erhalten, falls die Verbindungsherstellung lange braucht (z.B. aufgrund einer komplexen Login-Prozedur).

Diese Option kann mit Datenbank-Client- und HTTP/HTTPS-Anforderungen verwendet werden. Das Setzen der Option in einer gespeicherten Prozedur oder einer HTTP/HTTPS-Anforderung hat keine Auswirkung auf die aktuelle Anforderung, da der Optionswert am Anfang der Anforderung verwendet wird.

Ein Setzen der öffentlichen Option `request_timeout` sollte mit Umsicht getan werden, da dies bewirken kann, dass Anwendungen mit lange ausführenden Anforderungen (wie `dbvalid`, `dbbackup` und `dbunload`)

fehlschlagen. Auch können Anwendungen, die keine signifikanten Serverressourcen verbrauchen, aber andere Benutzer blockieren, fehlschlagen, wenn `request_timeout` gesetzt ist. Eine Möglichkeit, diese Probleme zu umgehen, wäre, die Option `request_timeout` nur für bestimmte Anwendungen in der Login-Prozedur zu setzen, basierend auf dem `APPINFO`-Wert der Verbindung.

Ein Setzen dieser Option verhindert möglicherweise nicht, dass Anwendungen signifikante Serverressourcen verbrauchen, deren einzelne Anforderungen schnell ausgewertet werden, z.B. wenn ein Ergebnis mit vielen Zeilen abgerufen wird.

**Siehe auch**

- [„blocking\\_timeout-Option“ auf Seite 587](#)
- [„Verbindungsparameter AppInfo \(APP\)“ auf Seite 338](#)
- [request\\_timeout-Verbindungseigenschaft auf Seite 735](#)

## reserved\_keywords-Option

Aktiviert einzelne Schlüsselwörter, die standardmäßig deaktiviert sind.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Leere Zeichenfolge

**Bereich**

Kann nur für `PUBLIC` gesetzt werden. Sie müssen das `SET ANY SYSTEM OPTION`-Systemprivileg haben, um diese Option setzen zu können.

**Bemerkungen**

Benutzer und temporäre Einstellungen sind nicht zulässig.

Diese Option aktiviert einzelne Schlüsselwörter, die standardmäßig deaktiviert sind. Nur das Schlüsselwort `LIMIT` kann aktiviert werden.

Die folgende Anweisung ermöglicht, dass das Schlüsselwort `LIMIT` als Schlüsselwort erkannt wird:

```
SET OPTION PUBLIC.reserved_keywords = 'LIMIT';
```

Es ist nicht möglich, die Anweisungen `set`, `option` und `options` als Schlüsselwörter zu aktivieren. Ob ein Wort als Schlüsselwort identifiziert wird, hängt von folgenden Faktoren ab (in der genannten Reihenfolge):

- Es ist in der SQL Anywhere-Liste der reservierten Wörter enthalten.
- Es wurde mit der `reserved_keywords`-Option aktiviert.
- Es wurde mithilfe der `non_keywords`-Option deaktiviert.

Jede neue Einstellung dieser Option ersetzt die frühere Einstellung. Die folgende Anweisung löscht alle früheren Einstellungen.

```
SET OPTION PUBLIC.reserved_keywords =;
```

Sie können einzelne Schlüsselwörter mithilfe der Option `non_keywords` deaktivieren.

### Siehe auch

- „`non_keywords`-Option“ auf Seite 641
- „Schlüsselwörter“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Reservierte Wörter“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## return\_date\_time\_as\_string-Option

Steuert, wie ein DATE-, TIME- oder TIMESTAMP-Wert bei einer Abfrage an die Clientanwendung übergeben wird.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option gibt an, ob DATE-, TIME- und TIMESTAMP-Werte als DATE-, TIME- oder TIMESTAMP-Datentyp oder als Zeichenfolge an Anwendungen zurückgegeben werden.

Wenn diese Option auf "On" gesetzt ist, konvertiert der Datenbankserver den DATE-, TIME- oder TIMESTAMP-Wert vor dem Senden an den Client in eine Zeichenfolge, sodass die Einstellung der Option `timestamp_format`, `date_format` bzw. `time_format` erhalten bleibt.

Sybase Central und Interactive SQL setzen die Option `return_date_time_as_string` automatisch auf "On".

### Siehe auch

- „`date_format`-Option“ auf Seite 599
- „`time_format`-Option“ auf Seite 690
- „`timestamp_format`-Option“ auf Seite 692
- „`timestamp_with_time_zone_format`-Option“ auf Seite 694
- `return_date_time_as_string`-Verbindungseigenschaft auf Seite 735

## rollback\_on\_deadlock-Option

Steuert, wie Transaktionen behandelt werden, wenn ein Deadlock auftritt

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn diese Option auf "On" eingestellt ist, wird eine Transaktion automatisch zurückgesetzt, wenn sie auf ein Deadlock stößt. Die Zurücksetzung findet statt, nachdem die aktuelle Anforderung abgeschlossen ist. Wenn diese Option auf "Off" eingestellt ist, setzt SQL Anywhere die Anweisung, die auf einen Deadlock gestoßen ist, automatisch zurück und gibt dieser Transaktion einen Fehler zurück, der angibt, welche Art von Deadlock aufgetreten ist. Beim Zurücksetzen der Anweisung würde wahrscheinlich keine der Sperren freigegeben, die die Anweisung gesetzt hat.

**Siehe auch**

- „Deadlocks“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- [rollback\\_on\\_deadlock-Verbindungseigenschaft auf Seite 735](#)

## row\_counts-Option

Legt fest, ob die Datenbank beim Öffnen immer die Anzahl der Zeilen in einer Abfrage zählen soll.

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Wenn die Option auf "Off" gesetzt ist, wird die Zeilenanzahl normalerweise nur geschätzt. Wenn die Option auf "On" gesetzt ist, stimmt die Zeilenanzahl immer genau.

**Vorsicht**

Wenn row\_counts auf "On" gesetzt ist, kann die Ausführung von Abfragen wesentlich mehr Zeit in Anspruch nehmen. Normalerweise bewirkt diese Einstellung sogar, dass SQL Anywhere die Abfrage zweimal ausführt und sich dadurch die Ausführungszeit verdoppelt.

**Siehe auch**

- C-API: [sqlany\\_num\\_rows-Methode \[SQL Anywhere C\] \[SQL Anywhere Server - Programmierung\]](#)
- PHP API: „[sasql\\_num\\_rows](#)“ [\[SQL Anywhere Server - Programmierung\]](#)
- [row\\_counts-Verbindungseigenschaft auf Seite 735](#)

## save\_remote\_passwords-Option [SQL Remote]

Speichert das Kennwort, das in die Nachrichtenverbindung eingegeben wird

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bemerkungen**

Wenn Sie die Nachrichtenverbindungsparameter extern und nicht in der Datenbank speichern, ist ein Speichern der Kennwörter nicht zu empfehlen. Sie können verhindern, dass die Kennwörter gespeichert werden, indem Sie diese Option auf "Off" setzen.

**Siehe auch**

- „[SQL Remote-Optionen](#)“ [\[SQL Remote\]](#)

## scale-Option

Legt die Mindestanzahl der Stellen nach dem Dezimalzeichen fest, wenn ein arithmetisches Ergebnis auf die maximale Gesamtstellenanzahl gekürzt wird

**Zulässige Werte**

Ganzzahl zwischen 0 und 127 (inklusive), die kleiner ist als der für die Datenbankoption precision angegebene Wert

**Standardwert**

6

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

**Bemerkungen**

Multiplikation, Division, Addition, Subtraktion und Aggregatfunktionen können jeweils Ergebnisse haben, die die maximale Gesamtstellenzahl übersteigen.

**Siehe auch**

- [„precision-Option“ auf Seite 653](#)
- [scale-Verbindungseigenschaft auf Seite 735](#)
- [precision-Verbindungseigenschaft auf Seite 730](#)

**secure\_feature\_key-Option (nicht mehr empfohlen)**

Ermöglicht es Ihnen, Funktionen für die Verbindung zu aktivieren, die mit der Datenbankserveroption -sf gesichert wurden.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

NULL

**Bereich**

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung eingestellt werden

**Bemerkungen**

Sie können Funktionen angeben, die nicht von auf einem Server laufenden Datenbanken verwendet werden können, indem Sie beim Starten des Datenbankservers die Option -sf verwenden. Mit der Serveroption -sk können Sie einen Schlüssel angeben, mit dem alle gesicherten (deaktivierten) Funktionen für eine Verbindung wieder aktiviert werden und die Verbindung die Berechtigung erhält, die Funktionen zu ändern, die für alle auf dem Datenbankserver laufenden Datenbanken gesichert sind. Wenn Sie den Wert der temporären Option secure\_feature\_key auf den von -sk angegebenen Wert beim Starten des Datenbankservers setzen, werden für diese Datenbankverbindung alle Funktionen wieder aktiviert und Sie können auf dieser Verbindung die sa\_server\_option-Systemprozedur verwenden, um den Zugriff auf Datenbankfunktionen zu steuern.

Wenn die secure\_feature\_key-Option auf einen anderen als den durch -sk angegebenen Wert gesetzt ist, wird kein Fehler ausgegeben und die durch die Datenbankserveroption -sf angegebenen Funktionen bleiben für die Verbindung deaktiviert.

### Siehe auch

- „sp\_use\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -sk “ auf Seite 288
- „Datenbankserveroption -sf “ auf Seite 280
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415

### Beispiel

Der folgende Befehl startet einen Datenbankserver namens secure\_server, bei dem der Zugriff auf das Anforderungslog und alle Ferndatenzugriffsfunktionen deaktiviert sind. Der von der Option -sk angegebene Schlüssel kann später verwendet werden, um diese Funktionen bei einer bestimmten Datenbank wieder zu aktivieren.

```
dbsrv16 -n secure_server -sf request_log,remote -sk j978kls12 testdb.db
```

Das Setzen der Option secure\_feature\_key auf den Wert, der von -sk für eine Datenbank angegeben wird, die auf dem Datenbankserver secure\_server läuft, aktiviert bei dieser Verbindung den Zugriff auf das Anforderungslog und Ferndaten-Zugriffsfunktionen:

```
SET TEMPORARY OPTION secure_feature_key = 'j978kls12';
```

## sort\_collation-Option

Ermöglicht die implizite Verwendung der SORTKEY-Funktion für ORDER BY-Ausdrücke

### Zulässige Werte

Internal, collation\_name oder collation\_id

### Standardwert

Internal

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn der Wert dieser Option "Internal" ist, bleibt die ORDER BY-Klausel unverändert.

Wenn die Option auf gültige Werte für Kollationsnamen oder Kollations-ID gesetzt ist, wird jeder CHAR- oder NCHAR-Zeichenfolgenausdruck in der ORDER BY-Klausel so behandelt, als wäre die Funktion SORTKEY aufgerufen worden. Zeichenfolgenausdrücke, die andere Zeichenfolgendatentypen, zum Beispiel BINARY, UUID, XML oder VARBIT, verwenden, werden nicht verändert.

**Siehe auch**

- „SORTKEY-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `sort_collation`-Verbindungseigenschaft auf Seite 736

**Beispiel**

Kollation auf "binary" setzen:

```
SET TEMPORARY OPTION sort_collation='binary';
```

Wenn die Kollation auf "binary" gesetzt wurde, werden die folgenden Abfragen umgewandelt:

```
SELECT Name, ID
FROM Products
ORDER BY Name, ID;
SELECT name, ID
FROM Products
ORDER BY 1, 2;
```

Die Abfragen werden folgendermaßen umgewandelt:

```
SELECT Name, ID
FROM Products
ORDER BY SORTKEY(Name, 'binary'), ID;
```

**sql\_flagger\_error\_level-Option**

Steuert die Antwort auf jeden SQL-Code, der nicht Teil des angegebenen Standards ist

**Zulässige Werte**

- Off
- SQL:1992/Entry
- SQL:1992/Intermediate
- SQL:1992/Full
- SQL:1999/Core
- SQL:1999/Package
- SQL:2003/Core
- SQL:2003/Package
- SQL:2008/Core
- SQL:2008/Package
- UltraLite

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Diese Option kennzeichnet SQL-Code, der nicht Teil eines bestimmten Standards ist, als Warnung.  
Beispiel: Die Angabe von "SQL:2003/Package" bewirkt, dass der Datenbankserver Syntax kennzeichnet, bei der es sich nicht um reine SQL/2003-Syntax handelt.

Das Standardverhalten ("Off") schaltet die Fehlerkennzeichnung aus.

Aus Gründen der Kompatibilität mit früheren SQL Anywhere-Versionen werden die folgenden Werte ebenfalls akzeptiert:

- **E** Diese Option entspricht "SQL:1992/Entry".
- **I** Diese Option entspricht "SQL:1992/Intermediate".
- **F** Diese Option entspricht "SQL:1992/Full".
- **W** Diese Option entspricht "Off".

### Siehe auch

- „sa\_ansi\_standard\_packages-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQLFLAGGER-Funktion [Verschiedene]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sql\_flagger\_warning\_level-Option“ auf Seite 672
- „Der SQL-Präprozessor“ [*SQL Anywhere Server - Programmierung*]
- „Kompatibilitätsoptionen“ auf Seite 559
- sql\_flagger\_error\_level-Verbindungseigenschaft auf Seite 737

## sql\_flagger\_warning\_level-Option

Steuert die Antwort auf jeden SQL-Code, der nicht Teil des angegebenen Standards ist

### Zulässige Werte

- Off
- SQL:1992/Entry
- SQL:1992/Intermediate
- SQL:1992/Full
- SQL:1999/Core
- SQL:1999/Package
- SQL:2003/Core
- SQL:2003/Package
- SQL:2008/Core
- SQL:2008/Package
- UltraLite

### Standardwert

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Diese Option kennzeichnet SQL-Code, der nicht Teil eines bestimmten Standards ist, als Warnung. Beispiel: Die Angabe von "SQL:2003/Package" bewirkt, dass der Datenbankserver Syntax kennzeichnet, bei der es sich nicht um reine SQL/2003-Syntax handelt.

Das Standardverhalten ("Off") schaltet die Warnungskennzeichnung aus.

Aus Gründen der Kompatibilität mit früheren Versionen werden die folgenden Werte ebenfalls akzeptiert:

- **E** Diese Option entspricht "SQL:1992/Entry".
- **I** Diese Option entspricht "SQL:1992/Intermediate".
- **F** Diese Option entspricht "SQL:1992/Full".
- **W** Diese Option entspricht "Off".

**Siehe auch**

- „sa\_ansi\_standard\_packages-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SQLFLAGGER-Funktion [Verschiedene]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sql\_flagger\_error\_level-Option“ auf Seite 671
- „Der SQL-Präprozessor“ [[SQL Anywhere Server - Programmierung](#)]
- „Kompatibilitätsoptionen“ auf Seite 559
- sql\_flagger\_warning\_level-Verbindungseigenschaft auf Seite 737

**sr\_date\_format-Option [SQL Remote]**

Legt das Format für aus der Datenbank abgerufene DATE-Werte fest.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

YYYY-MM-DD

**Bemerkungen**

Der Nachrichtenagent verwendet diese Option, wenn Spalten repliziert werden, die ein Datum speichern. Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig
MMM[m...]	Zeichenkurzform für Monate: so viele Zeichen wie "m"
DD	Tag des Monats zweistellig

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.
- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein.  
Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "MMM" gibt beispielsweise eine Länge von drei Zeichen für den Monat an.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

Diese Option ist eine Zeichenfolge, die aus folgenden Symbolen aufgebaut ist:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.

### Siehe auch

- „sr\_time\_format-Option [SQL Remote]“ auf Seite 675
- „sr\_timestamp\_format-Option [SQL Remote]“ auf Seite 676
- „sr\_timestamp\_with\_time\_zone\_format-Option [SQL Remote]“ auf Seite 677
- „SQL Remote-Optionen“ [SQL Remote]

## sr\_time\_format-Option [SQL Remote]

Legt das Format für aus der Datenbank abgerufene TIME-Werte fest.

### Zulässige Werte

Zeichenfolge

### Standardwert

HH:NN:SS.ssssss

### Bemerkungen

Der Nachrichtenagent verwendet diese Option, wenn Spalten repliziert werden, die eine Uhrzeit speichern. Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
HH	Stunden zweistellig (24-Stunden-Angabe)
NN	Minuten zweistellig
MM	Minuten zweistellig, falls nach einem Doppelpunkt (z.B. HH:MM)
SS.ssssss	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.

Jedes Symbol wird durch die entsprechenden Daten für die Uhrzeit ersetzt, die formatiert wird.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Groß- und Kleinschreibung (z.B. NN oder nn) ein, um das Auffüllen mit Nullen zuzulassen. Beispiel: hh:nn:ss.sss kann 02:34:56.123 ergeben.
- Geben Sie das Symbol in gemischter Groß- und Kleinschreibung (z.B. Mm) ein, um das Auffüllen mit Nullen zu unterdrücken. Beispiel: Hh:nn:ss.sss kann 2:34:56.123 ergeben.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSsss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

### Bemerkungen

Führende Nullen werden durch gemischte Schreibweise in der Formatzeichenfolge unterdrückt.

**Siehe auch**

- „sr\_date\_format-Option [SQL Remote]“ auf Seite 673
- „sr\_timestamp\_format-Option [SQL Remote]“ auf Seite 676
- „sr\_timestamp\_with\_time\_zone\_format-Option [SQL Remote]“ auf Seite 677
- „SQL Remote-Optionen“ [*SQL Remote*]

**sr\_timestamp\_format-Option [SQL Remote]**

Legt das Format für aus der Datenbank abgerufene TIMESTAMP-Werte fest.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

YYYY-MM-DD HH:NN:SS.ssssss

**Bemerkungen**

Der Nachrichtenagent verwendet diese Option, um DATETIME- und TIMESTAMP-Informationen zu replizieren.

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig bzw. Minuten zweistellig, falls nach einem Doppelpunkt (z.B. HH:MM)
MMM[m...]	Zeichenkurzform für Monate: so viele Zeichen wie "m"
DD	Tag des Monats zweistellig
DDD[d...]	Zeichenkurzform für Wochentag
HH	Stunden zweistellig
NN	Minuten zweistellig
SS.ssssss	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.
AA	A.M. oder P.M. (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen

Symbol	Beschreibung
PP	P.M. falls nötig (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.
- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein.  
Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "MMM" gibt beispielsweise eine Länge von drei Zeichen für den Monat an.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSsss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

#### Siehe auch

- „sr\_date\_format-Option [SQL Remote]“ auf Seite 673
- „sr\_time\_format-Option [SQL Remote]“ auf Seite 675
- „sr\_timestamp\_with\_time\_zone\_format-Option [SQL Remote]“ auf Seite 677
- „SQL Remote-Optionen“ [SQL Remote]

## sr\_timestamp\_with\_time\_zone\_format-Option [SQL Remote]

Legt das Format für aus der Datenbank abgerufene TIMESTAMP WITH TIME ZONE-Werte fest.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

YYYY-MM-DD HH:NN:SS.ssssss +HH:NN

**Bemerkungen**

Der Nachrichtenagent verwendet diese Option, um TIMESTAMP WITH TIME ZONE-Informationen zu replizieren.

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig bzw. Minuten zweistellig, falls nach einem Doppelpunkt (z.B. HH:MM)
MMM[m...]	Zeichenkurzform für Monate: so viele Zeichen wie "m"
DD	Tag des Monats zweistellig
DDD[d...]	Zeichenkurzform für Wochentag
HH	Stunden zweistellig
NN	Minuten zweistellig
SS.ssssss	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.
AA	A.M. oder P.M. (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen
PP	P.M. falls nötig (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.

- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein. Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "MMM" gibt beispielsweise eine Länge von drei Zeichen für den Monat an.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSsss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

#### Siehe auch

- „sr\_date\_format-Option [SQL Remote]“ auf Seite 673
- „sr\_time\_format-Option [SQL Remote]“ auf Seite 675
- „sr\_timestamp\_format-Option [SQL Remote]“ auf Seite 676
- „SQL Remote-Optionen“ [*SQL Remote*]

## st\_geometry\_asbinary\_format-Option

Steuert, wie räumliche Werte vom Geometrieformat in Binärformat umgewandelt werden.

#### Zulässige Werte

Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste von Parametern (einschließlich Unterparametern), die für die ST\_AsBinary-Methode dokumentiert sind. Siehe [ST\\_AsBinary-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#).

#### Standardwert

WKB

#### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Mit dieser Option wird ermittelt, wie eine Geometrie in Binärformat umgewandelt wird. Im Folgenden finden Sie die zwei Hauptkontexte, in denen die Option verwendet wird:

- Abrufen eines Werts als Binärwert von einer Clientanwendung
- Ausführen einer CAST-Anweisung Beispiel: `CAST( geometry-expression AS LONG BINARY )`

Zuweisungen von Geometrietypen zu BINARY-Typen führen zu einem Fehler, wenn die Daten nicht von einer Clientanwendung und der CAST-Anweisung abgerufen werden. Beispielsweise können Sie keine Funktion oder Prozedur aufrufen, die einen BINARY-Parameter als Argument verwendet und dann eine Geometrie übergeben. Auch können Sie eine Geometrie nicht einer LONG BINARY-Variablen zuweisen.

### Siehe auch

- [ST\\_AsBinary-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#)
- „st\_geometry\_astext\_format-Option“ auf Seite 680
- „st\_geometry\_asxml\_format-Option“ auf Seite 681
- „st\_geometry\_describe\_type-Option“ auf Seite 682
- „st\_geometry\_on\_invalid-Option“ auf Seite 684
- st\_geometry\_asbinary\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_astext\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_asxml\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_describe\_type-Verbindungseigenschaft auf Seite 737
- st\_geometry\_on\_invalid-Verbindungseigenschaft auf Seite 738

## st\_geometry\_astext\_format-Option

Steuert, wie räumliche Werte vom Geometrieformat in Text umgewandelt werden.

### Zulässige Werte

Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste von Parametern (einschließlich Unterparametern), die für die ST\_AsText-Methode dokumentiert sind. Siehe [ST\\_AsText-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#).

### Standardwert

WKT

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

## Bemerkungen

Mit dieser Option wird ermittelt, wie eine Geometrie in Text umgewandelt wird. Im Folgenden finden Sie die zwei Hauptkontexte, in denen die Option verwendet wird:

- Abrufen eines Werts als Binärwert von einer Clientanwendung
- Ausführen einer CAST-Anweisung. Beispiel: `CAST( geometry-expression AS LONG VARCHAR )`

Zuweisungen von Geometrietypen zu CHAR-Typen führen zu einem Fehler, wenn die Daten nicht von einer Clientanwendung und der CAST-Anweisung abgerufen werden. Beispielsweise können Sie keine Funktion oder Prozedur aufrufen, die einen CHAR-Parameter als Argument verwendet, und dann eine Geometrie übergeben. Auch können Sie eine Geometrie nicht einer LONG VARCHAR-Variablen zuweisen.

## Siehe auch

- [ST\\_AsText-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#)
- „st\_geometry\_asbinary\_format-Option“ auf Seite 679
- „st\_geometry\_asxml\_format-Option“ auf Seite 681
- „st\_geometry\_describe\_type-Option“ auf Seite 682
- „st\_geometry\_on\_invalid-Option“ auf Seite 684
- st\_geometry\_asbinary\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_astext\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_asxml\_format-Verbindungseigenschaft auf Seite 737
- st\_geometry\_describe\_type-Verbindungseigenschaft auf Seite 737
- st\_geometry\_on\_invalid-Verbindungseigenschaft auf Seite 738

## st\_geometry\_asxml\_format-Option

Steuert, wie räumliche Werte vom Geometrieformat in XML umgewandelt werden.

## Zulässige Werte

Die Liste der für diese Option unterstützten Werte ist identisch mit der Liste von Parametern (einschließlich Unterparametern), die für die ST\_AsXML-Methode dokumentiert sind. Siehe [ST\\_AsXML-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#).

## Standardwert

GML

## Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Mit dieser Option wird ermittelt, wie eine Geometrie in XML umgewandelt wird. Im Folgenden finden Sie die zwei Hauptkontexte, in denen die Option verwendet wird:

- Abrufen eines Werts als XML von einer Clientanwendung
- Ausführen einer CAST-Anweisung. Beispiel: `CAST( geometry-expression AS XML )`

Zuweisungen von Geometrietypen zu XML führen zu einem Fehler, wenn die Daten nicht von einer Clientanwendung und der CAST-Anweisung abgerufen werden. Beispielsweise können Sie keine Funktion oder Prozedur aufrufen, die einen XML-Parameter als Argument verwendet, und dann eine Geometrie übergeben. Auch können Sie eine Geometrie nicht einer XML-Variablen zuweisen

### Siehe auch

- [ST\\_AsXML-Methode für den ST\\_Geometry-Datentyp \[SQL Anywhere Server - Unterstützung für räumliche Daten\]](#)
- [„st\\_geometry\\_asbinary\\_format-Option“ auf Seite 679](#)
- [„st\\_geometry\\_astext\\_format-Option“ auf Seite 680](#)
- [„st\\_geometry\\_describe\\_type-Option“ auf Seite 682](#)
- [„st\\_geometry\\_on\\_invalid-Option“ auf Seite 684](#)
- [st\\_geometry\\_asbinary\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_astext\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_asxml\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_describe\\_type-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_on\\_invalid-Verbindungseigenschaft auf Seite 738](#)

## st\_geometry\_describe\_type-Option

Steuert, wie räumliche Werte beschrieben werden.

### Zulässige Werte

- CHAR
- NCHAR
- BINARY

### Standardwert

CHAR

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Räumliche Werte werden als Zeichen- oder Binärdatentypen abgerufen, da Clientbibliotheken die räumlichen Datentypen nicht direkt unterstützen. Die st\_geometry\_describe\_type-Option gibt an, wie eine

Geometriespalte bzw. ein Ausdruck dem Client beschrieben wird. Viele der Clientanwendungen verwenden den DESCRIBE-Typ bei einer Spalte oder einem Ausdruck zur Ermittlung des Client-Datentyps, der für den Abruf der Spalte oder des Ausdrucks verwendet wird. Einige Clientanwendungen ignorieren den DESCRIBE-Typ, sodass das Setzen der `st_geometry_describe_type`-Option möglicherweise nicht die gewünschte Wirkung hat.

Wenn eine Geometrie als Zeichenfolgentyp abgerufen wird, wird die `st_geometry_astext_format`-Option verwendet um zu ermitteln, wie die Geometrie in Text konvertiert werden soll. Wenn sie als Binärtyp abgerufen wird, wird die `st_geometry_asbinary_format`-Option verwendet. Hierbei handelt es sich um dieselben Regeln, die von einer CAST-Anweisung verwendet werden.

In ODBC-Anwendungen geben die Feldkennungen `SQL_DESC_TYPE_NAME` und `SQL_DESC_LOCAL_TYPE_NAME` von `SQLColAttribute` die Zeichenfolge `st_geometry` für Spalten eines beliebigen Geometrietyps zurück. In JDBC wird dies durch Verwendung der Methode `ResultSetMetaData.getColumnTypeName` ausgedrückt.

### Siehe auch

- „`st_geometry_asbinary_format`-Option“ auf Seite 679
- „`st_geometry_astext_format`-Option“ auf Seite 680
- „`st_geometry_asxml_format`-Option“ auf Seite 681
- „`st_geometry_on_invalid`-Option“ auf Seite 684
- `st_geometry_asbinary_format`-Verbindungseigenschaft auf Seite 737
- `st_geometry_astext_format`-Verbindungseigenschaft auf Seite 737
- `st_geometry_asxml_format`-Verbindungseigenschaft auf Seite 737
- `st_geometry_describe_type`-Verbindungseigenschaft auf Seite 737
- `st_geometry_on_invalid`-Verbindungseigenschaft auf Seite 738

## st\_geometry\_interpolation-Option

Steuert die Interpolation, wenn räumliche Berechnungen Kreisbögen enthalten.

### Zulässige Werte

Diese Datenbankoption übernimmt eine durch Semikola begrenzte Reihe von Schlüssel=Wert-Paaren (`Schlüssel1=Wert1;Schlüssel2=Wert2;...`). Zulässige Schlüssel sind `relative-tolerance-percent` und `absolute-tolerance`.

- **relative-tolerance-percent=DOUBLE** Verwenden Sie `relative-tolerance-percent` zur Angabe der als Prozentwert ausgedrückten maximalen Variation, die bei einem Abstand vom Mittelpunkt des `ST_CircularString`-Segments zum interpolierten `ST_LineString`-Segment zulässig ist, relativ zum Radius des `ST_CircularString`-Segments. Der minimal zulässige Wert für `relative-tolerance-percent` ist 0. Das bedeutet, dass immer die `absolute-tolerance`-Einstellung verwendet wird.
- **absolute-tolerance=DOUBLE** Verwenden Sie `absolute-tolerance`, um die maximal zulässige, in Liniereinheiten ausgedrückte absolute Variante festzulegen, die beim Abstand vom Mittelpunkt des `ST_CircularString`-Segments des interpolierten `ST_LineString`-Segments zulässig ist. Der zulässige Mindestwert für `absolute-tolerance` ist auch die Toleranz, die durch die `SRID` festgelegt wird.

### Standardwerte

Wenn kein Schlüssel angegeben ist, hat `relative-tolerance-percent` den Standardwert 0,3. Dies entspricht 40 Punkten in einem kompletten Kreisbogen. Der Wert für `absolute-tolerance` hat standardmäßig die durch SRID festgelegte Toleranz.

Wenn nur ein Schlüssel angegeben wird, wird der andere auf den Mindestwert gesetzt.

Wenn beide Schlüssel angegeben werden, wird die minimale Anzahl von Punkten so erzeugt, dass alle Einschränkungen eingehalten werden.

### Bereich

Kann für eine einzelne Verbindung oder für `PUBLIC` gesetzt werden. Sie müssen das `SET ANY PUBLIC OPTION`-Systemprivileg haben, um diese Option für `PUBLIC` oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Unabhängig von der Einstellung für diese Datenbankoption gibt es mindestens drei Punkte pro Kurvensegment. Außerdem liegen keine zwei aufeinander folgenden Punkte im interpolierten `ST_LineString` innerhalb der Toleranz zueinander.

Weitere Punkte können hinzugefügt werden, um sicherzustellen, dass `ST_Envelope` des `ST_LineString`-Segments gleich ist wie der des ursprünglichen `ST_CircularString`-Werts.

### Siehe auch

- „Auswirkungen der Interpolation auf räumliche Berechnungen“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]
- „`ST_CircularString`-Datentyp“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]
- „`ST_LineString`-Datentyp“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]
- `ST_Envelope`-Methode für den `ST_Geometry`-Datentyp [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]
- „Wie sich Ausrichten am Raster und Toleranz auf räumliche Berechnungen auswirken“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]

## st\_geometry\_on\_invalid-Option

Steuert das Verhalten, wenn die Basisvalidierung für eine Geometrie fehlschlägt (z.B. eine Linienfolge mit nur einem Punkt, ein Polygon mit einem nicht geschlossenen Ring oder eine Geometrie, die über die Grenzen des räumlichen Bezugssystems hinausgeht).

### Zulässige Werte

- **Ignore** Keine Aktion, wenn die Oberflächenvalidierung für eine Geometrie fehlschlägt, und fortfahren mit dem Vorgang.
- **Error** Es wird ein Fehler zurückgegeben, wenn die Oberflächenvalidierung für eine Geometrie fehlschlägt, und der gesamte Vorgang schlägt fehl.

**Standardwert**

Error

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Wenn Sie ungültig räumliche Daten laden müssen, können Sie den Wert für die Option auf "Ignore" einstellen und die ungültigen Daten laden. Sobald die Daten geladen sind, können Sie mit Methoden wie ST\_IsSimple und ST\_IsValue die ungültige Zeile ermitteln und mit ST\_AsText die WKT-Darstellung der Daten abrufen. Die meisten anderen räumlichen Methoden geben einen Fehler zurück, wenn ungültige Geometrien an sie übergeben werden. Mit einem Texteditor können Sie die ungültige Geometrie in WKT korrigieren und dann die Geometrie in der Datenbank aktualisieren.

**Siehe auch**

- [„st\\_geometry\\_asbinary\\_format-Option“ auf Seite 679](#)
- [„st\\_geometry\\_astext\\_format-Option“ auf Seite 680](#)
- [„st\\_geometry\\_asxml\\_format-Option“ auf Seite 681](#)
- [„st\\_geometry\\_describe\\_type-Option“ auf Seite 682](#)
- [st\\_geometry\\_asbinary\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_astext\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_asxml\\_format-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_describe\\_type-Verbindungseigenschaft auf Seite 737](#)
- [st\\_geometry\\_on\\_invalid-Verbindungseigenschaft auf Seite 738](#)

## string\_truncation-Option

Legt fest, ob beim Kürzen einer Zeichenfolge eine Fehlermeldung ausgegeben wird.

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

## Bemerkungen

Wenn die gekürzten Zeichen nur aus Leerstellen bestehen, wird keine Ausnahmebedingung erzeugt. Die Einstellung "On" entspricht dem ANSI/ISO SQL/2008-Verhalten. Wenn die Option auf "Off" gesetzt ist, tritt die Ausnahmebedingung nicht ein und die Zeichenfolge wird stillschweigend gekürzt.

Die Kürzung einer Zeichenfolge kann an mehreren Stellen erfolgen. So kann eine Zeichenfolge etwa bei der Verwendung von INSERT, UPDATE, CAST oder bei der Zuweisung zu einer Variablen gekürzt werden, wenn der deklarierte Zieltyp zu kurz ist.

## Siehe auch

- „Zeichendatentypen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsoptionen“ auf Seite 559
- „SET-Anweisung [T-SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `string_truncation`-Verbindungseigenschaft auf Seite 738

## subscribe\_by\_remote-Option [SQL Remote]

Steuert die Interpretation von NULL- oder SUBSCRIBE BY-Werten mit leeren Zeichenfolgen.

## Zulässige Werte

On, Off

## Standardwert

On

## Bemerkungen

Wenn die Option auf "On" gesetzt ist, gehen Vorgänge von externen Datenbanken bei Zeilen mit einem SUBSCRIBE\_BY-Wert, der NULL oder eine leere Zeichenfolge ist, von der Annahme aus, dass der externe Benutzer die Zeile subskribiert hat. Wenn die Option auf "Off" gesetzt ist, wird angenommen, dass der externe Benutzer nicht für die Zeile subskribiert ist.

Die einzige Einschränkung dieser Option ist, dass es zu Fehlern führt, wenn ein entfernter Benutzer tatsächlich eine Zeile mit NULL oder einem leeren Subskriptionsausdruck einfügen (oder aktualisieren) möchte (bei Informationen, die nur in der konsolidierten Datenbank gespeichert werden). Das ist recht selten und kann umgangen werden, indem ein Subskriptionswert in der Installation verwendet wird, der keinem entfernten Benutzer gehört.

## Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „Die subscribe\_by\_remote-Option in Viele-zu-Viele-Beziehungen“ [[SQL Remote](#)]

## subsume\_row\_locks-Option

Steuert, wann der Datenbankserver individuelle Zeilensperren für eine Tabelle erwirbt

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

**Bemerkungen**

Wenn die Option `subsume_row_locks` auf "On" gesetzt ist (Standard), gilt Folgendes: Wenn eine Tabelle *t* exklusiv mit `LOCK TABLE t IN EXCLUSIVE MODE` gesperrt ist, erwirbt der Datenbankserver keine weiteren individuellen Zeilensperren für *t*.

Dies kann zu deutlichen Performanceverbesserungen führen, wenn exklusive Aktualisierungen in *t* in einer einzelnen Transaktion durchgeführt werden, insbesondere wenn *t* im Vergleich zur Cachegröße sehr groß ist. Außerdem können damit atomare Aktualisierungsoptionen durchgeführt werden, die größer sind als die Sperrentabelle derzeit verarbeiten kann (ca. 2-4 Mio. Zeilen).

Wenn diese Option auf "On" gesetzt ist, geben Keyset-gesteuerte Cursor über eine auf diese Weise gesperrte Tabelle für jede Zeile im Cursor Warnungen wegen geänderter Zeilen zurück, falls in der Datenbank eine Zeile geändert wurde. Der Datenbankserver kann aus diesem Grund einen aktualisierbaren Cursor mit einer ORDER BY-Klausel in einen Keyset-gesteuerten Cursor verwandeln.

**Siehe auch**

- „LOCK TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `subsume_row_locks`-Verbindungseigenschaft auf Seite 738

## **suppress\_tds\_debugging-Option**

Legt fest, ob TDS-Fehlersuche-Informationen im Fenster der Datenbankservermeldungen angezeigt werden.

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Wenn der Datenbankserver mit der Option -z gestartet wird, erscheinen im Fenster der Datenbankservermeldungen Fehlersuche-Informationen, einschließlich der Fehlersuche-Informationen über das TDS-Protokoll.

Die SUPPRESS\_TDS\_DEBUGGING-Option beschränkt die Fehlersuche-Informationen über TDS, die im Fenster der Datenbankservermeldungen angezeigt werden. Wenn die Option auf "Off " (Standardwert) eingestellt ist, werden TDS-Fehlersuche-Informationen im Fenster der Datenbankservermeldungen angezeigt.

### Siehe auch

- [„Datenbankserveroption -z “ auf Seite 312](#)
- [suppress\\_tds\\_debugging-Verbindungseigenschaft auf Seite 738](#)

## synchronize\_mirror\_on\_commit

Steuert, wann es als sicher gilt, dass Datenbankänderungen an einen Spiegelserver gesendet wurden, der im asynchronen oder Asynchron-Ganzseiten-Modus ausgeführt wird.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Die Option synchronize\_mirror\_on\_commit ermöglicht eine Feinabstimmung darüber, wann es als sicher gilt, dass Datenbankänderungen an einen Spiegelserver gesendet wurden, der im asynchronen oder Asynchron-Ganzseiten-Modus ausgeführt wird. Diese Option ist standardmäßig "Off". Wenn auf "On" gesetzt, bewirkt jedes COMMIT, dass jede im Transaktionslog aufgezeichnete Änderung an den Spiegelserver gesendet wird, und dass eine Bestätigung vom Spiegelserver an den Primärserver gesendet wird, sobald die Änderungen vom Spiegelserver empfangen wurden. Diese Option kann bei bestimmten Transaktionen unter Verwendung von SET TEMPORARY OPTION gesetzt werden. Es kann auch nützlich sein, die Option bei bestimmten Anwendungen zu verwenden, indem die APPINFO-Zeichenfolge in einer Login-Prozedur untersucht wird. Dadurch kann das Spiegelungsverhalten an die Bedürfnisse verschiedener Anwendungen angepasst werden.

### Siehe auch

- [„Datenbankspiegelung“ auf Seite 1467](#)
- [synchronize\\_mirror\\_on\\_commit-Verbindungseigenschaft auf Seite 738](#)

## tds\_empty\_string\_is\_null-Option

Steuert, ob bei TDS-Verbindungen leere Zeichenfolgen als NULL oder als Zeichenfolge mit einem Leerzeichen ausgegeben werden

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Standardmäßig ist diese Option auf "Off" eingestellt, und leere Zeichenfolgen werden bei TDS-Verbindungen als eine Zeichenfolge mit einem Leerzeichen ausgegeben. Wenn diese Option auf "On" eingestellt ist, werden bei TDS-Verbindungen leere Zeichenfolgen als NULL-Zeichenfolgen ausgegeben. Nicht-TDS-Verbindungen unterscheiden leere Zeichenfolgen von NULL-Zeichenfolgen.

### Siehe auch

- „NULL-Spezialwert“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- [tds\\_empty\\_string\\_is\\_null-Verbindungseigenschaft auf Seite 738](#)

## temp\_space\_limit\_check-Option

Überprüft die Menge des von einer Verbindung verwendeten Speichers für temporäre Dateien, wobei die Anforderung fehlschlägt, wenn die Menge des angeforderten Speichers größer als die der Verbindung zustehenden Quote ist

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Wenn die Option temp\_space\_limit\_check auf "On" (Standardwert) eingestellt ist und eine Verbindung mehr als ihre Quote von temporären Speicher anfordert, schlägt die Anforderung fehl und der Fehler

SQLSTATE\_TEMP\_SPACE\_LIMIT wird zurückgegeben. Wenn diese Option auf "Off" eingestellt ist, überprüft der Datenbankserver nicht die Menge des Speichers für temporäre Dateien, die eine Verbindung verwendet. Wenn eine Verbindung mehr als ihren Anteil an temporärem Speicher anfordert und diese Option auf "Off" gesetzt ist, kann ein fataler Fehler auftreten.

Die Speicherquote für temporäre Dateien bei einer Verbindung ist das Minimum der folgenden zwei Schwellenwerte:

1. Die maximale Speichermenge für temporäre Dateien, die bei einer Verbindung zulässig ist, wie durch die Einstellung der Option max\_temp\_space angegeben
2. Die maximale potenzielle Größe der temporären Datei, dividiert durch die Anzahl der Verbindungen

Dieser Schwellenwert wird nur verwendet, wenn die temporäre Datei auf 80% oder mehr ihrer maximalen Größe angewachsen ist, was anhand des auf dem Device verbliebenen freien Speicherplatzes bestimmt wird, wie er vom Betriebssystem gemeldet wird. Wenn eine Verbindung mehr freien Speicherplatz anfordert, als es die Quote zulässt, schlägt die aktuelle Anforderung der Verbindung mit SQLSTATE 54W05 (TEMP\_SPACE\_LIMIT) fehl.

Sie können eine "harte" Begrenzung für den Speicherplatz für temporäre Dateien, die eine Verbindung verwenden kann, mit der Option max\_temp\_space angeben.

### Siehe auch

- „sa\_disk\_free\_space-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „max\_temp\_space-Option“ auf Seite 636
- „Datenbankserveroption -dt“ auf Seite 228
- temp\_space\_limit\_check-Verbindungseigenschaft auf Seite 739
- „SQL Anywhere-Einschränkungen von Größe und Anzahl“ auf Seite 791

## time\_format-Option

Setzt das Format für Zeitwerte, die aus der Datenbank abgerufen werden

### Zulässige Werte

Zeichenfolge

### Standardwert

HH:NN:SS[.sss]

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
HH	Stunden zweistellig
NN	Minuten zweistellig
SS[.ssssss]	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.
AA	AM oder PM (12-Stunden-Angabe), bei 24-Stunden-Angabe AA und PP weglassen
PP	P.M. falls nötig (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen

Jedes Symbol wird durch die entsprechenden Daten für die Uhrzeit ersetzt, die formatiert wird.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Groß- und Kleinschreibung (z.B. NN oder nn) ein, um das Auffüllen mit Nullen zuzulassen. Beispiel: hh:nn:ss.sss kann 02:34:56.123 ergeben.
- Geben Sie das Symbol in gemischter Groß- und Kleinschreibung (z.B. Mm) ein, um das Auffüllen mit Nullen zu unterdrücken. Beispiel: Hh:nn:ss.sss kann 2:34:56.123 ergeben.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSssss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

#### Siehe auch

- „date\_format-Option“ auf Seite 599
- „timestamp\_format-Option“ auf Seite 692
- „timestamp\_with\_time\_zone\_format-Option“ auf Seite 694
- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Abrufen von Datums- und Zeitangabe aus der Datenbank“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- time\_format-Verbindungseigenschaft auf Seite 739

## time\_zone\_adjustment-Option

Gestattet es, die Zeitzonenanpassung einer Verbindung zu ändern

#### Zulässige Werte

Ganzzahl ohne Vorzeichen (z.B. 300)

Eine Ganzzahl mit positivem oder negativem Vorzeichen in Anführungszeichen (z.B. "+300" oder "-300")

Zeichenfolge für eine Zeitangabe in Stunden und Minuten mit vorangestelltem "+" oder "-" in Anführungszeichen (zum Beispiel "+5:00" oder "-5:00")

### Standardwert

Wenn der Client über Embedded SQL, ODBC, OLE DB, ADO oder ADONET eine Verbindung herstellt, wird der Standardwert entsprechend der Zeitzone des Clients eingestellt. Wenn der Client die Verbindung über jConnect oder Sybase Open Client herstellt, basiert der Standardwert auf der Zeitzone des Datenbankservers.

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

Standardmäßig wird die Option temporär gesetzt.

### Bemerkungen

Der time\_zone\_adjustment-Optionswert ist derselbe wie der von SELECT CONNECTION\_PROPERTY( 'TimeZoneAdjustment' ) ausgegebene Wert. Der Wert stellt die Anzahl der Minuten dar, die der Coordinated Universal Time (UTC) hinzugefügt werden muss, um die für die Verbindung lokale Uhrzeit anzuzeigen.

Weitere Hinweise dazu, wie diese Option die Konvertierung von TIMESTAMP in TIMESTAMP WITH TIME ZONE steuert, finden Sie unter [Konvertierung in oder aus TIMESTAMP WITH TIME ZONE \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#).

### Siehe auch

- [time\\_zone\\_adjustment-Verbindungseigenschaft auf Seite 739](#)

## timestamp\_format-Option

Setzt das Format für Zeitstempel, die aus der Datenbank abgerufen werden

### Zulässige Werte

Zeichenfolge

### Standardwert

YYYY-MM-DD HH:NN:SS[.sss]

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

## Bemerkungen

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig bzw. Minuten zweistellig, falls nach einem Doppelpunkt (z.B. HH:MM)
MMM[m...]	Zeichenkurzform für Monate: so viele Zeichen wie "m"
D	Wochentag einstellig (1 = Sonntag, 7 = Samstag)
DD	Tag des Monats zweistellig
DDD[d...]	Zeichenkurzform für Wochentag
JJJ	Jahrestag von 1 bis 366
HH	Stunden zweistellig
NN	Minuten zweistellig
SS[.ssssss]	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.
AA	AM oder PM (12-Stunden-Angabe), bei 24-Stunden-Angabe AA und PP weglassen
PP	P.M. falls nötig (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.
- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein.  
Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "mmm" gibt z.B. eine Länge von drei Zeichen für den Monat an.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSsss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

### Hinweis

Wenn Sie die Einstellung für timestamp\_format so ändern, dass das Datumsformat neu geordnet wird, achten Sie darauf, auch die date\_order-Option entsprechend zu ändern, und umgekehrt. Siehe „date\_order-Option“ auf Seite 601.

### Siehe auch

- „date\_format-Option“ auf Seite 599
- „time\_format-Option“ auf Seite 690
- „timestamp\_with\_time\_zone\_format-Option“ auf Seite 694
- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- timestamp\_format-Verbindungseigenschaft auf Seite 739

## timestamp\_with\_time\_zone\_format-Option

Stellt das Format für von der Datenbank abgerufene TIMESTAMP WITH TIME ZONE-Werte ein.

### Zulässige Werte

Zeichenfolge

### Standardwert

YYYY-MM-DD HH:NN:SS[.sss]+HH:NN

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

## Bemerkungen

Das Format ist eine Zeichenfolge mit folgenden Symbolen:

Symbol	Beschreibung
YY	Jahr zweistellig
YYYY	Jahr vierstellig
MM	Monat zweistellig bzw. Minuten zweistellig, falls nach einem Doppelpunkt (z.B. HH:MM)
MMM[m...]	Zeichenkurzform für Monate: so viele Zeichen wie "m"
D	Wochentag einstellig (1 = Sonntag, 7 = Samstag)
DD	Tag des Monats zweistellig
DDD[d...]	Zeichenkurzform für Wochentag
JJJ	Jahrestag von 1 bis 366
HH	Zweistellige Stundenzahl bzw. zweistellige Stundenzahl als Zeitzone-Offset (falls nach "+")
NN	Zweistellige Minutenzahl bzw. zweistellige Minutenzahl als Zeitzone-Offset (falls nach "+")
SS[.ssssss]	Sekunden und Sekundenbruchteile bis zu sechs Dezimalstellen. Nicht alle Plattformen unterstützen Zeitstempel mit einer Genauigkeit von bis zu sechs Stellen.
AA	AM oder PM (12-Stunden-Angabe), bei 24-Stunden-Angabe AA und PP weglassen
PP	P.M. falls nötig (12-Stunden-Angabe), AA und PP bei 24-Stunden-Angabe weglassen
HH	Stunden zweistellig (Zeitzoneverschiebung)
NN	Minuten zweistellig (Zeitzoneverschiebung)

Jedes Symbol wird durch die entsprechenden Daten für das Datum ersetzt, das formatiert wird.

Für Symbole, die Zeichendaten darstellen (wie z.B. MMM), können Sie die Groß- und Kleinschreibung in der Ausgabe wie folgt steuern:

- Wenn nur Großschreibung verwendet werden soll, geben Sie das Symbol in Großbuchstaben ein.  
Beispiel: MMM ergibt JAN.

- Wenn nur Kleinschreibung verwendet werden soll, geben Sie das Symbol in Kleinbuchstaben ein. Beispiel: mmm ergibt jan.
- Wenn Sie das Symbol in Groß- und Kleinbuchstaben eingeben, wählt SQL Anywhere jeweils die richtige Schreibweise für die betreffende Sprache. In Deutsch ergibt z.B. die Schreibweise Mmm die Ausgabe Mai, während dieselbe Schreibweise in Französisch die Ausgabe mai ergibt.

Wenn die Zeichendaten Mehrbyte-Zeichen sind, spiegelt die Länge der einzelnen Symbole die Anzahl der Zeichen und nicht die Anzahl der Bytes wieder. Das Symbol "mmm" gibt z.B. eine Länge von drei Zeichen für den Monat an.

Für Symbole, die numerische Daten darstellen, können Sie das Auffüllen mit Nullen durch die Schreibweise der Symbole steuern:

- Geben Sie das Symbol in einheitlicher Schreibung (z.B. MM oder mm) ein, um das Auffüllen mit Nullen zu gestatten. Beispiel: yyyy/mm/dd ergibt 2002/01/01.
- Geben Sie das Symbol in Groß- und Kleinschreibung (z.B. Mm) ein, wenn das Auffüllen mit Nullen nicht gestattet werden soll. Beispiel: yyyy/Mm/Dd ergibt 2002/1/1.
- Wenn die beiden ersten Ziffern des Sekundenbruchteils in gemischter Groß- und Kleinschreibung (wie Ss oder sSsss) eingegeben wurden, werden nachgestellte Nullen entfernt. Beispiel: hh:nn:ss.Sss kann 12:34:56.1 ergeben.

### Hinweis

Wenn Sie die Einstellung für timestamp\_with\_time\_zone\_format so ändern, dass das Datumsformat neu geordnet wird, achten Sie darauf, auch die date\_order-Option entsprechend zu ändern, und umgekehrt. Siehe „date\_order-Option“ auf Seite 601.

### Siehe auch

- „TIMESTAMP WITH TIME ZONE-Datentyp“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „date\_format-Option“ auf Seite 599
- „time\_format-Option“ auf Seite 690
- „timestamp\_format-Option“ auf Seite 692

## trusted\_certificates\_file-Option

Legt die Datei fest, die die Liste der Zertifikate vertrauenswürdiger Zertifizierungsstellen enthält, wenn der Datenbankserver als Client für einen LDAP-Server fungiert. Diese Option gilt nicht, wenn der Datenbankserver als Client für eine sichere Web-Prozedur fungiert.

### Zulässige Werte

NULL, 'filepath-to-certificate'

### Standardwert

NULL

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Die Einstellung tritt sofort in Kraft.

**Bemerkungen**

Eine eingehende TLS-Verbindung mit SQL Anywhere verwendet Zertifikateinstellungen, die durch die Serveroption -ec festgelegt werden. Damit SQL Anywhere als Client für einen anderen Server fungieren kann, z.B. wenn SQL Anywhere eine Verbindung mit einem LDAP-Server herstellt, muss die Zertifizierungsstelle bekannt sein, die das TLS-Zertifikat signiert hat.

Für Clientverbindungen wird die trusted\_certificates-Option mit dem Pfad zu einer Datei gesetzt, die eine Liste von Zertifikaten vertrauenswürdiger Zertifizierungsstellen enthält. Ebenso wird die trusted\_certificates\_file-Datenbankoption verwendet, um Zertifikate vertrauenswürdiger Zertifizierungsstellen anzugeben, wenn SQL Anywhere als Client fungiert.

Wenn diese Option auf NULL gesetzt ist, können keine ausgehenden TLS-Verbindungen gestartet werden, weil es keine vertrauenswürdigen Zertifizierungsstellen gibt.

**Siehe auch**

- „Datenbankserveroption -ec“ auf Seite 230
- „trusted\_certificates-Protokolloption“ auf Seite 421

**Beispiel**

In diesem Beispiel befindet sich die Liste der vertrauenswürdigen Zertifizierungsstellen, die Serverzertifikate signieren, in einer lokalen Datei namens *trusted.txt*:

```
SET OPTION PUBLIC.trusted_certificates_file = 'C:\\sybase\\shared\\
\\trusted.txt';
```

**truncate\_timestamp\_values-Option**

Begrenzt die Auflösung von TIMESTAMP-Werten.

**Zulässige Werte**

On, Off

**Standardwert**

Off

**Bereich**

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Diese Option darf nicht für Datenbanken gesetzt werden, die bereits Zeitstempeldaten enthalten.

### Bemerkungen

Ein TIMESTAMP-Wert wird in SQL Anywhere auf sechs Dezimalstellen definiert. Um die Systemverträglichkeit mit anderen Datenbanken und Programmen zu gewährleisten, bei denen die TIMESTAMP-Werte auf drei Stellen gekürzt werden, können Sie die Option `truncate_timestamp_values` auf "On" setzen, um die Anzahl der von SQL Anywhere gespeicherten Dezimalstellen zu begrenzen. Die `default_timestamp_increment`-Option legt die Anzahl der Dezimalstellen fest, auf die der TIMESTAMP-Wert gekürzt wird.

Wenn Sie diese Option bei der MobiLink-Synchronisation verwenden, muss sie vor der Durchführung der ersten Synchronisation eingestellt werden.

Wenn der Datenbankserver TIMESTAMP-Werte mit einer höheren Auflösung als der findet, die sich aus der Kombination von `truncate_timestamp_values` und `default_timestamp_increment` ergibt, erscheint eine Fehlermeldung.

Die einfachste Lösung, um sicherzustellen, dass die richtigen TIMESTAMP-Werte verwendet werden, besteht normalerweise darin, die Datenbank zu entladen und anschließend in eine neue Datenbank zu laden, in der zuvor die Werte für `truncate_timestamp_values` und `default_timestamp_increment` gesetzt wurden. Je nach dem Typ der TIMESTAMP-Spalten in Ihrer Tabelle können Sie auch folgendermaßen vorgehen:

- Wenn die TIMESTAMP-Spalten mit DEFAULT TIMESTAMP oder DEFAULT UTC TIMESTAMP definiert wurden (sodass der Wert automatisch vom Datenbankserver aktualisiert wird, wenn die Zeile geändert wird), müssen Sie alle Zeilen in der Tabelle löschen, bevor die Option `truncate_timestamp_values` geändert wird. Sie können die Zeilen löschen, indem Sie die DELETE- oder TRUNCATE TABLE-Anweisung verwenden.
- Wenn die TIMESTAMP-Spalte mit einem anderen Wert als DEFAULT TIMESTAMP oder DEFAULT UTC TIMESTAMP definiert wurde, können Sie eine UPDATE-Anweisung ausführen, die die Werte in eine Zeichenfolge und anschließend zurück in einen TIMESTAMP-Wert umwandeln. Zum Beispiel:

```
UPDATE T
SET ts = CAST( DATEFORMAT( ts, 'yyyy/mm/dd hh:nn:ss.ss' )
AS TIMESTAMP );
```

Bei diesem Verfahren kann mehr Präzision als nötig verloren gehen. Welche Formatzeichenfolge zu verwenden ist, hängt von der beizubehaltenden Gesamtstellenzahl ab.

### Siehe auch

- „`default_timestamp_increment`-Option“ auf Seite 605
- „TIMESTAMP-Spezialwert“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CURRENT UTC TIMESTAMP-Spezialwert“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „UTC TIMESTAMP-Spezialwert“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- `truncate_timestamp_values`-Verbindungseigenschaft auf Seite 739

### Beispiel

Wenn die `default_timestamp_increment`-Option auf 100000 gesetzt wird, erfolgt die Kürzung nach der ersten Dezimalstelle im Sekundenelement, sodass ein Wert wie "2000/12/05 10:50:53:700" gespeichert werden kann.

## tsql\_outter\_joins-Option

Steuert die Fähigkeit, die Transact-SQL-Outter-Join-Operatoren \*= und =\* in Anweisungen und Ansichten zu verwenden

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Die Unterstützung für Transact-SQL-Outter-Joins ist veraltet. Wenn Sie diese Option auf "On" setzen, können Sie Transact-SQL-Outter-Joins verwenden.

### Siehe auch

- „Kompatibilitätsoptionen“ auf Seite 559
- „Transact-SQL-Outter-Joins (\*= oder =\*)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Join-Operatoren“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- tsql\_outter\_joins-Verbindungseigenschaft auf Seite 740

## tsql\_variables-Option

Legt fest, ob das Zeichen @ als Präfix für Hostvariablenamen von Embedded SQL verwendet werden darf

### Zulässige Werte

On, Off

### Standardwert

Off

On für Sybase Open Client- und jConnect-Verbindungen

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

## Bemerkungen

Wenn die Option auf "On" gesetzt ist, können Sie das Zeichen @ anstelle des Doppelpunkts als Präfix für einen Hostvariablenamen in Embedded SQL verwenden. Dies ist in erster Linie zur Kompatibilität mit Transact-SQL implementiert.

## Siehe auch

- „Kompatibilitätsoptionen“ auf Seite 559
- „sp\_tsql\_environment-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- tsql\_variables-Verbindungseigenschaft auf Seite 740

## updatable\_statement\_isolation-Option

Gibt die von aktualisierbaren Anweisungen verwendete Isolationsstufe an, wenn die Option isolation\_level auf Readonly-statement-snapshot gesetzt ist.

## Zulässige Werte

0, 1, 2, 3

## Standardwert

0

## Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

## Bemerkungen

Die in der Option updatable\_statement\_isolation angegebene Isolationsstufe wird von aktualisierbaren Anweisungen verwendet, wenn die Option isolation\_level auf Readonly-statement-snapshot gesetzt ist. Die folgenden Werte werden angenommen:

- **0** Lässt Dirty Reads, nicht wiederholbare Lesevorgänge und Phantomzeilen zu
- **1** Verhindert Dirty Reads. Lässt nicht wiederholbare Lesevorgänge und Phantomzeilen zu.
- **2** Verhindert Dirty Reads und nicht wiederholbare Lesevorgänge. Lässt Phantomzeilen zu.
- **3** Serialisierbar. Verhindert Dirty Reads, nicht wiederholbare Lesevorgänge und Phantomzeilen.

## Siehe auch

- „isolation\_level-Option“ auf Seite 619
- „Snapshot-Isolation“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Isolationsstufen und Konsistenz“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Richtlinien zum Auswählen der Isolationsstufen“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Typische Arten von Inkonsistenz“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- updatable\_statement\_isolation-Verbindungseigenschaft auf Seite 740

## update\_statistics-Option

Steuert, ob Verbindungen Abfragerückmeldungen an den Statistikwächter senden können.

### Zulässige Werte

On, Off

### Standardwert

On

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können.

### Bemerkungen

Der Datenbankserver sammelt Statistiken während der normalen Abfrageausführung und benutzt die erfassten Statistiken zur automatischen Optimierung der Spaltenstatistiken. Wenn Sie diese Option auf Off setzen, erhält der Statistikwächter keine Rückmeldung über den Zustand der Statistiken und behebt keine Statistikprobleme für die angegebene Verbindung. Er überwacht jedoch weiterhin die Verwendung von Statistiken und erstellt oder löscht Statistiken auf der Grundlage ihrer Verwendung.

Wenn diese Option von einem Benutzer mit SET ANY PUBLIC OPTION-Systemprivileg festgelegt wird, wirkt sich ihre Einstellung auf alle Verbindungen mit der Datenbank aus. Andernfalls sind nur die Verbindungen des aktuellen Benutzers betroffen.

Unter normalen Bedingungen braucht diese Option nicht deaktiviert zu werden.

Die Option update\_statistics hat keine Auswirkungen auf Statistiken aufgrund von Datenaktualisierungen (LOAD/INSERT/UPDATE/DELETE). Um zu steuern, ob Statistiken basierend auf diesen Anweisungen aktualisiert werden, verwenden Sie die Datenbankoption collect\_statistics\_on\_dml\_updates.

Der Unterschied zwischen der Option collect\_statistics\_on\_dml\_updates und der Option update\_statistics liegt darin, dass die Option update\_statistics die tatsächliche Anzahl der Zeilen, die das Prädikat erfüllen, mit der Anzahl der Zeilen vergleicht, bei denen eine Prädikaterfüllung geschätzt wird, und dann die Schätzung entsprechend aktualisiert. Die Option collect\_statistics\_on\_dml\_updates ändert die Spaltenstatistiken aufgrund der Werte der spezifischen Zeilen, die eingefügt, aktualisiert oder gelöscht werden.

### Siehe auch

- „collect\_statistics\_on\_dml\_updates-Option“ auf Seite 591
- „Verwaltung von Statistiken durch den Statistikwächter“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Tipp: Spaltenstatistiken aktualisieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- update\_statistics-Verbindungseigenschaft auf Seite 740

## user\_estimates-Option

Steuert, ob Benutzer-Selektivitätseinschätzungen in Abfrageprädikaten vom Abfrageoptimierer respektiert oder ignoriert werden.

### Zulässige Werte

Enabled, Disabled, Override-Magic

### Standardwert

Override-Magic

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

SQL Anywhere ermöglicht es Ihnen, Benutzer-Selektivitätsschätzungen anzugeben, die die Performance des Optimierers steigern können, wenn der Datenbankserver nicht in der Lage ist, die Selektivität eines Prädikats genau vorherzusagen. Benutzer-Selektivitätsschätzungen sollten allerdings nur unter den entsprechenden Umständen eingesetzt werden. So kann es zum Beispiel nützlich sein, eine Selektivitätsschätzung für ein Prädikat zu liefern, das eine oder mehrere Funktionen betrifft, wenn sich die vom Optimierer verwendete Override-Magic-Selektivitätsschätzung signifikant von der tatsächlichen Selektivität unterscheidet.

Wenn Sie Selektivitätsschätzungen verwendet haben, die als Behelfslösung für Performanceprobleme nicht ausreichen, bei denen der von der Software ausgewählte Zugriffsplan ungeeignet war, dann ist es empfehlenswert, diese Option auf "Disabled" einzustellen. Der Datenbankserver wählt möglicherweise nicht den optimalen Plan aus, wenn Sie unzutreffende Schätzungen verwenden.

Weitere Informationen zu Selektivitätsschätzungen finden Sie unter „[Explizite Selektivitätsschätzungen](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

Wenn eine Benutzer-Selektivitätsschätzung mit einem Prädikat übergeben wurde, wird die Schätzung abhängig von der Einstellung dieser Option entweder respektiert oder ignoriert. Die folgenden Werte werden angenommen:

- **Valid** Alle von Benutzern gelieferten Selektivitätsschätzungen werden respektiert. Sie können diese Option mit "On" einschalten.
- **Override-Magic** Eine Benutzer-Selektivitätsschätzung wird nur respektiert und verwendet, wenn der Optimierer sonst als letzte Möglichkeit seinen heuristischen Wert (auch magischer Wert genannt) verwenden würde.
- **Disabled** Alle Benutzerschätzungen werden ignoriert und magische Werte verwendet, wenn keine anderen Schätzungsdaten verfügbar sind. Sie können diese Option mit "Off" ausschalten.

Sie können temporäre oder PUBLIC-Einstellungen für diese Option in einzelnen INSERT-, UPDATE-, DELETE-, SELECT-, UNION-, EXCEPT- und INTERSECT-Anweisungen aufheben, indem Sie eine OPTION-Klausel in die Anweisung aufnehmen.

#### Siehe auch

- „INSERT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UPDATE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „DELETE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SELECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UNION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „EXCEPT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „INTERSECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Tipp: Explizite Selektivitätsschätzungen sparsam einsetzen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Explizite Selektivitätsschätzungen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- user\_estimates-Verbindungseigenschaft auf Seite 740

## uuid\_has\_hyphens-Option

Steuert die Formatierung von Werten für eindeutige Bezeichner, wenn sie in Zeichenfolgen konvertiert werden

#### Zulässige Werte

On, Off

#### Standardwert

On

#### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

#### Bemerkungen

Wenn die Option uuid\_has\_hyphens auf "On" gesetzt ist, enthalten die resultierenden Zeichenfolgen vier Bindestriche. Zum Beispiel: 12345678-1234-1234-1234-1234567890ab. Wenn diese Option auf "Off" gesetzt ist, werden die Bindestriche in der Zeichenfolge weggelassen. Der Datenbankserver unterstützt UUID-Zeichenfolgen sowohl mit als auch ohne Bindestriche, wenn eine Zeichenfolge in den Wert des eindeutigen Bezeichners konvertiert wird.

#### Siehe auch

- „UNIQUEIDENTIFIER-Datentyp“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## verify\_all\_columns-Option [SQL Remote]

Steuert, ob Nachrichten, die von der lokalen Datenbank publizierte Aktualisierungen enthalten, einschließlich aller Spaltenwerte gesendet werden

### Zulässige Werte

On, Off

### Standardwert

Off

### Bemerkungen

Diese Option wird nur von SQL Remote verwendet. Wenn die Option auf "On" gesetzt ist, werden Nachrichten, die von der lokalen Datenbank publizierte Aktualisierungen enthalten, einschließlich aller Spaltenwerte gesendet, und ein Konflikt in einer Spalte provoziert einen RESOLVE UPDATE-Trigger auf der Subskribenten-Datenbank.

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „Die verify\_all\_columns-Option“ [[SQL Remote](#)]

### Beispiel

Die folgende Anweisung stellt die Option verify\_all\_columns für alle Benutzer in SQL Anywhere auf Off:

```
SET OPTION PUBLIC.verify_all_columns = 'Off';
```

## verify\_password\_function-Option

Implementiert Kennwortregeln.

### Zulässige Werte

Zeichenfolge

### Standardwert

Leere Zeichenfolge (keine Funktion wird aufgerufen, wenn ein Kennwort eingestellt ist).

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben, um diese Option setzen zu können.

### Bemerkungen

Die durch diese Option angegebene Funktion wird automatisch aufgerufen, wenn ein Nicht-NULL-Kennwort erstellt oder festgelegt wird. Die angegebene Funktion wird nicht für Benutzer aufgerufen, in deren Login-Richtlinie die change\_password\_dual\_control-Option aktiviert ist. Um zu verhindern, dass ein Benutzer die Funktion außer Kraft setzen kann, stellen sie den Optionswert auf

*Eigentümer.Funktionsname* ein. Ein Benutzer kann eine Verbindung mit der Datenbank nur herstellen, wenn er ein Kennwort hat.

Nachdem die Anweisung validiert wurde, die für das Erstellen oder Einstellen eines Kennwort verwendet wurde, wird die Funktion aufgerufen, um das Kennwort anhand der angegebenen Regeln zu überprüfen. Wenn das Kennwort den angegebenen Regeln entspricht, gibt die Funktion NULL zurück, um einen Erfolg anzuzeigen, und die aufrufende Anweisung wird ausgeführt. Andernfalls wird eine Nicht-NULL-Zeichenfolge zurückgegeben und als Grund für den Fehler angezeigt.

Die Kennwort-Überprüfungsfunktion akzeptiert zwei Parameter: *Benutzername* VARCHAR(128) und *Neues\_Kennwort* VARCHAR(255). Sie gibt einen Wert vom Typ VARCHAR(255) zurück.

Es wird empfohlen, dass Sie die Anweisung ALTER FUNCTION *Funktionsname* SET HIDDEN auf die Kennwort-Überprüfungsfunktion anwenden, um zu gewährleisten, dass sie nicht mithilfe des Debuggers schrittweise durchgegangen werden kann.

Wenn die Option `verify_password_function` gesetzt ist, ist es nicht zulässig, mehr als eine Benutzer-ID bzw. Kennwort mit der Anweisung GRANT CONNECT anzugeben.

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

Weitere Informationen zu Kennwortregeln finden Sie unter [Kennwortüberprüfung verwenden auf Seite 1411](#).

## Beispiel

Das folgende Beispiel definiert eine Tabelle und eine Funktion und legt einige Login-Richtlinienoptionen fest. Zusammen implementieren sie erweiterte Kennwortregeln, einschließlich der Erzwingung bestimmter Zeichentypen im Kennwort, des Verbots einer Kennwort-Wiederverwendung und ablaufender Kennwörter. Die Funktion wird vom Datenbankserver mit der Option `verify_password_function` aufgerufen, wenn eine Benutzer-ID erstellt oder ein Kennwort geändert wird. Die Anwendung kann die von der Option `post_login_procedure` angegebene Prozedur aufrufen, um mitzuteilen, dass das Kennwort geändert werden sollte, bevor es abläuft.

Der Code für dieses Beispiel ist auch am folgenden Speicherort verfügbar: `%SQLANYSAMPI6%\SQLAnywhere\SQL\verify_password.sql`.

```
-- only DBA should have privileges on this table
CREATE TABLE DBA.t_pwd_history(
    pk          INT          DEFAULT AUTOINCREMENT PRIMARY KEY,
    user_name   CHAR(128),   -- the user whose password is set
```

```

        pwd_hash      CHAR(32) ); -- hash of password value to detect
                                -- duplicate passwords

-- called whenever a non-NULL password is set
-- to verify the password conforms to password rules
CREATE FUNCTION DBA.f_verify_pwd( uid      VARCHAR(128),
                                new_pwd VARCHAR(255) )
RETURNS VARCHAR(255)
BEGIN
    -- a table with one row per character in new_pwd
    DECLARE local temporary table pwd_chars(
        pos INT PRIMARY KEY,    -- index of c in new_pwd
        c   CHAR( 1 CHAR ) );  -- character
    -- new_pwd with non-alpha characters removed
    DECLARE pwd_alpha_only      CHAR(255);
    DECLARE num_lower_chars     INT;

    -- enforce minimum length (can also be done with
    -- min_password_length option)
    IF length( new_pwd ) < 6 THEN
        RETURN 'password must be at least 6 characters long';
    END IF;

    -- break new_pwd into one row per character
    INSERT INTO pwd_chars SELECT row_num, substr( new_pwd, row_num, 1 )
                        FROM dbo.RowGenerator
                        WHERE row_num <= length( new_pwd );

    -- copy of new_pwd containing alpha-only characters
    SELECT list( c, ' ' ORDER BY pos ) INTO pwd_alpha_only
        FROM pwd_chars WHERE c BETWEEN 'a' AND 'z' OR c BETWEEN 'A' AND 'Z';

    -- number of lowercase characters IN new_pwd
    SELECT count(*) INTO num_lower_chars
        FROM pwd_chars WHERE CAST( c AS BINARY ) BETWEEN 'a' AND 'z';

    -- enforce rules based on characters contained in new_pwd
    IF ( SELECT count(*) FROM pwd_chars WHERE c BETWEEN '0' AND '9' )
        < 1 THEN
        RETURN 'password must contain at least one numeric digit';
    ELSEIF length( pwd_alpha_only ) < 2 THEN
        RETURN 'password must contain at least two letters';
    ELSEIF num_lower_chars = 0
        OR length( pwd_alpha_only ) - num_lower_chars = 0 THEN
        RETURN 'password must contain both upper- and lowercase characters';
    END IF;

    -- not the same as any user name
    -- (this could be modified to check against a disallowed words table)
    IF EXISTS( SELECT * FROM SYS.SYSUSER
                WHERE lower( user_name ) IN ( lower( pwd_alpha_only ),
                                              lower( new_pwd ) ) ) THEN
        RETURN 'password or only alphabetic characters in password ' ||
            'must not match any user name';
    END IF;

    -- not the same as any previous password for this user
    IF EXISTS( SELECT * FROM t_pwd_history
                WHERE user_name = uid
                AND pwd_hash = hash( uid || new_pwd, 'md5' ) ) THEN
        RETURN 'previous passwords cannot be reused';
    END IF;

    -- save the new password

```

```

INSERT INTO t_pwd_history( user_name, pwd_hash )
VALUES( uid, hash( uid || new_pwd, 'md5' ) );

RETURN( NULL );
END;

ALTER FUNCTION DBA.f_verify_pwd SET HIDDEN;
GRANT EXECUTE ON DBA.f_verify_pwd TO PUBLIC;
SET OPTION PUBLIC.verify_password_function = 'DBA.f_verify_pwd';

-- All passwords expire in 180 days. Expired passwords can be changed
-- by the user using the NewPassword connection parameter.
ALTER LOGIN POLICY DEFAULT password_life_time = 180;

-- If an application calls the procedure specified by the
-- post_login_procedure option, then the procedure can be used to
-- warn the user that their password is about to expire. In particular,
-- Interactive SQL and Sybase Central call the post_login_procedure.
ALTER LOGIN POLICY DEFAULT password_grace_time = 30;

-- Five consecutive failed login attempts results in a non-DBA
-- user ID being locked.
ALTER LOGIN POLICY DEFAULT max_failed_login_attempts = 5;

```

**Siehe auch**

- „min\_password\_length-Option“ auf Seite 637
- „CREATE USER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE FUNCTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER FUNCTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER USER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Hinweise zur Sicherheit: Kennwörter“ auf Seite 1410
- „Verbindungsparameter NewPassword (NEWPWD)“ auf Seite 372
- verify\_password\_function-Verbindungseigenschaft auf Seite 743
- „Kennwörter für die Doppelkontrolle“ auf Seite 1370

**verify\_threshold-Option [SQL Remote]**

Steuert, welche Spalten beim Replizieren von Aktualisierungen überprüft werden

**Zulässige Werte**

Ganzzahl, in Byte

**Standardwert**

1000

**Bemerkungen**

Diese Option wird nur von SQL Remote verwendet. Wenn der Datentyp einer Spalte größer als der Schwellenwert ist, werden alte Werte in der Spalte nicht überprüft, wenn ein UPDATE repliziert wird. Dies hält die Größe von SQL Remote-Nachrichten niedrig, hat aber den Nachteil, dass kollidierende Aktualisierungen langer Werte nicht erkannt werden.

### Siehe auch

- „SQL Remote-Optionen“ [[SQL Remote](#)]
- „BLOBs“ [[SQL Remote](#)]

## wait\_for\_commit-Option

Bestimmt, wann die Integrität von Fremdschlüsseln beim Ändern von Daten geprüft wird

### Zulässige Werte

On, Off

### Standardwert

Off

### Bereich

Kann für eine einzelne Verbindung oder für PUBLIC gesetzt werden. Sie müssen das SET ANY PUBLIC OPTION-Systemprivileg haben, um diese Option für PUBLIC oder für andere Benutzer oder Rollen setzen zu können. Wird sofort wirksam.

### Bemerkungen

Wenn die Option auf "On" gesetzt ist, prüft die Datenbank die Integrität von Fremdschlüsseln bis zur nächsten COMMIT Anweisung nicht. Andernfalls werden alle Fremdschlüssel, die nicht mit der check\_on\_commit-Option erstellt wurden, beim Einfügen, Aktualisieren oder Löschen geprüft.

### Siehe auch

- „sa\_check\_commit-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Sperren bei Einfügungen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Referenzielle Integrität prüfen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- wait\_for\_commit-Verbindungseigenschaft auf Seite 743

## webservice\_namespace\_host-Option

Gibt den Hostnamen innerhalb der XML-Namespace-Spezifikation für DISH-Dienste an.

### Zulässige Werte

NULL oder Hostname-Zeichenfolge

### Standardwert

NULL

### Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

## Bemerkungen

Diese Option hebt die Standardverwendung des HTTP Host-Anforderungsheaders auf.

DISH-Dienste exportieren Webservices Description Language-Dokumente (WSDLs). Es sind XML-Dokumente, die Beschreibungen der verfügbaren SOAP-Dienste enthalten. Die URL der targetNamespace- und der soapAction-Vorgänge innerhalb dieses XML-Dokuments enthalten einen Hostnamen. Wenn diese Option auf NULL eingestellt ist (Standardwert), ist der Hostname der Name des Computers, auf dem der Datenbankserver läuft. Wenn diese Option auf einen Zeichenfolgewert eingestellt ist, wird stattdessen die Zeichenfolge als Hostname verwendet. Diese Option ist für die Entwicklung von Webdienst-Clientanwendungen gedacht, die nach der Bereitstellung einen anderen Zielhost als den für die Entwicklung verwendeten Host haben sollen.

## Siehe auch

- „SQL Anywhere als HTTP-Webserver“ [[SQL Anywhere Server - Programmierung](#)]
- [webservice\\_namespace\\_host-Verbindungseigenschaft auf Seite 744](#)

## webservice\_sessionid\_name-Option

Legt neu fest, anhand welcher Informationen der SQL Anywhere-Webserver ermittelt, ob die Sitzungsverwaltung verwendet wird.

## Zulässige Werte

NULL oder SessionID-Zeichenfolge

## Standardwert

NULL

## Bereich

Kann nur für PUBLIC gesetzt werden. Sie müssen das SET ANY SYSTEM OPTION-Systemprivileg haben, um diese Option setzen zu können. Wird sofort wirksam.

## Bemerkungen

Mit der webservice\_sessionid\_name-Option können Sie neu festlegen, wonach der Webserver suchen soll, um zu ermitteln, ob die Sitzungsverwaltung verwendet wird. Standardmäßig ist der Name des Sitzungsbezeichners SessionID.

Diese Datenbankoption ist nützlich, wenn Ihre Webanwendung für den Sitzungsbezeichner einen anderen Namen als SessionID verwendet, z.B. JSessionID.

Wenn die Webanwendung die URL-basierte Sitzungsverwaltung verwendet, wird der Sitzungsbezeichner in der GET-Anforderung angezeigt:

```
GET /service?JSessionID=session_63520025849921 HTTP/1.1
```

Wenn die Webanwendung die Cookie-basierte Sitzungsverwaltung verwendet, wird der Sitzungsbezeichner im Cookie-Header angezeigt.

```
Cookie: JSessionID=cookie_session_63520025481454
```

Der durch die `webservice_sessionid_name`-Datenbankoption angegebene Name wird nur verwendet, wenn der Webserver Webdienstanforderungen analysiert.

### Beispiel

- Das folgende Beispiel benennt den Sitzungsbezeichner für Webdienste in JSessionID um:

```
SET OPTION PUBLIC.webservice_sessionid_name="JSessionID";
```

### Siehe auch

- „SQL Anywhere als HTTP-Webserver“ [[SQL Anywhere Server - Programmierung](#)]
- [webservice\\_sessionid\\_name](#)-Verbindungseigenschaft auf Seite 744

## Verbindungs-, Datenbank- und Datenbankserveigenschaften

### Zugreifen auf Werte von Verbindungseigenschaften

Verbindungseigenschaften sind für jede einzelne Verbindung mit einer SQL Anywhere-Datenbank verfügbar. Sie können die `CONNECTION_PROPERTY`-Systemfunktion verwenden, um den Wert für eine einzelne Eigenschaft abzurufen, oder die `sa_conn_properties`-Systemprozedur, um die Werte aller Verbindungseigenschaften abzurufen.

### Voraussetzungen

Sie benötigen keine Privilegien, um die Verbindungseigenschaften für Ihre Verbindung anzuzeigen. Um die Verbindungseigenschaften für andere Verbindungen anzeigen zu können, benötigen Sie das Systemprivileg `SERVER OPERATOR`, `MONITOR` oder `DROP CONNECTION`.

### Kontext und Bemerkungen

Bei Eigenschaftsnamen wird die Groß- und Kleinschreibung nicht berücksichtigt.

### Aufgabe

- Verwenden Sie eine der folgenden Methoden, um auf Werte von Verbindungseigenschaften zuzugreifen:

Option	Aktion
Wert einer Verbindungseigenschaft abrufen	Verwenden Sie die <code>CONNECTION_PROPERTY</code> -Systemfunktion.
Werte aller Verbindungseigenschaften abrufen	Verwenden Sie die <code>sa_conn_properties</code> -Systemprozedur.

## Ergebnisse

Der Wert der Verbindungseigenschaft wird zurückgegeben. Für jede Verbindungseigenschaft wird eine eigene Zeile angezeigt.

## Beispiel

Die folgende Anweisung gibt die Anzahl der Seiten zurück, die von der aktuellen Verbindung aus der Datei gelesen wurden.

```
SELECT CONNECTION_PROPERTY ( 'DiskRead' );
```

Verwenden Sie die sa\_conn\_properties-Systemprozedur, um die Werte aller Verbindungseigenschaften abzurufen:

```
CALL sa_conn_properties( );
```

## Siehe auch

- „CONNECTION\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_conn\_properties-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Liste der Verbindungseigenschaften“ auf Seite 711
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „Liste der Datenbankservereigenschaften“ auf Seite 745

## Liste der Verbindungseigenschaften

Verbindungseigenschaften sind für jede einzelne Verbindung mit einer SQL Anywhere-Datenbank verfügbar. Bei Verbindungseigenschaftsnamen wird die Groß- und Kleinschreibung nicht berücksichtigt.

### Verbindungseigenschaften

Eigenschaftsname	Beschreibung
<b>allow_nulls_by_default</b>	Gibt einen Wert zurück, der angibt, ob Spalten, die ohne Festlegen von NULL oder NOT NULL erstellt wurden, NULL enthalten dürfen. Siehe <a href="#">„allow_nulls_by_default-Option“ auf Seite 572</a> .
<b>allow_read_client_file</b>	Gibt einen Wert zurück, der angibt, ob der Datenbankserver das Lesen von Dateien auf einem Clientcomputer zulässt. Siehe <a href="#">„allow_read_client_file-Option“ auf Seite 573</a> .
<b>allow_snapshot_isolation</b>	Gibt einen Wert zurück, der angibt, ob Snapshot-Isolation aktiviert oder deaktiviert ist. Siehe <a href="#">„allow_snapshot_isolation-Option“ auf Seite 574</a> .
<b>allow_write_client_file</b>	Gibt einen Wert zurück, der angibt, ob der Datenbankserver das Schreiben von Dateien auf einem Clientcomputer zulässt. Siehe <a href="#">„allow_write_client_file-Option“ auf Seite 575</a> .

Eigenschaftsname	Beschreibung
<b>ansi_blanks</b>	Gibt einen Wert zurück, der angibt, wann Zeichendaten clientseitig gekürzt werden. Siehe „ <a href="#">ansi_blanks-Option</a> “ auf Seite 575.
<b>ansi_close_cursors_on_rollback</b>	Gibt einen Wert zurück, der angibt, ob mit WITH HOLD geöffnete Cursor geschlossen werden, wenn ein ROLLBACK durchgeführt wird. Siehe „ <a href="#">ansi_close_cursors_on_rollback-Option</a> “ auf Seite 576.
<b>ansi_permissions</b>	Gibt einen Wert zurück, der angibt, ob Privilegien bei DELETE- und UPDATE-Anweisungen überprüft werden. Siehe „ <a href="#">ansi_permissions-Option</a> “ auf Seite 577.
<b>ansi_substring</b>	Gibt einen Wert zurück, der angibt, wie sich die Funktion SUBSTRING (SUBSTR) verhält, wenn negative Werte für die Start- oder Längenparameter angegeben werden. Siehe „ <a href="#">ansi_substring-Option</a> “ auf Seite 578.
<b>ansi_update_constraints</b>	Gibt einen Wert zurück, der den Bereich der Aktualisierungen angibt, die zulässig sind. Siehe „ <a href="#">ansi_update_constraints-Option</a> “ auf Seite 579.
<b>ansinull</b>	Gibt einen Wert zurück, der angibt, wie NULL interpretiert wird. Siehe „ <a href="#">ansinull-Option</a> “ auf Seite 580.
<b>AppInfo</b>	<p>Gibt Informationen über den Client zurück, der die Verbindung hergestellt hat. Bei HTTP-Verbindungen umfasst dies auch Angaben zum Browser. Bei Verbindungen, die ältere Versionen von jConnect oder Sybase Open Client verwenden, können die Informationen unvollständig sein.</p> <p>Der API-Wert kann DBLIB, ODBC, OLEDB, ADO.NET, iAnywhereJDBC, PHP, PerlDBD oder DBEXPRESS sein.</p> <p>Weitere Informationen zu Werten, die bei anderen Verbindungstypen zurückgegeben werden, finden Sie unter „<a href="#">Verbindungsparameter AppInfo (APP)</a>“ auf Seite 338.</p>
<b>ApproximateCPUTime</b>	Gibt eine Schätzung der Menge der CPU-Zeit zurück, die von einer gegebenen Verbindung verbraucht wurde, in Sekunden. Der zurückgegebene Wert kann sich vom tatsächlichen Wert um bis zu 50% unterscheiden, auch wenn übliche Abweichungen im 5 - 10%-Bereich liegen. Auf Mehrprozessorcomputern akkumuliert jede CPU (bzw. jeder Hyperthread oder Kern) Zeit, daher kann die Summe der akkumulierten Zeit größer als die verstrichene Zeit sein. Diese Eigenschaft wird unter Windows und Linux unterstützt.

Eigenschaftsname	Beschreibung
<b>auditing</b>	<p>Gibt "On" zurück, wenn die Option PUBLIC.auditing auf "On" gesetzt ist. Anderenfalls wird "Off" zurückgegeben.</p> <p>Wenn die Option auditing auf "On" und die Option conn_auditing auf "Off" gesetzt sind, gibt die Verbindungseigenschaft auditing dennoch "On" zurück, obwohl bei der aktuellen Verbindung kein Auditing stattfindet. Siehe „<a href="#">Auditing konfigurieren (Sybase Central)</a>“ auf Seite 1418 und „<a href="#">auditing-Option</a>“ auf Seite 582.</p>
<b>auditing_options</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>Authenticated</b>	Gibt "Yes" zurück, wenn die Anwendung eine gültige Zeichenfolge zur Verbindungsauthentifizierung gesendet hat. Gibt "No" zurück, wenn die Anwendung keine gültige Zeichenfolge zur Verbindungsauthentifizierung gesendet hat.
<b>AuthType</b>	Gibt den Typ der Authentifizierung zurück, der bei der Verbindungsherstellung verwendet wird. Der zurückgegebene Wert ist "Standard", "Integrated", "Kerberos", "LDAPUA", CloudAdmin oder eine leere Zeichenfolge. Eine leere Zeichenfolge wird bei internen Verbindungen und bei Verbindungen für HTTP-Dienste zurückgegeben, die AUTHORIZATION OFF verwenden.
<b>auto_commit_on_create_local_temp_index</b>	Gibt die Einstellung der auto_commit_on_create_local_temp_index-Option zurück. Siehe „ <a href="#">auto_commit_on_create_local_temp_index-Option</a> “ auf Seite 583.
<b>background_priority</b>	Diese Eigenschaft ist veraltet. Gibt einen Wert zurück, der angibt, welche Auswirkung die aktuelle Verbindung auf die Performance von anderen Verbindungen hat. Siehe „ <a href="#">background_priority-Option [nicht mehr empfohlen]</a> “ auf Seite 584.
<b>BlockedOn</b>	Gibt Null zurück, wenn die aktuelle Verbindung nicht blockiert ist, bzw. im Fall einer Blockierung die Verbindungsnummer, auf der die Verbindung aufgrund eines Sperrenkonflikts blockiert ist.
<b>blocking</b>	Gibt einen Wert zurück, der das Verhalten des Datenbankservers bei Sperrenkonflikten angibt. Siehe „ <a href="#">blocking-Option</a> “ auf Seite 585.
<b>blocking_others_timeout</b>	Gibt zurück, wie lange die Zeilen- und Tabellensperren der aktuellen Verbindung durch eine andere Verbindung blockiert werden, bevor die aktuelle Verbindung zurückgesetzt wird. Siehe „ <a href="#">blocking_others_timeout-Option</a> “ auf Seite 586.

Eigenschaftsname	Beschreibung
<b>blocking_timeout</b>	Gibt die Zeitspanne, in Millisekunden, zurück, die eine Transaktion auf den Erhalt einer Sperre wartet. Siehe „ <a href="#">blocking_timeout-Option</a> “ auf Seite 587.
<b>BytesReceived</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesReceivedUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. Dieser Wert ist derselbe wie für "BytesReceived", wenn die Komprimierung deaktiviert ist.
<b>BytesSent</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesSentUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. Dieser Wert ist derselbe wie für "BytesSent", wenn die Komprimierung deaktiviert ist.
<b>CacheHits</b>	Gibt die Anzahl der erfolgreichen Lesevorgänge im Cache zurück.
<b>CacheRead</b>	Gibt die Anzahl der Datenbankseiten zurück, die im Cache nachgeschlagen wurden.
<b>CacheReadIndInt</b>	Gibt die Anzahl der internen Knotenseiten des Indexes zurück, die aus dem Cache gelesen wurden.
<b>CacheReadIndLeaf</b>	Gibt die Anzahl der Indexblattseiten zurück, die aus dem Cache gelesen wurden.
<b>CacheReadTable</b>	Gibt die Anzahl der Tabellenseiten zurück, die aus dem Cache gelesen wurden.
<b>CacheReadWorkTable</b>	Gibt die Anzahl der Cache-Arbeitstabellen-Lesevorgänge zurück.
<b>CarverHeapPages</b>	Gibt die Anzahl der Blattseiten zurück, die für kurzzeitige Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.
<b>chained</b>	Gibt den Transaktionsmodus zurück, der beim Fehlen einer BEGIN TRANSACTION-Anweisung verwendet wird. Siehe „ <a href="#">chained-Option</a> “ auf Seite 587.

Eigenschaftsname	Beschreibung
<b>CharSet</b>	Gibt den von der Verbindung verwendeten CHAR-Zeichensatz zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „ <a href="#">CONNECTION_EXTENDED_PROPERTY-Funktion [Zeichenfolge]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>checkpoint_time</b>	Gibt die maximale Zeitspanne, in Minuten, zurück, die der Datenbankserver läuft, ohne einen Checkpoint auszuführen. Siehe „ <a href="#">checkpoint_time-Option</a> “ auf Seite 588.
<b>cis_option</b>	Gibt "7" zurück, wenn Fehlersuch-Informationen über den Ferndatenzugriff im Fenster "Servermeldungen" angezeigt werden, und "0", wenn diese Informationen nicht im Fenster "Servermeldungen" angezeigt werden. Siehe „ <a href="#">cis_option-Option</a> “ auf Seite 589.
<b>cis_rowset_size</b>	Gibt die Anzahl der Zeilen zurück, die vom Fremdserver bei jedem Abruf zurückgegeben werden. Siehe „ <a href="#">cis_rowset_size-Option</a> “ auf Seite 589.
<b>ClientLibrary</b>	Gibt jConnect bei jConnect-Verbindungen, CT_Library bei Sybase Open Client-Verbindungen, None bei HTTP-Verbindungen und CmdSeq bei ODBC-, Embedded SQL-, OLE DB-, ADO.NET- bzw. SQL Anywhere JDBC-Treiberverbindungen zurück.
<b>ClientNodeAddress</b>	Gibt den Knoten für den Client in einer Client/Server-Verbindung zurück. Wenn der Client und der Server auf demselben Computer sind, wird eine leere Zeichenfolge zurückgegeben. Dies ist ein Synonym für die Eigenschaft NodeAddress.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>ClientPort</b>	Gibt die TCP/IP-Portnummer des Clients oder "0" zurück, wenn die Verbindung keine TCP/IP-Verbindung ist.
<b>ClientStmtCacheHits</b>	Gibt die Anzahl der Vorbereitungen zurück, die aufgrund des Clientanweisungscache für diese Verbindung nicht erforderlich sind. Dies ist die Anzahl der Vorbereitungen, die erforderlich wären, wenn das clientseitige Caching von Anweisungen deaktiviert wäre. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.

Eigenschaftsname	Beschreibung
<b>ClientStmtCacheMisses</b>	Gibt die Anzahl der Anweisungen im Clientanweisungscache dieser Verbindung zurück, die erneut vorbereitet wurden. Dies ist die Angabe, wie oft eine zwischengespeicherte Anweisung für die Wiederverwendung in Frage kam, aber aufgrund einer Schemaänderung, einer Datenbank-Optionseinstellung oder einer DROP VARIABLE-Anweisung nicht wieder verwendet werden konnte. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>close_on_endtrans</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob Cursors am Ende einer Transaktion geschlossen werden. Siehe „ <a href="#">close_on_endtrans-Option</a> “ auf Seite 590.
<b>collect_statistics_on_dml_updates</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob Statistiken während der Ausführung von datenändernden DML-Anweisungen wie INSERT, DELETE und UPDATE gesammelt werden. Siehe „ <a href="#">collect_statistics_on_dml_updates-Option</a> “ auf Seite 591.
<b>Commit</b>	Gibt die Anzahl der Commit-Anforderungen zurück, die verarbeitet wurden.
<b>CommLink</b>	Gibt die Kommunikationsverbindung für die Verbindung zurück. Dies ist eines der von SQL Anywhere unterstützten Netzwerkprotokolle oder "local" bei einer Verbindung auf einem Computer.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>CommNetworkLink</b>	Gibt die Kommunikationsverbindung für die Verbindung zurück. Dies ist eines der von SQL Anywhere unterstützten Netzwerkprotokolle. Werte sind SharedMemory und TCPIP. Die Eigenschaft CommNetworkLink gibt immer den Namen der Verbindung zurück, unabhängig davon, ob es eine Verbindung auf einem Computer ist oder nicht.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>CommProtocol</b>	Gibt bei Sybase Open Client- bzw. jConnect-Verbindungen "TDS" zurück, bei HTTP-Verbindungen "HTTP", bei HTTPS-Verbindungen "HTTPS" sowie bei ODBC-, Embedded SQL-, OLE DB-, ADO.NET- und SQL Anywhere JDBC-Treiberverbindungen "CmdSeq".
<b>Compression</b>	Gibt "On" bzw. "Off" zurück, um anzuzeigen, ob die Kommunikationskomprimierung für die Verbindung aktiviert ist.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.

Eigenschaftsname	Beschreibung
<b>conn_auditing</b>	Gibt "On" zurück, wenn Auditing für die Verbindung aktiviert ist, auch wenn die Option auditing auf "Off" gesetzt ist. Siehe „ <a href="#">Auditing konfigurieren (Sybase Central)</a> “ auf Seite 1418 und „ <a href="#">conn_auditing-Option</a> “ auf Seite 592.
<b>ConnectedTime</b>	Gibt die Gesamtlänge der Zeit in Sekunden an, die eine Verbindung aktiv ist.
<b>connection_authentication</b>	Gibt die Zeichenfolge zurück, die zur Authentifizierung des Clients verwendet wird. Eine Authentifizierung ist erforderlich, bevor die Datenbank geändert werden kann. Siehe „ <a href="#">connection_authentication-Option</a> “ auf Seite 593.
<b>continue_after_raiserror</b>	Gibt "On" bzw. "Off" zurück, um anzuzeigen, ob die Ausführung einer Prozedur oder eines Triggers gestoppt wird, wenn die RAISERROR-Anweisung erkannt wird. Siehe „ <a href="#">continue_after_raiserror-Option</a> “ auf Seite 594.
<b>conversion_error</b>	Gibt "On" bzw. "Off" zurück, um anzuzeigen, dass Fehler beim Umwandeln von Datentypen gemeldet werden, wenn Informationen aus der Datenbank abgerufen werden. Siehe „ <a href="#">conversion_error-Option</a> “ auf Seite 595.
<b>cooperative_commit_timeout</b>	Gibt die Zeitspanne, in Millisekunden, zurück, die der Datenbankserver vor dem Schreiben auf die Festplatte wartet, bis andere Verbindungen eine Seite des Logs gefüllt haben. Siehe „ <a href="#">cooperative_commit_timeout-Option</a> “ auf Seite 596.
<b>cooperative_commits</b>	Gibt "On" bzw. "Off" zurück, um anzuzeigen, wann Festschreibungen auf die Festplatte geschrieben werden. Siehe „ <a href="#">cooperative_commits-Option</a> “ auf Seite 596.
<b>CurrentLineNumber</b>	Gibt die aktuelle Zeilennummer der Prozedur oder Kombinationsanweisung zurück, die eine Verbindung ausführt. Die Prozedur kann unter Verwendung der Eigenschaft CurrentProcedure identifiziert werden. Wenn die Zeile ein Bestandteil einer Kombinationsanweisung vom Client ist, wird eine leere Zeichenfolge zurückgegeben.
<b>CurrentProcedure</b>	Gibt den Namen der Prozedur zurück, die eine Verbindung derzeit ausführt. Wenn die Verbindung verschachtelte Prozeduraufrufe ausführt, ist der Name derjenige der aktuellen Prozedur. Wenn keine Prozedur ausgeführt wird, wird eine leere Zeichenfolge zurückgegeben.
<b>Cursor</b>	Gibt die Anzahl der deklarierten Cursor zurück, die derzeit vom Datenbankserver aufrechterhalten werden.

Eigenschaftsname	Beschreibung
<b>CursorOpen</b>	Gibt die Anzahl der offenen Cursor zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>database_authentication</b>	Gibt die Zeichenfolge zurück, die zur Authentifizierung der Datenbank verwendet wird. Eine Authentifizierung ist für authentifizierte Datenbankserver erforderlich, bevor die Datenbank geändert werden kann. Siehe <a href="#">„database_authentication-Option“ auf Seite 597</a> .
<b>date_format</b>	Gibt eine Zeichenfolge zurück, die das Format für Datumsangaben, die von der Datenbank abgerufen werden, angibt. Siehe <a href="#">„date_format-Option“ auf Seite 599</a> .
<b>date_order</b>	Gibt eine Zeichenfolge zurück, die angibt, wie Datumsangaben formatiert werden. Siehe <a href="#">„date_order-Option“ auf Seite 601</a> .
<b>db_publisher</b>	Gibt die Benutzer-ID für den Publikationseigentümer der Datenbank zurück. Siehe <a href="#">„db_publisher-Option“ auf Seite 602</a> .
<b>DBNumber</b>	Gibt die ID-Nummer der Datenbank zurück.
<b>debug_messages</b>	Gibt "On" oder "Off" zurück um anzuzeigen, ob MESSAGE-Anweisungen, die eine DEBUG ONLY-Klausel enthalten, ausgeführt werden. Siehe <a href="#">„debug_messages-Option“ auf Seite 602</a> .
<b>dedicated_task</b>	Gibt "On" oder "Off" zurück um anzuzeigen, ob eine Aufgabe zur Verarbeitung einer Anforderung exklusiv zugewiesen wird, um Anforderungen der Verbindung zu verarbeiten. Siehe <a href="#">„dedicated_task-Option“ auf Seite 603</a> .
<b>default_dbspace</b>	Gibt den Namen des Standard-DBSpaces oder eine leere Zeichenfolge zurück, wenn kein Standard-DBSpace angegeben wurde. Siehe <a href="#">„default_dbspace-Option“ auf Seite 604</a> .
<b>default_timestamp_increment</b>	Gibt einen Wert, in Mikrosekunden, zurück, der einer Spalte vom Typ TIMESTAMP hinzugefügt wird, um die Werte in der Spalte eindeutig zu halten. Siehe <a href="#">„default_timestamp_increment-Option“ auf Seite 605</a> .
<b>delayed_commit_timeout</b>	Gibt die Zeit, in Millisekunden, zurück, die der Datenbankserver wartet, bevor er nach einem COMMIT die Kontrolle an die Anweisung zurückgibt. Siehe <a href="#">„delayed_commit_timeout-Option“ auf Seite 606</a> .
<b>delayed_commits</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob der Datenbankserver nach einem COMMIT die Kontrolle an die Anweisung zurückgibt. Siehe <a href="#">„delayed_commits-Option“ auf Seite 606</a> .

Eigenschaftsname	Beschreibung
<b>disk_sandbox</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob Dateivorgänge der Datenbank mit Lese-/Schreibzugriff auf das Verzeichnis beschränkt sind, in dem sich die Hauptdatenbankdatei befindet. Siehe „ <a href="#">disk_sandbox-Option</a> “ auf Seite 608.
<b>DiskRead</b>	Gibt die Anzahl der Seiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadHint</b>	Gibt die Anzahl der Hints für Festplattenlesevorgänge zurück.
<b>DiskReadHintPages</b>	Gibt die Anzahl der Hintseiten für Festplattenlesevorgänge zurück.
<b>DiskReadIndInt</b>	Gibt die Anzahl der internen Knotenseiten des Indexes zurück, die von der Festplatte gelesen wurden.
<b>DiskReadIndLeaf</b>	Gibt die Anzahl der Indexblattseiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadTable</b>	Gibt die Anzahl der Tabellenseiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadWorkTable</b>	Gibt die Anzahl der Festplatten-Arbeitstabellen-Lesevorgänge zurück.
<b>DiskSyncRead</b>	Gibt die Anzahl der synchron ausgegebenen Festplattenlesevorgänge zurück.
<b>DiskSyncWrite</b>	Gibt die Anzahl der synchron ausgegebenen Schreibvorgänge zurück.
<b>DiskWaitRead</b>	Gibt zurück, wie oft der Datenbankserver auf einen asynchronen Lesevorgang gewartet hat.
<b>DiskWaitWrite</b>	Gibt zurück, wie oft der Datenbankserver auf einen asynchronen Schreibvorgang gewartet hat.
<b>DiskWrite</b>	Gibt die Anzahl der geänderten Seiten zurück, die auf die Festplatte geschrieben wurden.
<b>DiskWriteHint</b>	Gibt die Anzahl der Hints für Festplattenschreibvorgänge zurück.
<b>DiskWriteHintPages</b>	Gibt die Anzahl der Hintseiten für Festplattenschreibvorgänge zurück.
<b>divide_by_zero_error</b>	Gibt "On" zurück, wenn ein Teilen durch Null einen Fehler ergibt, und "Off", wenn dies nicht der Fall ist. Siehe „ <a href="#">divide_by_zero_error-Option</a> “ auf Seite 609.
<b>Encryption</b>	Gibt einen Wert zurück, der angibt, ob die Verbindung verschlüsselt ist. Siehe „ <a href="#">Verbindungsparameter Encryption (ENC)</a> “ auf Seite 359.

Eigenschaftsname	Beschreibung
<b>escape_character</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>EventName</b>	Gibt den Namen des zugeordneten Ereignisses zurück, wenn die Verbindung einen Event-Handler ausführt. Sonst wird eine leere Zeichenfolge zurückgegeben.
<b>exclude_operators</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>ExprCacheAbandons</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache aufgegeben wurde, weil die Trefferrate zu niedrig war.
<b>ExprCacheDropsToReadOnly</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache auf den schreibgeschützten Status zurückfiel, weil die Trefferrate niedrig war.
<b>ExprCacheEvicts</b>	Gibt die Anzahl der aus dem Ausdruckcache entfernten Einträge zurück.
<b>ExprCacheHits</b>	Gibt die Anzahl der Treffer im Ausdruckcache zurück.
<b>ExprCacheInserts</b>	Gibt die Anzahl der in den Ausdruckcache eingetragenen Werte zurück.
<b>ExprCacheLookups</b>	Gibt die Anzahl der Suchvorgänge im Ausdruckcache zurück.
<b>ExprCacheResumesOfReadWrite</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache in den schreibgeschützten Status wechselte, weil die Trefferrate zunahm.
<b>ExprCacheStarts</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache gestartet wurde.
<b>extended_join_syntax</b>	Gibt "On" (aktiviert) zurück, wenn Abfragen mit doppelter Korrelationsnamenssyntax für Multitable-Joins zulässig sind, und "Off" (deaktiviert), wenn sie als Fehler gemeldet werden. Siehe „ <a href="#">extended_join_syntax-Option</a> “ auf Seite 610.
<b>extern_login_credentials</b>	Gibt zurück, ob Verbindungen zu entfernten Datenbanken mit den Anmeldeinformationen für das externe Login des angemeldeten Benutzers oder den Anmeldeinformationen für das externe Login des effektiven Benutzers hergestellt werden. Siehe „ <a href="#">extern_login_credentials-Option</a> “ auf Seite 611.
<b>fire_triggers</b>	Gibt "On" zurück, wenn Trigger in der Datenbank ausgelöst werden. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">fire_triggers-Option</a> “ auf Seite 612.

Eigenschaftsname	Beschreibung
<b>first_day_of_week</b>	Gibt die Ziffer zurück, die für den ersten Wochentag verwendet wird, wobei 7=Sonntag und 1=Montag ist. Siehe „ <a href="#">first_day_of_week-Option</a> “ auf Seite 613.
<b>for_xml_null_treatment</b>	Gibt "Omit" zurück, wenn Elemente und Attribute, die NULL enthalten, aus dem Ergebnis ausgeklammert werden, und "Empty", wenn leere Elemente oder Attribute für NULL erstellt werden, weil die FOR XML-Klausel in einer Abfrage verwendet wird. Siehe „ <a href="#">for_xml_null_treatment-Option</a> “ auf Seite 614.
<b>force_view_creation</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>FullCompare</b>	Gibt die Anzahl der Vergleiche zurück, die über den Hash-Wert hinaus in einem Index durchgeführt wurden.
<b>GetData</b>	Gibt die Anzahl der GETDATA-Anforderungen zurück.
<b>global_database_id</b>	Gibt den Startwert bei Spalten zurück, die mit DEFAULT GLOBAL AUTOINCREMENT erstellt wurden. Siehe „ <a href="#">global_database_id-Option</a> “ auf Seite 614.
<b>HashForcedPartitions</b>	Gibt die Häufigkeit zurück, mit der ein Hash-Operator zur Teilung gezwungen war, weil um Speicher konkurriert wurde.
<b>HashRowsFiltered</b>	Gibt die Anzahl der von Bitvektorfiltren zurückgewiesenen Suchzeilen zurück.
<b>HashRowsPartitioned</b>	Gibt die Anzahl der in Hash-Arbeitstabellen geschriebenen Zeilen zurück.
<b>HashWorkTables</b>	Gibt die Anzahl der für Hash-basierte Vorgänge erstellten Arbeitstabellen zurück.
<b>HeapsCarver</b>	Gibt die Anzahl der Heaps zurück, die für kurzzeitige Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.
<b>HeapsLocked</b>	Gibt die Anzahl von neu positionierbaren, derzeit im Cache gesperrten Heaps zurück.
<b>HeapsQuery</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Heaps zurück.
<b>HeapsRelocatable</b>	Gibt die Anzahl von neu positionierbaren Heaps zurück.
<b>http_connection_pool_basesize</b>	Gibt die nominale Schwellenwertgröße von Datenbankverbindungen zurück. Siehe „ <a href="#">http_connection_pool_basesize-Option</a> “ auf Seite 615.

Eigenschaftsname	Beschreibung
<b>http_connecti-on_pool_timeout</b>	Gibt die maximale Zeitdauer an, über die nicht benutzte Verbindungen im Verbindungspool gespeichert werden. Siehe „ <a href="#">http_connecti-on_pool_timeout-Option</a> “ auf Seite 616.
<b>http_session_timeout</b>	Gibt das aktuelle Timeout für HTTP-Sitzungen in Minuten zurück. Siehe „ <a href="#">http_session_timeout</a> “ auf Seite 617.
<b>HttpServiceName</b>	Gibt den Namen des Dienst-Eintrittspunkts für die aktuelle HTTP-Anforderung an. Diese Eigenschaft ist bei der Fehler-Berichterstellung und der Datenflusssteuerung nützlich. Es wird eine leere Zeichenfolge zurückgegeben, wenn diese Eigenschaft in einer gespeicherten Prozedur enthalten ist, die nicht von einer HTTP-Anforderung stammt, oder wenn die Verbindung derzeit inaktiv ist oder auf die Fortsetzung einer HTTP-Sitzung wartet.
<b>IdleTimeout</b>	<p>Gibt den Wert für das Inaktivitäts-Timeout der Verbindung zurück. Siehe „<a href="#">Verbindungsparameter Idle</a>“ auf Seite 365.</p> <p>Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.</p>
<b>IndAdd</b>	Gibt die Anzahl der Einträge zurück, die Indizes hinzugefügt wurden.
<b>IndLookup</b>	Gibt die Anzahl der Einträge zurück, nach denen in Indizes gesucht wurde.
<b>integrated_server_name</b>	Gibt den Namen des Domain Controller-Servers zurück, der bei integrierten Logins zum Nachschlagen von Windows-Benutzergruppenmitgliedschaften verwendet wird. Siehe „ <a href="#">integrated_server_name-Option</a> “ auf Seite 618.
<b>IsDebugger</b>	Gibt "Yes" oder "No" zurück, um Verbindungen zu unterscheiden, die verwendet werden, um den SQL Anywhere Debugger auszuführen. Der Wert ist "Yes", wenn die aktuelle Verbindungsnummer der Verbindungsnummer einer Debugger-Verbindung entspricht, und "No" im gegenteiligen Fall. Siehe „ <a href="#">SQL Anywhere-Debugger</a> “ [ <i>SQL Anywhere Server - SQL-Benutzerhandbuch</i> ].
<b>isolation_level</b>	Gibt die Isolationsstufe der Verbindung (0, 1, 2, 3, Snapshot, Anweisungs-Snapshot oder Readonly-Anweisungs-Snapshot) zurück. Siehe „ <a href="#">isolation_level-Option</a> “ auf Seite 619.
<b>java_class_path</b>	Gibt eine Liste von zusätzlichen Verzeichnissen oder JAR-Dateien zurück, die nach Klassen durchsucht werden. Siehe „ <a href="#">java_class_path-Option</a> “ auf Seite 620.

Eigenschaftsname	Beschreibung
<b>java_location</b>	Gibt den Pfad der Java VM für die Datenbank zurück, falls einer angegeben wurde. Siehe „ <a href="#">java_location-Option</a> “ auf Seite 621.
<b>java_main_userid</b>	Diese Eigenschaft ist veraltet.
<b>java_vm_options</b>	Gibt die Befehlszeilenoptionen zurück, die der Datenbankserver verwendet, wenn er die Java VM startet. Siehe „ <a href="#">java_vm_options-Option</a> “ auf Seite 622.
<b>Language</b>	Gibt die Sprachumgebungsprache zurück.
<b>LastCommitRedoPos</b>	Gibt die Wiederherstellungslog-Position zurück, nachdem der letzte COMMIT-Vorgang von der Verbindung in das Transaktionslog geschrieben wurde.
<b>LastIdle</b>	Gibt die Anzahl der Computertakte zwischen Anforderungen zurück.
<b>LastPlanText</b>	Gibt den ausführlichen Textplan der letzten auf der Verbindung ausgeführten Abfrage zurück. Sie steuern die Verfügbarkeit des letzten Plans, indem Sie die Option RememberLastPlan der sa_server_option-Systemprozedur setzen oder die Serveroption -zp verwenden. Siehe „ <a href="#">Datenbankserveroption -zp</a> “ auf Seite 316.
<b>LastReqTime</b>	Gibt den Zeitpunkt zurück, an dem die letzte Anforderung für die angegebene Verbindung gestartet wurde. Diese Eigenschaft kann eine leere Zeichenfolge für interne Verbindungen wie zum Beispiel Ereignisse zurückgeben.
<b>LastStatement</b>	<p>Gibt die zuletzt vorbereitete SQL-Anweisung für die aktuelle Verbindung zurück.</p> <p>Der LastStatement-Wert wird gesetzt, wenn eine Anweisung vorbereitet wird, und gelöscht, wenn eine Anweisung gelöscht wird. Bei jeder Verbindung ist jeweils nur eine Anweisungszeichenfolge verfügbar.</p> <p>Wenn sa_conn_activity einen nicht-leeren Wert für eine Verbindung meldet, ist dies höchstwahrscheinlich die Anweisung, die die Verbindung derzeit ausführt. Wenn die Anweisung abgeschlossen wäre, wäre sie wahrscheinlich gelöscht und der Eigenschaftswert bereinigt worden. Wenn eine Anwendung mehrere Anweisungen vorbereitet und ihre Anweisungs-Handles beibehält, spiegelt der LastStatement-Wert nicht wieder, was eine Verbindung derzeit ausführt.</p> <p>Wenn das clientseitige Caching von Anweisungen aktiviert ist und eine zwischengespeicherte Anweisung wieder verwendet wird, gibt diese Eigenschaft eine leere Zeichenfolge zurück.</p>

Eigenschaftsname	Beschreibung
<b>LivenessTimeout</b>	Gibt die Zeitspanne für das Verfügbarkeits-Timeout der aktuellen Verbindung zurück. Siehe „ <a href="#">LivenessTimeout-Verbindungsparameter (LTO)</a> “ auf Seite 370.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>lock_rejected_rows</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>LockCount</b>	Gibt die Anzahl der von der Verbindung gehaltenen Sperren zurück.
<b>LockIndexID</b>	Gibt den Bezeichner der gesperrten Indexes zurück.
<b>LockName</b>	Gibt einen 64-Bit-Ganzzahlwert ohne Vorzeichen zurück, der die Sperre darstellt, auf die eine Verbindung wartet.
<b>LockRowID</b>	Gibt den Bezeichner der gesperrten Zeile zurück.
<b>LockTableOID</b>	Gibt Null zurück, wenn die Verbindung nicht blockiert ist oder die Verbindung mit einer anderen Datenbank besteht als die Verbindung, die CONNECTION_PROPERTY aufruft. Anderenfalls ist dies die Objekt-ID der Tabelle für die Sperre, bei der die Verbindung wartet. Die Objekt-ID kann verwendet werden, um mithilfe der Systemansicht SYSTAB Tabelleninformationen nachzuschlagen. Siehe „ <a href="#">SYSTAB-Systemansicht</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>log_deadlocks</b>	Gibt "On" zurück, wenn Deadlock-Informationen gemeldet werden. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">log_deadlocks-Option</a> “ auf Seite 623.
<b>LogFreeCommit</b>	Gibt die Anzahl der Redo Free Commits zurück. Ein Redo Free Commit tritt auf, wenn das Festschreiben des Transaktionslogs verlangt wurde, das Log aber schon geschrieben ist (das Festschreiben war daher umsonst).
<b>login_mode</b>	Gibt einen oder mehrere der Werte "Standard", "Integrated", "Kerberos", "CloudAdmin" oder "LDAPUA" zurück, um die unterstützten Login-Typen anzuzeigen. Siehe „ <a href="#">login_mode-Option</a> “ auf Seite 623.
<b>login_procedure</b>	Gibt den Namen der gespeicherten Prozedur zurück, die beim Start zum Setzen von Kompatibilitätsoptionen verwendet wurde. Siehe „ <a href="#">login_procedure-Option</a> “ auf Seite 625.
<b>LoginTime</b>	Gibt das Datum und die Uhrzeit zurück, zu der die Verbindung hergestellt wurde.

Eigenschaftsname	Beschreibung
<b>LogWrite</b>	Gibt die Anzahl der Seiten zurück, die in das Transaktionslog geschrieben wurden.
<b>materialized_view_optimization</b>	<p>Gibt einen Wert zurück, der angibt, ob materialisierte Ansichten während der Abfrageoptimierung verwendet werden:</p> <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Fresh</li> <li>• Stale</li> <li>• N Minute[s]</li> <li>• N Hour[s]</li> <li>• N Day[s]</li> <li>• N Week[s]</li> <li>• N Month[s]</li> </ul> <p>Siehe „<a href="#">materialized_view_optimization-Option</a>“ auf Seite 628.</p>
<b>max_client_statements_cached</b>	Gibt die Anzahl der Anweisungen zurück, die vom Client im Cache gehalten werden. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>max_cursor_count</b>	Gibt einen Wert zurück, der die maximale Anzahl von Cursors angibt, die eine Verbindung gleichzeitig verwenden kann. Siehe „ <a href="#">max_cursor_count-Option</a> “ auf Seite 631.
<b>max_hash_size</b>	Diese Eigenschaft ist veraltet.
<b>max_plans_cached</b>	Gibt einen Wert zurück, der die maximale Anzahl der Ausführungspläne angibt, die in einem Cache gespeichert werden können. Siehe „ <a href="#">max_plans_cached-Option</a> “ auf Seite 632.
<b>max_priority</b>	Gibt einen Wert zurück, der die maximale Prioritätsstufe angibt, die eine Verbindung haben kann. Siehe „ <a href="#">max_priority-Option</a> “ auf Seite 632.
<b>max_query_tasks</b>	Gibt die maximale Anzahl von Anforderungen zurück, die der Datenbankserver zur Verarbeitung einer Abfrage verwenden kann. Siehe „ <a href="#">max_query_tasks-Option</a> “ auf Seite 633.
<b>max_recursive_iterations</b>	Gibt einen Wert zurück, der die maximale Anzahl der Wiederholungen angibt, die ein rekursiver allgemeiner Tabellenausdruck durchführen kann. Siehe „ <a href="#">max_recursive_iterations-Option</a> “ auf Seite 634.
<b>max_statement_count</b>	Gibt einen Wert zurück, der die maximale Anzahl von vorbereiteten Anweisungen angibt, die eine Verbindung gleichzeitig verwenden kann. Siehe „ <a href="#">max_statement_count-Option</a> “ auf Seite 635.

Eigenschaftsname	Beschreibung
<b>max_temp_space</b>	Gibt einen Wert zurück, der die maximale Menge von Speicher für temporäre Dateien angibt, der einer Verbindung zur Verfügung steht. Siehe <a href="#">„max_temp_space-Option“ auf Seite 636</a> .
<b>MessageReceived</b>	Gibt die Zeichenfolge zurück, die von der MESSAGE-Anweisung generiert wurde, die bewirkt hat, dass die WAITFOR-Anweisung unterbrochen wurde. Sonst wird eine leere Zeichenfolge zurückgegeben.
<b>min_password_length</b>	Gibt die Mindestlänge für neue Kennwörter in der Datenbank zurück. Siehe <a href="#">„min_password_length-Option“ auf Seite 637</a> .
<b>min_role_admins</b>	Gibt die minimale Anzahl von Administratoren zurück, die für eine Rolle erforderlich ist. Siehe <a href="#">„min_role_admins-Option“ auf Seite 638</a> .

Eigenschaftsname	Beschreibung
<b>Name</b>	<p>Gibt den Namen der aktuellen Verbindung zurück.</p> <p>Sie können einen Verbindungsnamen mit dem ConnectionName (CON)-Verbindungsparameter angeben. Siehe „<a href="#">Verbindungsparameter ConnectionName (CON)</a>“ auf Seite 349.</p> <p>Die folgenden Namen werden für temporäre Verbindungen verwendet, die vom Datenbankserver erstellt werden:</p> <ul style="list-style-type: none"> <li>• INT:ApplyRecovery</li> <li>• INT:BackupDB</li> <li>• INT:Checkpoint</li> <li>• INT:Cleaner</li> <li>• INT:CloseDB</li> <li>• INT&gt;CreateDB</li> <li>• INT&gt;CreateMirror</li> <li>• INT:DelayedCommit</li> <li>• INT:DiagRcvr</li> <li>• INT:DropDB</li> <li>• INT:EncryptDB</li> <li>• INT:Exchange</li> <li>• INT:FlushMirrorLog</li> <li>• INT:FlushStats</li> <li>• INT:HTTPReq</li> <li>• INT:PromoteMirror</li> <li>• INT:PurgeSnapshot</li> <li>• INT:ReconnectMirror</li> <li>• INT:RecoverMirror</li> <li>• INT:RedoCheckpoint</li> <li>• INT:RefreshIndex</li> <li>• INT:ReloadTrigger</li> <li>• INT:RenameMirror</li> <li>• INT:RestoreDB</li> <li>• INT:StartDB</li> <li>• INT:VSS</li> </ul> <p>Siehe „<a href="#">Temporäre Verbindungen</a>“ auf Seite 78.</p>
<b>NcharCharSet</b>	<p>Gibt den von der Verbindung verwendeten NCHAR-Zeichensatz zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">CONNECT-ON_EXTENDED_PROPERTY-Funktion [Zeichenfolge]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>

Eigenschaftsname	Beschreibung
<b>nearest_century</b>	Gibt einen Wert zurück, der angibt, wie zweistellige Jahresangaben bei Konvertierungen von Zeichenfolgen in Datumsangaben interpretiert werden. Siehe „nearest_century-Option“ auf Seite 640.
<b>NodeAddress</b>	Gibt den Knoten für den Client in einer Client/Server-Verbindung zurück. Wenn der Client und der Server auf demselben Computer sind, wird eine leere Zeichenfolge zurückgegeben.
<b>non_keywords</b>	Gibt ggf. eine Liste von Schlüsselwörtern zurück, die deaktiviert sind, um als Bezeichner verwendet werden zu können. Siehe „non_keywords-Option“ auf Seite 641.
<b>Number</b>	Gibt die Verbindungs-ID (eine Nummer) für die aktuelle Verbindung zurück.
<b>NumLocalTempTables</b>	Gibt die Anzahl der lokalen temporären Tabellen zurück, die von der Verbindung verwendet werden. Wenn eine lokale temporäre Tabelle gelöscht wird oder aus dem gültigen Bereich herausfällt, gilt sie bis zum nächsten COMMIT-Vorgang weiterhin als verwendet.
<b>odbc_describe_binary_as_varbinary</b>	Gibt "Off" zurück, wenn der SQL Anywhere ODBC-Treiber BINARY- und VARBINARY-Spalten als SQL_BINARY beschreibt, und "On", wenn der ODBC-Treiber BINARY- und VARBINARY-Spalten als SQL_VARBINARY beschreibt. Siehe „odbc_describe_binary_as_varbinary“ auf Seite 642.
<b>odbc_distinguish_char_and_varchar</b>	Gibt "Off" zurück, wenn CHAR-Spalten als SQL_VARCHAR beschrieben werden, und "On", wenn CHAR-Spalten als SQL_CHAR beschrieben werden. Siehe „odbc_distinguish_char_and_varchar-Option“ auf Seite 642.
<b>oem_string</b>	Gibt die Zeichenfolge zurück, die in der Header-Seite der Datenbankdatei gespeichert ist. Siehe „oem_string-Option“ auf Seite 643.
<b>on_charset_conversion_failure</b>	Gibt "Ignore", "Warning" oder "Error" zurück, um das Verhalten anzuzeigen, wenn ein Fehler während der Zeichensatzkonvertierung auftritt. Siehe „on_charset_conversion_failure-Option“ auf Seite 645.
<b>on_tsql_error</b>	Gibt "Stop", "Conditional" oder "Continue" zurück, um das Verhalten anzuzeigen, wenn ein Fehler während der Ausführung einer gespeicherten Prozedur oder eines T-SQL-Batch auftritt. Siehe „on_tsql_error-Option“ auf Seite 646.
<b>optimization_goal</b>	Gibt entweder "First-row" oder "All-rows" zurück, um anzuzeigen, wie die Abfrageverarbeitung optimiert wird. Siehe „optimization_goal-Option“ auf Seite 647.

Eigenschaftsname	Beschreibung
<b>optimization_level</b>	Gibt einen Wert zwischen 0 und 15 aus. Diese Zahl wird verwendet, um den vom SQL Anywhere-Abfrageoptimierer getätigten Aufwand zum Finden eines Zugriffplans für eine SQL-Anweisung zu steuern. Siehe „ <a href="#">optimization_level-Option</a> “ auf Seite 648.
<b>optimization_workload</b>	Gibt einen Wert zurück, der den vom SQL Anywhere-Abfrageoptimierer getätigten Aufwand zum Finden eines Zugriffplans für eine SQL-Anweisung anzeigt. Siehe „ <a href="#">optimization_workload-Option</a> “ auf Seite 649.
<b>OSUser</b>	Gibt den Betriebssystem-Benutzernamen zurück, der dem Clientprozess zugewiesen ist. Wenn der Clientprozess einen anderen Benutzer impersoniert (oder das gesetzte ID-Bit auf Unix gesetzt ist), wird der Name des impersonierten Benutzers zurückgegeben. Für Clients der Version 10.0.1 und früher sowie auch für HTTP- und TDS-Clients wird eine leere Zeichenfolge zurückgegeben.
<b>PacketSize</b>	Gibt die Paketgröße (in Byte) zurück, die von der Verbindung verwendet wird.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>PacketsReceived</b>	Gibt die Anzahl der empfangenen Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsReceivedUncomp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommunikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsReceived", wenn die Komprimierung deaktiviert ist.)
<b>PacketsSent</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsSentUncomp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommunikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsSent", wenn die Komprimierung deaktiviert ist.)
<b>ParentConnection</b>	Gibt die Verbindungs-ID der Verbindung an, die eine temporäre Verbindung für die Ausführung eines Datenbankvorgangs erstellt hat (wie etwa die Durchführung einer Sicherung oder das Erstellen einer Datenbank). Bei anderen Typen von Verbindungen gibt diese Eigenschaft NULL zurück.

Eigenschaftsname	Beschreibung
<b>pinned_cursor_percent_of_cache</b>	Gibt den Prozentsatz des Caches zurück, der für die Bereithaltung von Cursorsn benutzt werden kann. Siehe „ <a href="#">pinned_cursor_percent_of_cache-Option</a> “ auf Seite 650.
<b>post_login_procedure</b>	Gibt den Namen der Prozedur zurück, deren Ergebnismenge Meldungen enthält, die von Anwendungen angezeigt werden sollen, wenn ein Benutzer eine Verbindung herstellt. Siehe „ <a href="#">post_login_procedure-Option</a> “ auf Seite 651.
<b>precision</b>	Gibt die Einstellung für die dezimale und numerische Gesamtstellenzahl zurück. Siehe „ <a href="#">precision-Option</a> “ auf Seite 653.
<b>prefetch</b>	Gibt "Off" zurück, wenn kein Prefetch durchgeführt wird. Gibt "Conditional" zurück, wenn ein Prefetch durchgeführt wird, außer der Cursortyp ist SENSITIVE oder die Abfrage enthält eine Proxytabelle. Gibt "Always" zurück, wenn ein Prefetch selbst bei SENSITIVE-Cursortypen und bei Cursorsn durchgeführt wird, die eine Proxytabelle betreffen. Siehe „ <a href="#">prefetch-Option</a> “ auf Seite 653.
<b>Prepares</b>	Gibt die Anzahl von Anweisungsvorbereitungen zurück, die für die Verbindung durchgeführt wurden.
<b>PrepStmt</b>	Gibt die Anzahl der vorbereiteten Anweisungen zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>preserve_source_format</b>	Gibt "On" zurück, wenn die Original-Quellendefinition von Prozeduren, Triggern, Ansichten und Event-Handlern in Systemtabellen gespeichert werden. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">preserve_source_format-Option</a> “ auf Seite 655.
<b>prevent_article_pkey_update</b>	Gibt "On" zurück, wenn Aktualisierungen von Primärschlüsselspalten der Tabellen, die in Publikationen einbezogen sind, nicht zulässig sind. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">prevent_article_pkey_update-Option</a> “ auf Seite 655.
<b>priority</b>	Gibt einen Wert zurück, der die Prioritätsstufe einer Verbindung angibt. Siehe „ <a href="#">priority-Option</a> “ auf Seite 656.

Eigenschaftsname	Beschreibung
<b>Progress</b>	<p>Gibt Informationen darüber zurück, wie lange eine Abfrage gelaufen ist. Zum Beispiel:</p> <pre>43% (9728 of 22230 pages) complete after 00:00:05; estimated 00:00:06 remaining</pre> <p>Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">CONNECTION_EXTENDED_PROPERTY-Funktion [Zeichenfolge]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>
<b>progress_messages</b>	Gibt den Wert für die progress_messages-Option zurück. Siehe „ <a href="#">progress_messages-Option</a> “ auf Seite 657.
<b>query_mem_timeout</b>	Gibt den Wert der Option query_mem_timeout zurück. Siehe „ <a href="#">query_mem_timeout-Option</a> “ auf Seite 659.
<b>QueryBypassed</b>	Gibt die Anzahl der Anforderungen zurück, die durch den Bypass-Mechanismus des Optimierers optimiert wurden.
<b>QueryBypassedCosted</b>	Gibt die Anzahl von Anforderungen zurück, die vom Optimierer-Bypass mit Kostenermittlung verarbeitet wurden.
<b>QueryBypassedHeuristic</b>	Gibt die Anzahl von Anforderungen zurück, die vom Optimierer-Bypass mit Heuristik verarbeitet wurden.
<b>QueryBypassedOptimized</b>	Gibt die Anzahl von Anforderungen zurück, die ursprünglich vom Optimierer-Bypass verarbeitet und danach vom SQL Anywhere-Optimierer voll optimiert wurden.
<b>QueryCachedPlans</b>	Gibt die Anzahl der Ausführungspläne für Abfragen zurück, die derzeit für die Verbindung im Cache gehalten werden.
<b>QueryCachePages</b>	Gibt die Anzahl der Cacheseiten zurück, die benutzt wurden, um Ausführungspläne im Cache zu halten.
<b>QueryDescribedBypass</b>	Gibt die Anzahl der Anforderungen zurück, die vom Optimierer-Bypass verarbeitet wurden.
<b>QueryDescribedOptimizer</b>	Gibt die Anzahl der Anforderungen zurück, die vom Optimierer verarbeitet wurden.
<b>QueryHeapPages</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Cacheseiten zurück.

Eigenschaftsname	Beschreibung
<b>QueryJHToJNLOptUsed</b>	Gibt die Häufigkeit zurück, mit der ein Hash-Join in einen Nested Loops Join umgewandelt wurde.
<b>QueryLowMemoryStrategy</b>	Gibt die Häufigkeit zurück, mit der der Server wegen Speichermangels seinen Ausführungsplan geändert hat. Die Strategie kann sich ändern, weil weniger Speicher als vom Optimierer geschätzt verfügbar ist, oder weil der Ausführungsplan mehr Speicher beansprucht, als der Optimierer geschätzt hat.
<b>QueryMemActiveCurr</b>	Gibt die Anzahl der Anforderungen zurück, die den Abfragespeicher aktiv nutzen.
<b>QueryMemGrantFailed</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Zuweisung von Abfragespeicher gewartet, aber nicht erhalten hat.
<b>QueryMemGrantGranted</b>	Gibt die Anzahl der Seiten zurück, die derzeit für Anforderungen bereitgestellt sind.
<b>QueryMemGrantRequested</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt versucht hat, Abfragespeicher zu erhalten.
<b>QueryMemGrantWaited</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Speicherzuordnung gewartet hat.
<b>QueryMemGrantWaiting</b>	Gibt die aktuelle Anzahl der Anforderungen zurück, die auf Zuweisung von Abfragespeicher warten.
<b>QueryOpened</b>	Gibt die Anzahl der OPEN-Anforderungen für die Ausführung zurück.
<b>QueryOptimized</b>	Gibt die Anzahl der vollständig optimierten Anforderungen zurück.
<b>QueryReused</b>	Gibt die Anzahl der Anforderungen zurück, die aus dem Plancache wieder verwendet wurden.
<b>QueryRowsFetched</b>	Gibt die Anzahl der Zeilen zurück, die aus den Basistabellen über einen sequenziellen Scan oder einen Index-Scan für diese Verbindung gelesen wurden.
<b>QueryRowsMaterialized</b>	Gibt die Anzahl der Zeilen zurück, die während der Abfrageverarbeitung in Arbeitstabellen geschrieben werden.
<b>quoted_identifier</b>	Gibt "On" zurück, wenn in Anführungszeichen eingeschlossene Zeichenfolgen als Bezeichner interpretiert werden, oder "Off", wenn sie als Literal-Zeichenfolgen interpretiert werden. Siehe „ <a href="#">quoted_identifier-Option</a> “ auf Seite 660.

Eigenschaftsname	Beschreibung
<b>read_past_deleted</b>	Gibt "On" zurück, wenn sequenzielle Scans auf Isolationsstufe 1 und 2 nicht festgeschriebene gelöschte Zeilen überspringen, und "Off", wenn sequenzielle Scans bei nicht festgeschriebenen gelöschten Zeilen auf Isolationsstufe 1 und 2 blockieren. Siehe „ <a href="#">read_past_deleted-Option</a> “ auf Seite 661.
<b>recovery_time</b>	Gibt die maximale Zeitdauer in Minuten zurück, die dem Datenbankserver zum Wiederherstellen nach einem Systemausfall zur Verfügung steht. Siehe „ <a href="#">recovery_time-Option</a> “ auf Seite 661.
<b>RecursiveIterations</b>	Gibt die Anzahl von Wiederholungen für rekursive Vereinigungen zurück.
<b>RecursiveIterationsHash</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join eine Hash-Strategie verwendet hat.
<b>RecursiveIterationsNested</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join eine Nested Loops-Strategie verwendet hat.
<b>RecursiveJNLMisses</b>	Gibt die Anzahl der Indexsuche-Cachefehlschläge für rekursive Hash-Joins zurück.
<b>RecursiveJNLProbes</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join eine Indexsuche versucht hat.
<b>remote_idle_timeout</b>	Gibt die Zeitspanne, in Sekunden, der Inaktivität zurück, die Webdienst-Clientprozeduren und -funktionen tolerieren werden. Siehe „ <a href="#">remote_idle_timeout-Option</a> “ auf Seite 662.
<b>replicate_all</b>	Wird nur intern verwendet.
<b>ReqCountActive</b>	Gibt die Anzahl der verarbeiteten Anforderungen zurück, oder NULL, wenn die Servereigenschaft RequestTiming auf "Off" gesetzt ist. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountBlockContenti-on</b>	Gibt die Häufigkeit zurück, mit der die Verbindung auf einen unteilbaren Zugriff gewartet hat, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountBlockIO</b>	Gibt die Häufigkeit zurück, mit der die Verbindung auf den Abschluss von I/O-Vorgängen gewartet hat, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountBlockLock</b>	Gibt die Häufigkeit zurück, mit der die Verbindung auf eine Sperre gewartet hat, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.

Eigenschaftsname	Beschreibung
<b>ReqCountUnscheduled</b>	Gibt die Häufigkeit zurück, mit der die Verbindung auf einen Zeitplan gewartet hat, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „Datenbankserveroption -zt“ auf Seite 319.
<b>ReqStatus</b>	<p>Gibt den Status der Anforderung zurück. Dies kann einer der folgenden Werte sein:</p> <ul style="list-style-type: none"> <li>• <b>Idle</b> Die Verbindung verarbeitet derzeit keine Anforderung.</li> <li>• <b>Unscheduled*</b> Die Verbindung hat Arbeit und wartet auf einen verfügbaren Datenbankserver-Worker.</li> <li>• <b>BlockedIO*</b> Die Verbindung ist beim Warten auf einen I/O-Vorgang blockiert.</li> <li>• <b>BlockedContention*</b> Die Verbindung ist blockiert, weil sie auf den Zugriff auf gemeinsam genutzte Datenstrukturen des Datenbankservers wartet.</li> <li>• <b>BlockedLock</b> Die Verbindung ist beim Warten auf eine gesperrtes Objekt blockiert.</li> <li>• <b>Executing</b> Die Verbindung führt eine Anforderung aus.</li> </ul> <p>Die mit einem Stern (*) markierten Werte werden nur zurückgegeben, wenn die Protokollierung der Anforderungszeitinformationen beim Datenbankserver unter Verwendung der Serveroption -zt aktiviert ist. Wenn keine Anforderungszeitinformationen protokolliert werden (Standardeinstellung), werden die Werte als "Executing" gemeldet.</p> <p>Siehe „Datenbankserveroption -zt“ auf Seite 319.</p>
<b>ReqTimeActive</b>	Gibt die bei der Verarbeitung von Anforderungen verstrichene Zeit in Sekunden zurück oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „Datenbankserveroption -zt“ auf Seite 319.
<b>ReqTimeBlockContention</b>	Gibt die beim Warten auf einen atomaren Zugriff verstrichene Zeit in Sekunden zurück oder NULL, wenn die RequestTiming-Serveigenschaft auf "Off" gesetzt ist. Siehe „Datenbankserveroption -zt“ auf Seite 319.
<b>ReqTimeBlockIO</b>	Gibt die beim Warten auf den Abschluss von I/O-Vorgängen verstrichene Zeit in Sekunden zurück oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „Datenbankserveroption -zt“ auf Seite 319.

Eigenschaftsname	Beschreibung
<b>ReqTimeBlockLock</b>	Gibt die beim Warten auf eine Sperre verstrichene Zeit in Sekunden zurück oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe <a href="#">„Datenbankserveroption -zt“ auf Seite 319</a> .
<b>ReqTimeUnscheduled</b>	Gibt die Menge der Wartezeit ohne Zeitplanung zurück, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe <a href="#">„Datenbankserveroption -zt“ auf Seite 319</a> .
<b>ReqType</b>	Gibt den Typ der letzten Anforderung zurück. Wenn eine Verbindung vom Verbindungspooling im Cache abgelegt wurde, lautet ihr Req-Type-Wert CONNECT_POOL_CACHE.
<b>request_timeout</b>	Gibt die maximale Zeit zurück, die eine einzelne Anforderung benötigen darf. Siehe <a href="#">„request_timeout-Option“ auf Seite 664</a> .
<b>RequestsReceived</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationsanforderungen oder Roundtrips zurück. Dies unterscheidet sich von PacketsReceived, da Mehrfachpaketanforderungen als eine Anforderung zählen und Verfügbarkeitspakete nicht aufgenommen werden.
<b>reserved_keywords</b>	Gibt eine Liste von standardmäßig reservierten Schlüsselwörtern zurück die für die Datenbank aktiviert sind. Siehe <a href="#">„reserved_keywords-Option“ auf Seite 665</a> .
<b>return_date_time_as_string</b>	Gibt "On" zurück, wenn DATE-, TIME- und TIMESTAMP-Werte als Zeichenfolge an Anwendungen zurückgegeben werden, und "Off", wenn sie als DATE- oder TIME-Datentyp zurückgegeben werden. Siehe <a href="#">„return_date_time_as_string-Option“ auf Seite 666</a> .
<b>Rlbk</b>	Gibt die Anzahl der Rollback-Anforderungen zurück, die verarbeitet wurden.
<b>rollback_on_deadlock</b>	Gibt "After" zurück, wenn Aktionen der referenziellen Integrität nach UPDATE oder DELETE ausgeführt werden, und "Before", wenn sie vor UPDATE oder DELETE ausgeführt werden. Siehe <a href="#">„rollback_on_deadlock-Option“ auf Seite 666</a> .
<b>RollbackLogPages</b>	Gibt die Anzahl der Seiten im Rollback-Log zurück.
<b>row_counts</b>	Gibt "On" zurück, wenn die Zeilenanzahl immer genau ist, und "Off", wenn die Zeilenanzahl üblicherweise eine Schätzung ist. Siehe <a href="#">„row_counts-Option“ auf Seite 667</a> .
<b>scale</b>	Gibt die dezimalen und numerischen Dezimalstellen für die Verbindung zurück. Siehe <a href="#">„scale-Option“ auf Seite 668</a> .

Eigenschaftsname	Beschreibung
<b>secure_feature_key</b>	Speichert den Schlüssel, der verwendet wird, um Funktionen für einen Datenbankserver zu aktivieren und zu deaktivieren. Die Auswahl des Werts dieser Eigenschaft gibt stets eine leere Zeichenfolge zurück.
<b>ServerNodeAddress</b>	Gibt den Knoten für den Server in einer Client/Server-Verbindung zurück. Wenn der Client und der Server auf demselben Computer sind, wird eine leere Zeichenfolge zurückgegeben.  Diese Eigenschaft gibt <b>NA</b> zurück, wenn die derzeit ausgeführte Anforderung Teil eines Event-Handlers ist.
<b>ServerPort</b>	Gibt die TCP/IP-Portnummer des Datenbankservers zurück, oder "0".
<b>SessionCreateTime</b>	Gibt die Uhrzeit zurück, zu der die HTTP-Sitzung erstellt wurde.
<b>SessionID</b>	Gibt die Sitzungs-ID für die Verbindung zurück, falls eine vorhanden ist, sonst eine leere Zeichenfolge.
<b>SessionLastTime</b>	Gibt die Uhrzeit der letzten Anforderung für die HTTP-Sitzung zurück.
<b>SessionTimeout</b>	Gibt in Minuten zurück, wie lange die HTTP-Sitzung während der Inaktivität aufrecht bleibt. Siehe „ <a href="#">sa_set_http_option-Systemprozedur</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>SnapshotCount</b>	Gibt die Anzahl der der Verbindung zugeordneten Snapshots zurück.
<b>sort_collation</b>	Gibt "Internal" zurück, wenn die ORDER BY-Klausel unverändert bleibt. Anderenfalls wird der Kollationsname oder die Kollations-ID zurückgegeben. Siehe „ <a href="#">sort_collation-Option</a> “ auf Seite 670.
<b>SortMergePasses</b>	Gibt die Anzahl der Zusammenführungsdurchgänge zurück, die während des Sortierens benutzt wurden.
<b>SortRowsMaterialized</b>	Gibt die Anzahl der Zeilen zurück, die in Arbeitstabellen sortiert werden.
<b>SortRunsWritten</b>	Gibt die Anzahl sortierter Folgen zurück, die während des Sortierens geschrieben wurden.
<b>SortSortedRuns</b>	Gibt die Anzahl sortierter Folgen zurück, die während der Folgenbildung erstellt wurden.
<b>SortWorkTables</b>	Gibt die Anzahl der für Sortierungen erstellten Arbeitstabellen zurück.

Eigenschaftsname	Beschreibung
<b>sql_flagger_error_level</b>	<p>Gibt einen der folgenden Werte zurück um anzuzeigen, welche SQL-Anweisung, die kein Teil eines bestimmten Sets von SQL/2003 ist, als Fehler gekennzeichnet wird:</p> <ul style="list-style-type: none"> <li>• <b>E</b> Kennzeichnet Syntax, die nicht Entry-Level der SQL/2003 Syntax ist</li> <li>• <b>I</b> Kennzeichnet Syntax, die nicht Intermediate-Level der SQL/2003 Syntax ist</li> <li>• <b>F</b> Kennzeichnet Syntax, die nicht Full-SQL/2003 Syntax ist</li> <li>• <b>W</b> Lässt jede unterstützte Syntax zu.</li> </ul> <p>Siehe „<a href="#">sql_flagger_error_level-Option</a>“ auf Seite 671.</p>
<b>sql_flagger_warning_level</b>	<p>Gibt einen der folgenden Werte zurück, um anzuzeigen, welche SQL-Anweisung, die kein Teil eines bestimmten Sets von SQL/2003 ist, als Warnung gekennzeichnet wird:</p> <ul style="list-style-type: none"> <li>• <b>E</b> Kennzeichnet Syntax, die nicht Entry-Level der SQL/2003 Syntax ist</li> <li>• <b>I</b> Kennzeichnet Syntax, die nicht Intermediate-Level der SQL/2003 Syntax ist</li> <li>• <b>F</b> Kennzeichnet Syntax, die nicht Full-SQL/2003 Syntax ist</li> <li>• <b>W</b> Lässt jede unterstützte Syntax zu.</li> </ul> <p>Siehe „<a href="#">sql_flagger_warning_level-Option</a>“ auf Seite 672.</p>
<b>st_geometry_asbinary_format</b>	<p>Gibt einen Wert zurück, der anzeigt, wie räumliche Werte aus einer Geometrie in ein Binärformat konvertiert werden. Siehe „<a href="#">st_geometry_asbinary_format-Option</a>“ auf Seite 679.</p>
<b>st_geometry_astext_format</b>	<p>Gibt einen Wert zurück, der darauf hinweist, wie räumliche Werte in einer Geometrie in Text umgewandelt werden. Siehe „<a href="#">st_geometry_astext_format-Option</a>“ auf Seite 680.</p>
<b>st_geometry_asxml_format</b>	<p>Gibt einen Wert zurück, der darauf hinweist, wie räumliche Werte in einer Geometrie in XML-Code umgewandelt werden. Siehe „<a href="#">st_geometry_asxml_format-Option</a>“ auf Seite 681.</p>
<b>st_geometry_describe_type</b>	<p>Gibt einen Wert zurück, der darauf hinweist, dass räumliche Werte beschrieben werden. Siehe „<a href="#">st_geometry_describe_type-Option</a>“ auf Seite 682.</p>

Eigenschaftsname	Beschreibung
<b>st_geometry_interpolation</b>	Gibt die Interpolationseinstellung für ST_CircularString-Geometrien zurück. Siehe „ <a href="#">st_geometry_interpolation-Option</a> “ auf Seite 683.
<b>st_geometry_on_invalid</b>	Gibt einen Wert zurück, der auf das Verhalten hinweist, wenn die Flächenvalidierung einer Geometrie fehlschlägt. Siehe „ <a href="#">st_geometry_on_invalid-Option</a> “ auf Seite 684.
<b>StatementDescribes</b>	Gibt die Gesamtanzahl von Anweisungen zurück, die von DESCRIBE-Anforderungen verarbeitet werden.
<b>StatementPostAnnotates</b>	Gibt die Anzahl von Anweisungen zurück, die von der semantischen Abfragetransformationsphase verarbeitet werden.
<b>StatementPostAnnotatesSimple</b>	Gibt die Anzahl von Anweisungen zurück, die von der semantischen Abfragetransformationsphase verarbeitet wurden, wobei aber einige semantische Transformationen übersprungen wurden.
<b>StatementPostAnnotatesSkipped</b>	Gibt die Anzahl von Anweisungen zurück, die die semantische Abfragetransformationsphase komplett übersprungen haben.
<b>string_rtruncation</b>	Gibt "On" zurück, wenn ein Fehler ausgegeben wird, weil eine Zeichenfolge gekürzt wird, oder "Off", wenn kein Fehler ausgegeben und die Zeichenfolge stillschweigend gekürzt wird. Siehe „ <a href="#">string_rtruncation-Option</a> “ auf Seite 685.
<b>subsume_row_locks</b>	Gibt "On" zurück, wenn der Datenbankserver individuelle Zeilensperren für eine Tabelle setzt. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">subsume_row_locks-Option</a> “ auf Seite 686.
<b>suppress_tds_debugging</b>	Gibt "Off" zurück, wenn TDS-Fehlersuche-Informationen im Meldungsfenster des Datenbankservers angezeigt werden. Gibt "On" zurück, wenn diese Informationen nicht im Meldungsfenster des Datenbankservers angezeigt werden. Siehe „ <a href="#">suppress_tds_debugging-Option</a> “ auf Seite 687.
<b>synchronize_mirror_on_commit</b>	Gibt "On" zurück, wenn der Datenbank-Spiegelserver beim Festschreiben synchronisiert wird. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">synchronize_mirror_on_commit</a> “ auf Seite 688.
<b>tds_empty_string_is_null</b>	Gibt "On" zurück, wenn bei TDS-Verbindungen leere Zeichenfolgen als NULL-Zeichenfolgen ausgegeben werden. Gibt "Off" zurück, wenn bei TDS-Verbindungen eine Zeichenfolge mit einem Leerzeichen ausgegeben wird. Siehe „ <a href="#">tds_empty_string_is_null-Option</a> “ auf Seite 689.

Eigenschaftsname	Beschreibung
<b>temp_space_limit_check</b>	Gibt "On" zurück, wenn der Datenbankserver die Menge des für eine Verbindung verfügbaren temporären Speicherplatzes überprüft, oder "Off", wenn der Datenbankserver die Menge an verfügbarem Speicherplatz nicht überprüft. Siehe „ <a href="#">temp_space_limit_check-Option</a> “ auf Seite 689.
<b>TempFilePages</b>	Gibt die von der Verbindung verwendete Anzahl an Seiten der temporären Datei zurück.
<b>TempTablePages</b>	Gibt die Anzahl der Seiten in der temporären Datei zurück, die für temporäre Tabellen verwendet werden.
<b>time_format</b>	Gibt das Zeichenfolgenformat zurück, das für Zeitwerte verwendet wird, die aus der Datenbank abgerufen werden. Siehe „ <a href="#">time_format-Option</a> “ auf Seite 690.
<b>time_zone_adjustment</b>	Gibt die Anzahl der Minuten zurück, die der Coordinated Universal Time (UTC) hinzugefügt werden muss, um die für die Verbindung lokale Uhrzeit anzuzeigen. Siehe „ <a href="#">time_zone_adjustment-Option</a> “ auf Seite 691.
<b>timestamp_format</b>	Gibt das Format für aus der Datenbank abgerufene Zeitstempel zurück. Siehe „ <a href="#">timestamp_format-Option</a> “ auf Seite 692.
<b>time-stamp_with_time_zone_format</b>	Gibt das Format für von der Datenbank abgerufene TIMESTAMP WITH TIME ZONE-Werte zurück. Siehe „ <a href="#">time-stamp_with_time_zone_format-Option</a> “ auf Seite 694.
<b>TimeZoneAdjustment</b>	Gibt die Anzahl der Minuten zurück, die der Coordinated Universal Time (UTC) hinzugefügt werden muss, um die für die Verbindung lokale Uhrzeit anzuzeigen. Siehe „ <a href="#">time_zone_adjustment-Option</a> “ auf Seite 691.
<b>TransactionStartTime</b>	Gibt eine Zeichenfolge mit der Uhrzeit zurück, zu der die Datenbank erstmals nach einem COMMIT oder ROLLBACK geändert wurde, oder eine leere Zeichenfolge, wenn seit dem letzten COMMIT oder ROLLBACK keine Änderungen in der Datenbank durchgeführt wurden.
<b>truncate_timestamp_values</b>	Gibt "On" zurück, wenn die Anzahl der Dezimalstellen in den TIMESTAMP-Werten beschränkt ist. Andernfalls wird "Off" zurückgegeben. Siehe „ <a href="#">truncate_timestamp_values-Option</a> “ auf Seite 697.
<b>trusted_certificates_file</b>	Gibt die Datei mit der Liste von Zertifikaten vertrauenswürdiger Zertifizierungsstellen zurück, wenn der Datenbankserver als Client eines LDAP-Servers fungiert. Siehe „ <a href="#">trusted_certificates_file-Option</a> “ auf Seite 696.

Eigenschaftsname	Beschreibung
<b>tsql_outer_joins</b>	Gibt "On" (aktiviert) zurück, wenn TSQL-Outer-Joins in DML-Anweisungen verwendet werden können. Siehe „ <a href="#">tsql_outer_joins-Option</a> “ auf Seite 699.
<b>tsql_variables</b>	Gibt "On" zurück, wenn Sie das Zeichen @ anstelle des Doppelpunkts als Präfix für einen Hostvariablenamen in Embedded SQL verwenden können. Anderenfalls wird "Off" zurückgegeben. Siehe „ <a href="#">tsql_variables-Option</a> “ auf Seite 699.
<b>UncommitOp</b>	Gibt die Anzahl der nicht festgeschriebenen Vorgänge zurück.
<b>updatable_statement_isolation</b>	Gibt die von aktualisierbaren Anweisungen verwendete Isolationsstufe (0, 1, 2 oder 3) zurück, wenn die Option isolation_level auf Readonly-statement-snapshot gesetzt ist. Siehe „ <a href="#">updatable_statement_isolation-Option</a> “ auf Seite 700.
<b>update_statistics</b>	Gibt On zurück, wenn diese Verbindung Abfragerückmeldungen an den Statistikwächter senden kann. Wenn die update_statistics-Option auf Off eingestellt ist, empfängt der Statistikwächter keine Abfragerückmeldungen von der aktuellen Verbindung. Siehe „ <a href="#">update_statistics-Option</a> “ auf Seite 701.
<b>upgrade_database_capability</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Option nicht.
<b>user_estimates</b>	<p>Gibt einen der folgenden Werte zurück, die steuern, ob Selektivitätsschätzungen in Abfrageprädikaten vom Abfrageoptimierer respektiert oder ignoriert werden:</p> <ul style="list-style-type: none"> <li>• <b>Valid</b> Alle von Benutzern gelieferten Selektivitätsschätzungen werden respektiert. Sie können diese Option mit "On" einschalten.</li> <li>• <b>Override-Magic</b> Eine Benutzer-Selektivitätsschätzung wird nur respektiert und verwendet, wenn der Optimierer sonst als letzte Möglichkeit seinen heuristischen Wert (auch magischer Wert genannt) verwenden würde.</li> <li>• <b>Disabled</b> Alle Benutzerschätzungen werden ignoriert und magische Werte verwendet, wenn keine anderen Schätzungsdaten verfügbar sind. Sie können diese Option mit "Off" ausschalten.</li> </ul> <p>Siehe „<a href="#">user_estimates-Option</a>“ auf Seite 702.</p>

Eigenschaftsname	Beschreibung
<b>UserAppInfo</b>	<p>Gibt die Zeichenfolge zurück, die der AppInfo-Verbindungsparameter in einer Verbindungszeichenfolge angegeben hat.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Verbindungsparameter AppInfo (APP)</a>“ auf Seite 338.</p>
<b>UserDefinedCounterRate01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung am Wert des Indikators im Laufe der Zeit an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounterRate02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung am Wert des Indikators im Laufe der Zeit an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounterRate03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung am Wert des Indikators im Laufe der Zeit an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounterRate04</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung am Wert des Indikators im Laufe der Zeit an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounterRate05</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung am Wert des Indikators im Laufe der Zeit an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounterRaw01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounterRaw02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounterRaw03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounterRaw04</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounter-Raw05</b>	Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.  Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a> .
<b>UserID</b>	Gibt die Benutzer-ID für die Verbindung zurück.
<b>UtilCmdsPermitted</b>	Gibt diese Option mit "On" oder "Off" zurück um anzuzeigen, ob Dienstprogrammbeefehle wie CREATE DATABASE, DROP DATABASE und RESTORE DATABASE bei der Verbindung zulässig sind. Siehe <a href="#">„Datenbankserveroption -gu“ auf Seite 255</a> .
<b>uuid_has_hyphens</b>	Diese Eigenschaft steuert die Formatierung von Werten für eindeutige Bezeichner, wenn sie in Zeichenfolgen konvertiert werden. Siehe <a href="#">„uuid_has_hyphens-Option“ auf Seite 703</a> .
<b>verify_password_function</b>	Gibt den Namen der Kennwort-Überprüfungsfunktion zurück, falls eine angegeben wurde. Siehe <a href="#">„verify_password_function-Option“ auf Seite 704</a> .
<b>wait_for_commit</b>	Gibt "On" zurück, wenn die Datenbank die Integrität von Fremdschlüsseln bis zur nächsten COMMIT-Anweisung nicht überprüft. Andernfalls wird "Off" zurückgegeben und alle Fremdschlüssel, die nicht mit der Option check_on_commit erstellt wurden, werden beim Einfügen, Aktualisieren oder Löschen geprüft. Siehe <a href="#">„wait_for_commit-Option“ auf Seite 708</a> .
<b>WaitStartTime</b>	Gibt den Zeitpunkt zurück, zu dem die Verbindung mit dem Warten begonnen hat (oder eine leere Zeichenfolge, wenn die Verbindung nicht wartet).
<b>WaitType</b>	Gibt die Ursache für das Warten zurück, sofern sie verfügbar ist. Mögliche Werte für WaitType sind: <ul style="list-style-type: none"> <li>• <b>lock</b> Wird zurückgegeben, wenn die Verbindung auf eine Sperre wartet.</li> <li>• <b>waitfor</b> Wird zurückgegeben, wenn die Verbindung eine waitfor-Anweisung ausführt.</li> <li>• <b>Leere Zeichenfolge</b> Wird zurückgegeben, wenn die Verbindung nicht wartet oder die Ursache für das Warten nicht ermittelbar ist.</li> </ul>

Eigenschaftsname	Beschreibung
<b>webservice_namespace_host</b>	Gibt den Hostnamen zurück (falls einer angegeben wurde), der als der XML-Namespace innerhalb generierter WSDL-Dokumente verwendet werden soll. Siehe „webservice_namespace_host-Option“ auf Seite 708.
<b>webservice_sessionid_name</b>	Gibt den Namen des Sitzungsbezeichners zurück, anhand dessen der Webserver ermittelt, ob die Sitzungsverwaltung verwendet wird. Siehe „webservice_sessionid_name-Option“ auf Seite 709.

## Auf Werte von Datenbankservereigenschaften zugreifen

Sie können die PROPERTY-Systemfunktion verwenden, um den Wert für eine einzelne Eigenschaft abzurufen, oder die sa\_eng\_properties-Systemprozedur, um die Werte aller Datenbankservereigenschaften abzurufen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Bei Eigenschaftsnamen wird die Groß- und Kleinschreibung nicht berücksichtigt. Datenbankservereigenschaften gelten für den Datenbankserver als Ganzes.

### Aufgabe

- Verwenden Sie eine der folgenden Methoden, um auf Werte von Datenbankservereigenschaften zuzugreifen:

Option	Aktion
Wert einer Datenbankservereigenschaft abrufen	Verwenden Sie die PROPERTY-Systemfunktion.
Werte aller Datenbankservereigenschaften abrufen	Verwenden Sie die sa_eng_properties-Systemprozedur.

### Ergebnisse

Der Wert der Datenbankservereigenschaft wird zurückgegeben.

### Beispiel

Die folgende Anweisung gibt die Anzahl der Cacheseiten zurück, die für globale Server-Datenstrukturen verwendet werden:

```
SELECT PROPERTY ( 'MainHeapPages' );
```

Verwenden Sie die sa\_eng\_properties-Systemprozedur, um die Werte aller Datenbankservereigenschaften abzurufen:

```
CALL sa_eng_properties;
```

#### Siehe auch

- „PROPERTY-Funktion [System]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sa\_eng\_properties-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „Liste der Verbindungseigenschaften“ auf Seite 711
- „Liste der Datenbankservereigenschaften“ auf Seite 745

## Liste der Datenbankservereigenschaften

### Datenbankservereigenschaften

Eigenschaftsname	Beschreibung
<b>ActiveReq</b>	Gibt die Anzahl der Server-Worker zurück, die derzeit clientseitige Anforderungen abarbeiten.
<b>ApproximateCPUTime</b>	Gibt eine Schätzung der CPU-Zeit in Sekunden zurück, die vom Datenbankserver genutzt wurde. Der zurückgegebene Wert kann sich vom tatsächlichen Wert um bis zu 50 % unterscheiden, auch wenn übliche Abweichungen im Bereich von 5 - 10 % liegen. Auf Mehrprozessorcomputern akkumuliert jede CPU (bzw. jeder Hyperthread oder Kern) Zeit, daher kann die Summe der akkumulierten Zeit für alle Verbindungen größer als die verstrichene Zeit sein. Diese Eigenschaft wird unter Windows und Linux unterstützt.
<b>AutoMultiProgrammingLevel</b>	Gibt einen Wert zurück, der angibt, ob der Datenbankserver automatisch seine Multiprogramming-Stufe anpasst. Siehe „ <a href="#">Datenbankserveroption - gna</a> “ auf Seite 245.
<b>AutoMultiProgrammingLevelStatistics</b>	Gibt einen Wert zurück, der angibt, ob Meldungen über automatische Anpassungen an die Multiprogramming-Stufe des Datenbankserver im Meldungslog des Datenbankservers angezeigt werden. Siehe „ <a href="#">Datenbankserveroption - gns</a> “ auf Seite 248.
<b>AvailIO</b>	Gibt die aktuelle Anzahl der verfügbaren I/O-Kontrollblöcke zurück.
<b>BuildChange</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Eigenschaft nicht.
<b>BuildClient</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Eigenschaft nicht.

Eigenschaftsname	Beschreibung
<b>BuildProduction</b>	Gibt "Yes" zurück, wenn der Datenbankserver für die Produktion kompiliert ist, und "No", wenn der Datenbankserver ein Debug-Build ist.
<b>BuildReproducible</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Eigenschaft nicht.
<b>BytesReceived</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesReceivedUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "BytesReceived", wenn die Komprimierung deaktiviert ist.)
<b>BytesSent</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesSentUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie der Wert für BytesSent, wenn die Komprimierung deaktiviert ist.)
<b>CacheAllocated</b>	Gibt die Anzahl der Cacheseiten zurück, die für Server-Datenstrukturen zugewiesen wurden.
<b>CacheFile</b>	Gibt die Anzahl der Cacheseiten zurück, die für die Aufnahme von Daten aus Datenbankdateien verwendet werden.
<b>CacheFileDirty</b>	Gibt die Anzahl der Cacheseiten zurück, die verändert wurden (und ausgeschrieben werden müssten).
<b>CacheFree</b>	Gibt die Anzahl von nicht benutzten Cacheseiten zurück.
<b>CacheHits</b>	Gibt die Anzahl der Suchvorgänge nach Datenbankseiten zurück.
<b>CachePanics</b>	Gibt die Häufigkeit zurück, mit der der Cachemanager keine Seite für die Zuweisung finden konnte.
<b>CachePinned</b>	Gibt die Anzahl der vorgemerkten Cacheseiten zurück.
<b>CacheRead</b>	Gibt die Anzahl der Cache-Lesevorgänge zurück.
<b>CacheReplacements</b>	Gibt die Anzahl von Seiten im Cache zurück, die ersetzt wurden.

Eigenschaftsname	Beschreibung
<b>CacheScavenges</b>	Gibt die Häufigkeit zurück, mit der der Cachemanager aufräumen musste, um eine Seite zuweisen zu können.
<b>CacheScavengeVisited</b>	Gibt die Anzahl der Seiten zurück, die während des Aufräumens besucht wurden, um eine Seite zuweisen zu können.
<b>CacheSizingStatistics</b>	Gibt "Yes" zurück, wenn der Server bei einer Änderung der Cachegrößen-zuweisung Statistiken zur Cachedimensionierung anzeigt. Andernfalls wird "No" zurückgegeben. Siehe „ <a href="#">Datenbankserveroption -cs</a> “ auf Seite 227.
<b>CarverHeapPages</b>	Gibt die Anzahl von Heap-Seiten zurück, die für Kurzzeit Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.
<b>CharSet</b>	Gibt den vom Datenbankserver verwendeten CHAR-Zeichensatz zurück.
<b>ClientStmtCacheHits</b>	Gibt die Anzahl der Vorbereitungen zurück, die aufgrund des Clientanweisungscache nicht erforderlich waren. Dies ist die Anzahl der Vorbereitungen, die erforderlich wären, wenn das clientseitige Caching von Anweisungen deaktiviert wäre. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>ClientStmtCacheMisses</b>	Gibt die Anzahl der Vorbereitungen im Clientanweisungscache zurück, die erneut vorbereitet wurden. Dies ist die Angabe, wie oft eine zwischengespeicherte Anweisung für die Wiederverwendung in Frage kam, aber aufgrund einer Schemaänderung, einer Datenbank-Optionseinstellung oder einer DROP VARIABLE-Anweisung nicht wieder verwendet werden konnte. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>CollectStatistics</b>	Gibt "Yes" oder "No" zurück um anzuzeigen, ob der Datenbankserver Performance-Statistiken sammelt. Siehe „ <a href="#">Datenbankserveroption -k</a> “ auf Seite 259.
<b>CommandLine</b>	Gibt die beim Start des Datenbankservers verwendeten Befehlszeilen zurück.  Wenn der Chiffrierschlüssel für eine Datenbank mit der Option -ek angegeben wurde, wird der Schlüssel im von dieser Eigenschaft zurückgegebenen Wert durch eine Reihe von Sternchen ersetzt.
<b>Commit</b>	Gibt die Anzahl der Commit-Anforderungen zurück, die verarbeitet wurden.
<b>CompactPlatformVer</b>	Gibt eine gekürzte Version der PlatformVer-Eigenschaft zurück.
<b>CompanyName</b>	Gibt den Namen der Firma zurück, der diese Software gehört.

Eigenschaftsname	Beschreibung
<b>ConnectedTime</b>	<p>Gibt an, wie lange (in Sekunden) alle Verbindungen mit dem Datenbankserver aktiv waren.</p> <p>Der Wert wird nur aktualisiert, wenn eine Anforderung für eine Verbindung abgeschlossen wird oder wenn eine Verbindung getrennt wird. Daher kann der Wert für Verbindungen, die inaktiv sind oder seit längerer Zeit im Datenbankserver ausgeführt werden, nicht aktuell sein. Der Wert beinhaltet die Zeit, die sich von beliebigen Verbindungen angesammelt hat, einschließlich Datenbankereignissen und Hintergrundserververbindungen (z.B. Datenbankaufräumvorgang).</p>
<b>ConnsDisabled</b>	Gibt "Yes" oder "No" zurück, um die aktuelle Einstellung der Serveroption zur Deaktivierung von neuen Verbindungen anzuzeigen. Siehe „ <a href="#">sa_server_option-Systemprozedur</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>ConsoleLogFile</b>	Gibt den Namen der Datei zurück, in der Datenbankservermeldungen protokolliert werden, falls die Option -o angegeben wurde. Anderenfalls wird eine leere Zeichenfolge zurückgegeben. Siehe „ <a href="#">Datenbankserveroption -o</a> “ auf Seite 268 und „ <a href="#">Protokollieren von Datenbankserver-Aktionen</a> “ auf Seite 163.
<b>ConsoleLogMaxSize</b>	Gibt die maximale Größe (in Byte) der Datei zurück, die zum Protokollieren der Datenbankservermeldungen verwendet wird. Siehe „ <a href="#">Datenbankserveroption -os</a> “ auf Seite 270.
<b>CurrentCacheSize</b>	Gibt die aktuelle Cachegröße in kB zurück.
<b>CurrentMultiProgrammingLevel</b>	Gibt die aktuelle Anzahl von Aufgaben zurück, die der Datenbankserver gleichzeitig ausführen kann. Siehe „ <a href="#">Datenbankserverkonfiguration der Multiprogramming-Stufe</a> “ auf Seite 175.
<b>Cursor</b>	Gibt die Anzahl der deklarierten Cursor zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>CursorOpen</b>	Gibt die Anzahl der offenen Cursor zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>DebuggingInformation</b>	Gibt "Yes" zurück, wenn der Server Diagnosemeldungen zum Zweck der Fehlerbehandlung anzeigt. Anderenfalls wird "No" zurückgegeben. Siehe „ <a href="#">Datenbankserveroption -z</a> “ auf Seite 312.
<b>DefaultCollation</b>	Gibt die Kollation zurück, die bei neuen Datenbanken verwendet wird, wenn keine explizit angegeben ist.

Eigenschaftsname	Beschreibung
<b>DefaultNcharCollation</b>	Gibt den Namen der Standard-NCHAR-Kollation auf dem Servercomputer zurück (UCA, wenn ICU installiert ist, ansonsten UTF8BIN).
<b>DiskRead</b>	Gibt die Anzahl der Festplatten-Lesevorgänge zurück.
<b>DiskReadHintScatter-Limit</b>	Gibt die erzwungene Beschränkung der Größe (in Byte) von Hints für verteilte Lesevorgänge zurück.
<b>DiskRetryRead</b>	Gibt die Anzahl der Festplattenlese-Neuersuche zurück.
<b>DiskRetryReadScatter</b>	Gibt die Anzahl der Festplattenlese-Neuersuche für verteilte Lesevorgänge zurück.
<b>DiskRetryWrite</b>	Gibt die Anzahl der Festplattenschreib-Neuersuche zurück.
<b>DiskSandbox</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob Dateivorgänge der Datenbank mit Lese-/Schreibzugriff auf das Verzeichnis beschränkt sind, in dem sich die Hauptdatenbankdatei befindet. Siehe „ <a href="#">Datenbankserveroption - sbx</a> “ auf Seite 279.
<b>EventTypeDesc</b>	Gibt die Beschreibung des Ereignistyps zurück, der einer gegebenen Ereignistyp-ID zugeordnet ist.
<b>EventTypeName</b>	Gibt den Namen des Systemereignistyps zurück, der einer gegebenen Ereignistyp-ID zugewiesen ist.
<b>ExchangeTasks</b>	Gibt die Anzahl der Aufgaben zurück, die derzeit für die parallele Ausführung von Abfragen verwendet werden.
<b>ExchangeTasksCompleted</b>	Gibt die Gesamtanzahl von internen Aufgaben zurück, die seit dem Start der Datenbank für die abfrageinterne Parallelität verwendet wurde. Siehe „ <a href="#">Fortgeschrittene Aufgaben: Parallelität während der Abfrageausführung</a> “ [ <a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a> ].
<b>FipsMode</b>	Gibt "Yes" zurück, wenn die Option -fips beim Start der Datenbank angegeben wurde. Anderenfalls wird "No" zurückgegeben.
<b>FirstOption</b>	Gibt die Nummer zurück, die die erste Verbindungseigenschaft darstellt, die einer Datenbankoption entspricht.
<b>FreeBuffers</b>	Gibt die Anzahl der verfügbaren Netzwerkpuffer zurück.

Eigenschaftsname	Beschreibung
<b>FunctionMaxParms</b>	<p>Gibt die maximale Anzahl von Parametern zurück, die von einer Funktion angegeben werden können. Die Funktion wird durch den Wert identifiziert, der mit <i>function-number</i> angegeben wird, einer positiven Ganzzahl. Zum Beispiel:</p> <pre>SELECT PROPERTY ( 'FunctionMaxParms', function-number );</pre> <p><i>function-number</i> kann sich von Version zu Version ändern.</p>
<b>FunctionMinParms</b>	<p>Gibt die minimale Anzahl von Parametern zurück, die von einer Funktion angegeben werden müssen. Die Funktion wird durch den Wert identifiziert, der mit <i>function-number</i> angegeben wird, einer positiven Ganzzahl. Zum Beispiel:</p> <pre>SELECT PROPERTY ( 'FunctionMinParms', function-number );</pre> <p><i>function-number</i> kann sich von Version zu Version ändern.</p>
<b>FunctionName</b>	<p>Gibt den Namen der Funktion zurück, die durch den mit <i>function-number</i> (einer positiven Ganzzahl) angegebenen Wert identifiziert wird:</p> <pre>SELECT PROPERTY ( 'FunctionName', function-number );</pre> <p><i>function-number</i> kann sich von Version zu Version ändern.</p>
<b>HeapsCarver</b>	Gibt die Anzahl der Heaps zurück, die für kurzzeitige Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.
<b>HeapsLocked</b>	Gibt die Anzahl von neu positionierbaren, derzeit im Cache gesperrten Heaps zurück.
<b>HeapsQuery</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Heaps zurück.
<b>HeapsRelocatable</b>	Gibt die Anzahl von neu positionierbaren Heaps zurück.
<b>HttpAddresses</b>	<p>Gibt eine durch Semikola getrennte Liste der TCP/IP-Adressen zurück, die der Datenbankserver bei HTTP-Verbindungen abhört. Zum Beispiel:</p> <pre>(::1):80;127.0.0.1:80</pre>
<b>HttpNumActiveReq</b>	Gibt die Anzahl der HTTP-Verbindungen zurück, die aktiv eine HTTP-Anforderung abarbeiten. HTTP-Verbindungen, die ihre Antwort gesendet haben, sind nicht enthalten.

Eigenschaftsname	Beschreibung
<b>HttpNumConnections</b>	Gibt die Anzahl der HTTP-Verbindungen zurück, die derzeit im Datenbankserver geöffnet sind. Diese können eine Anforderung aktiv abarbeiten oder in der Warteschlange von langlebigen (keep-alive) Verbindungen warten.
<b>HttpNumSessions</b>	Gibt die Anzahl von aktiven und nicht-aktiven HTTP-Sitzungen im Datenbankserver zurück.
<b>HttpPorts</b>	Gibt die HTTP-Portnummern für den Webserver als kommasetrennte Liste zurück.
<b>HttpsAddresses</b>	Gibt eine durch Semikola getrennte Liste der TCP/IP-Adressen zurück, die der Datenbankserver bei HTTPS-Verbindungen abhört. Zum Beispiel:  <code>(::1):443;127.0.0.1:443</code>
<b>HttpsNumActiveReq</b>	Gibt die Anzahl der HTTP-Verbindungen zurück, die aktiv eine HTTPS-Anforderung abarbeiten. HTTPS-Verbindungen, die ihre Antwort gesendet haben, sind nicht enthalten.
<b>HttpsNumConnections</b>	Gibt die Anzahl der HTTPS-Verbindungen zurück, die derzeit im Datenbankserver geöffnet sind. Diese können eine Anforderung aktiv abarbeiten oder in der Warteschlange von langlebigen (keep-alive) Verbindungen warten.
<b>HttpsPorts</b>	Gibt die HTTPS-Portnummern für den Webserver als kommasetrennte Liste zurück.
<b>IdleTimeout</b>	Gibt den Standardwert für das Inaktivitäts-Timeout zurück. Siehe „ <a href="#">Datenbankserveroption -ti</a> “ auf Seite 291.
<b>IPAddressMonitorPeriod</b>	Gibt die Zeit in Sekunden zurück, während derer ein Datenbankserver nach neuen IP-Adressen sucht. Siehe „ <a href="#">Datenbankserveroption -xm</a> “ auf Seite 309.
<b>IsAesniAvailable</b>	Gibt "Yes" zurück, wenn die CPU des Datenbankservercomputers den Intel AES-NI-Anweisungssatz unterstützt und auf dem Computer ein unterstütztes Betriebssystem läuft, bzw. andernfalls "No".
<b>IsFipsAvailable</b>	Gibt "Yes" zurück, wenn die FIPS-zertifizierte DLL installiert ist. Andernfalls wird "No" zurückgegeben.
<b>IsIQ</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Eigenschaft nicht.

Eigenschaftsname	Beschreibung
<b>IsNetworkServer</b>	Gibt "Yes" zurück, wenn es sich um eine Verbindung zu einem Netzwerk-Datenbankserver handelt, und "No", wenn es sich um eine Verbindung zu einem Personal Datenbankserver handelt.
<b>IsPortableDevice</b>	<p>Gibt "Yes" zurück, wenn der Datenbankserver auf einem Laptop, Notebook oder anderen tragbaren Gerät läuft, sonst "No". Auf Windows Mobile wird immer "Yes" zurückgegeben. VMWare wird nicht berücksichtigt, daher gibt ein Datenbankserver, der auf einer VM auf einem Laptop läuft, "No" zurück.</p> <p>Wenn unter Windows nicht ermittelbar ist, ob das Gerät ein tragbares Gerät ist, gibt diese Eigenschaft NULL zurück.</p> <p>Diese Eigenschaft gibt unter Unix immer NULL zurück.</p>
<b>IsRsaAvailable</b>	Gibt "Yes" zurück, wenn die RSA DLL installiert ist. Andernfalls wird "No" zurückgegeben.
<b>IsRuntimeServer</b>	Gibt für alle Versionen des Datenbankservers "No" zurück.
<b>IsService</b>	Gibt "Yes" zurück, wenn der Datenbankserver als Dienst läuft, sonst "No".
<b>Language</b>	Gibt die Sprachumgebungsprache für den Server zurück.
<b>LastConnectionProperty</b>	Gibt die Nummer zurück, die die letzte Verbindungseigenschaft darstellt.
<b>LastDatabaseProperty</b>	Gibt die Nummer zurück, die die letzte Datenbankeigenschaft darstellt.
<b>LastOption</b>	Gibt die Nummer zurück, die die letzte Verbindungseigenschaft darstellt, die einer Datenbankoption entspricht.
<b>LastServerProperty</b>	Gibt die Nummer zurück, die die letzte Servereigenschaft darstellt.
<b>LegalCopyright</b>	Gibt die Copyright-Zeichenfolge für die Software zurück.
<b>LegalTrademarks</b>	Gibt die Markenzeicheninformationen für die Software zurück.
<b>LicenseCount</b>	Gibt die Anzahl der lizenzierten Arbeitsplätze oder Prozessoren zurück.
<b>LicensedCompany</b>	Gibt den Namen des lizenzierten Unternehmens zurück.
<b>LicensedUser</b>	Gibt den Namen des lizenzierten Benutzers zurück.
<b>LicenseKey</b>	Wird nur intern verwendet.

Eigenschaftsname	Beschreibung
<b>LicenseType</b>	Gibt den Lizenztyp zurück. Kann Networked Seat (pro Arbeitsplatz) oder CPU-basiert sein.
<b>LivenessTimeout</b>	Gibt den Standardwert des Verfügbarkeits-Timeouts für Clients zurück. Siehe „ <a href="#">Datenbankserveroption -tl</a> “ auf Seite 292.
<b>LockedCursorPages</b>	Gibt die Anzahl der Seiten zurück, die verwendet werden, um Cursor-Heaps im Speicher bereit zu halten.
<b>LockedHeapPages</b>	Gibt die Anzahl der im Cache gesperrten Heap-Seiten zurück.
<b>MachineName</b>	Gibt den Namen des Computers zurück, auf dem ein Datenbankserver läuft. Das ist üblicherweise der Hostname des Computers.
<b>MainHeapBytes</b>	Gibt die Anzahl der Bytes zurück, die für globale Server-Datenstrukturen verwendet werden.
<b>MainHeapPages</b>	Gibt die Anzahl der Seiten zurück, die für globale Server-Datenstrukturen verwendet werden.
<b>MapPhysicalMemoryEng</b>	Gibt die Anzahl der Adressraumfenster für Datenbankseiten zurück, die dem physischen Speicher im Cache über Address Windowing Extensions zugewiesen werden.
<b>MaxCacheSize</b>	Gibt die maximal zulässige Cachegröße in Kilobyte zurück.
<b>MaxConnections</b>	<p>Gibt die maximale Anzahl der gleichzeitigen Verbindungen zurück, die der Server zulässt. Beim Personal Server ist dieser Wert standardmäßig "10". Beim Netzwerkserver ist dieser Wert standardmäßig "32000". Dieser Wert kann mit der Serveroption -gn verringert werden. Siehe „<a href="#">Datenbankserveroption -gm</a>“ auf Seite 244.</p> <p>Computerressourcen begrenzen üblicherweise die Anzahl der Verbindungen zu einem Netzwerkserver auf einen niedrigeren Wert als den Standardwert.</p>
<b>MaxEventType</b>	Gibt die maximale gültige Ereignistyp-ID zurück.
<b>MaxMessage</b>	Diese Eigenschaft ist veraltet. Gibt die aktuelle höchste Zeilennummer zurück, die aus dem Fenster "Datenbankservermeldungen" abgerufen werden kann. Dies stellt die zuletzt im Fenster "Datenbankservermeldungen" angezeigte Meldung dar.
<b>MaxMultiProgrammingLevel</b>	Gibt die maximale Anzahl von Aufgaben zurück, die der Datenbankserver gleichzeitig ausführen kann. Siehe „ <a href="#">Datenbankserverkonfiguration der Multiprogramming-Stufe</a> “ auf Seite 175.

Eigenschaftsname	Beschreibung
<b>MaxRemoteCapability</b>	Gibt die maximale gültige Funktionalitäts-ID zurück.
<b>Message</b>	<p>Diese Eigenschaft ist veraltet. Gibt eine Zeile aus den Fenster "Datenbankservermeldungen" zurück, der das Datum und die Uhrzeit der Meldungsanzeige vorangestellt ist. Der zweite Parameter gibt die Zeilennummer an.</p> <p>Der von <code>PROPERTY( "message" )</code> zurückgegebene Wert ist die erste Zeile der Ausgabe, die im Fenster "Datenbankservermeldungen" angezeigt wird. Das Aufrufen von <code>PROPERTY( "message", n )</code> gibt die n-te Zeile der Serverausgabe zurück (wobei Null die erste Zeile ist). Der Puffer ist begrenzt, daher werden während der Generierung von Meldungen die ersten Zeilen gelöscht und stehen möglicherweise im Speicher nicht mehr zur Verfügung. In diesem Fall wird NULL zurückgegeben.</p>
<b>MessageCategoryLimit</b>	Gibt die Mindestanzahl von Meldungen des jeweiligen Schweregrads bzw. Kategorie zurück, die unter Verwendung der Systemprozedur <code>sa_server_messages</code> abgerufen werden können. Der Standardwert ist "400". Siehe <a href="#">„sa_server_messages-Systemprozedur“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a> .
<b>MessageText</b>	Diese Eigenschaft ist veraltet. Gibt den Text ohne Datum- und Uhrzeit-Präfix zurück, der im Fenster "Datenbankservermeldungen" der angegebenen Zeilennummer zugeordnet ist. Der zweite Parameter gibt die Zeilennummer an.
<b>MessageTime</b>	Diese Eigenschaft ist veraltet. Gibt das Datum und die Uhrzeit zurück, die im Fenster "Datenbankservermeldungen" der angegebenen Zeilennummer zugeordnet sind. Der zweite Parameter gibt die Zeilennummer an.
<b>MessageWindowSize</b>	Diese Eigenschaft ist veraltet. Gibt die maximale Anzahl der Zeilen zurück, die aus dem Fenster "Datenbankservermeldungen" abgerufen werden können.
<b>MinCacheSize</b>	Gibt die minimal zulässige Cachegröße in Kilobyte zurück.
<b>MinMultiProgrammingLevel</b>	Gibt die minimale Anzahl von Aufgaben zurück, die der Server gleichzeitig ausführen kann. Siehe <a href="#">„Datenbankserverkonfiguration der Multiprogramming-Stufe“ auf Seite 175</a> .
<b>MultiPacketsReceived</b>	Gibt die Anzahl von Mehrfachpaketanforderungen zurück, die während der Client/Server-Kommunikation empfangen wurden.
<b>MultiPacketsSent</b>	Gibt die Anzahl von Mehrfachpaketantworten zurück, die während der Client/Server-Kommunikation gesendet wurden.
<b>MultiPageAllocs</b>	Gibt die Anzahl der Cachezuweisungen von Mehrfachseiten zurück.

Eigenschaftsname	Beschreibung
<b>MultiProgrammingLevel</b>	Gibt die maximale Anzahl der gleichzeitigen Aufgaben zurück, die der Server verarbeiten kann. Anforderungen werden in die Warteschlange gestellt, wenn es mehr gleichzeitige Aufgaben gibt, als der Wert zulässt. Dies kann mit der Serveroption <code>-gn</code> geändert werden. Siehe „ <a href="#">Datenbankserveroption -gn</a> “ auf Seite 244.
<b>Name</b>	<p>Gibt den alternativen Namen des Servers zurück, der für die Verbindung mit der Datenbank verwendet wurde, falls einer angegeben wurde. Anderenfalls wird der echte Servername zurückgegeben. Siehe „<a href="#">Datenbankoption -sn</a>“ auf Seite 332 und <a href="#">ServerName-Servereigenschaft</a> auf Seite 762.</p> <p>Wenn der Client mit einem Kopieknotten verbunden ist und <code>NodeType=COPY</code> in der Verbindungszeichenfolge angegeben hat, ist der Wert dieser Eigenschaft gegebenenfalls anders als der Datenbankname, der in der Clientverbindungszeichenfolge mit dem <code>ServerName</code>-Verbindungsparameter angegeben wurde. Siehe „<a href="#">Verbindungsparameter NodeType (NODE)</a>“ auf Seite 375.</p>
<b>NativeProcessorArchitecture</b>	<p>Gibt eine Zeichenfolge zurück, die den nativen Prozessortyp identifiziert, auf dem die Software läuft. Bei Plattformen, auf denen ein Prozessor emuliert werden kann (z.B. x86 auf x64), wird der tatsächliche Prozessortyp zurückgegeben, nicht der Typ der Betriebssystemarchitektur.</p> <p>Diese Eigenschaft gibt keinen Wert zurück, der anzeigt, ob das System 32 Bit oder 64 Bit ist.</p> <p>Folgende Werte sind möglich:</p> <ul style="list-style-type: none"> <li>• Windows (außer Windows Mobile) - X86 oder X86_64</li> <li>• Windows Mobile - ARM</li> <li>• Solaris - SPARC oder X86_64</li> <li>• AIX - PPC</li> <li>• MAC OS - X86_64</li> <li>• HP - IA64</li> <li>• Linux - X86 oder X86_64</li> </ul> <p>X86 stellt eine 32-Bit-Hardwarearchitektur dar. X86_64 stellt eine 64-Bit-Hardwarearchitektur dar.</p> <p>Siehe auch <a href="#">ProcessorArchitecture-Servereigenschaft</a> auf Seite 758.</p> <p>Weitere Informationen zu unterstützten Plattformen finden Sie unter <a href="http://www.sybase.com/detail?id=1002288">http://www.sybase.com/detail?id=1002288</a>.</p>
<b>NumLogicalProcessors</b>	Gibt die Anzahl der logischen Prozessoren (einschließlich Kerne und Hyperthreads) zurück, die auf dem Servercomputer aktiviert sind.

Eigenschaftsname	Beschreibung
<b>NumLogicalProcessorsUsed</b>	Gibt die Anzahl der logischen Prozessoren zurück, die der Datenbankserver verwenden wird. Unter Windows verwenden Sie die Option -gtc, um die Anzahl der verwendeten logischen Prozessoren zu ändern. Siehe „ <a href="#">Datenbankserveroption -gtc</a> “ auf Seite 253.
<b>NumPhysicalProcessors</b>	Gibt die Anzahl der physischen Prozessoren zurück, die auf dem Servercomputer aktiviert sind. Dieser Wert ist "NumLogicalProcessors" dividiert durch die Anzahl der Kerne oder Hyperthreads pro physischem Prozessor. Auf manchen Nicht-Windows-Plattformen werden möglicherweise Kerne oder Hyperthreads zu den physischen Prozessoren gezählt.
<b>NumPhysicalProcessorsUsed</b>	Gibt die Anzahl der physischen Prozessoren zurück, die der Datenbankserver verwenden wird. Auf einigen Plattformen ist der Personal Server auf vier Prozessorkerne eines Prozessors beschränkt. Unter Windows können Sie die Option -gt verwenden, um die Anzahl der physischen Prozessoren zu ändern, die der Datenbankserver verwendet. Siehe „ <a href="#">Datenbankserveroption -gt</a> “ auf Seite 251.
<b>ObjectType</b>	Gibt den Typ des Datenbankobjekts zurück. Dieser Wert wird von der SYOBJECT-Systemansicht verwendet. Siehe „ <a href="#">SYOBJECT-Systemansicht</a> “ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>OmniIdentifier</b>	Diese Eigenschaft ist für die Verwendung durch das System reserviert. Ändern Sie die Einstellung für diese Eigenschaft nicht.
<b>PacketsReceived</b>	Gibt die Anzahl der empfangenen Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsReceivedUncomp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommunikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsReceived", wenn die Komprimierung deaktiviert ist.)
<b>PacketsSent</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsSentUncomp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommunikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsSent", wenn die Komprimierung deaktiviert ist.)
<b>PageSize</b>	Gibt die Größe der Datenbankserver-Cacheseiten zurück. Sie kann mit der Option -gp gesetzt werden und ist standardmäßig die maximale Datenbank-Seitengröße der in der Befehlszeile angegebenen Datenbanken.

<b>Eigenschaftsname</b>	<b>Beschreibung</b>
<b>PeakCacheSize</b>	Gibt den höchsten Wert zurück, den der Cache in der aktuellen Sitzung erreicht hat, in kB.
<b>Platform</b>	Gibt das Betriebssystem zurück, auf dem die Software läuft. Beispiel: Wenn Sie die Software unter Windows XP ausführen, gibt diese Eigenschaft WindowsXP zurück.
<b>PlatformVer</b>	Gibt das Betriebssystem zurück, auf dem die Software läuft, einschließlich Build-Nummern, Service-Packs etc.
<b>PrepStmt</b>	Gibt die Anzahl der vorbereiteten Anweisungen zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>ProcessCPU</b>	<p>Gibt die CPU-Nutzung für den Datenbankserverprozess zurück. Werte werden in Sekunden angegeben. Diese Eigenschaft wird unter Windows und Unix unterstützt. Diese Eigenschaft wird unter Windows Mobile nicht unterstützt.</p> <p>Der für diese Eigenschaft zurückgegebene Wert ist kumulativ seit dem Start des Datenbankservers. Der Wert stimmt nicht mit dem Momentanwert überein, der von Anwendungen wie dem Windows Task-Manager oder dem Windows-Systemmonitor zurückgegeben wird.</p>
<b>ProcessCPUSystem</b>	<p>Gibt die CPU-Nutzung des Systems für den Datenbankserverprozess-CPU zurück. Dies ist die Menge an CPU-Zeit, die der Datenbankserver im Betriebssystem-Kernel verbracht hat. Werte werden in Sekunden angegeben. Diese Eigenschaft wird unter Windows und Unix unterstützt. Diese Eigenschaft wird unter Windows Mobile nicht unterstützt.</p> <p>Der für diese Eigenschaft zurückgegebene Wert ist kumulativ seit dem Start des Datenbankservers. Der Wert stimmt nicht mit dem Momentanwert überein, der von Anwendungen wie dem Windows-Task-Manager oder Systemmonitor zurückgegeben wird.</p>
<b>ProcessCPUUser</b>	<p>Gibt Benutzer-CPU-Nutzung für den Datenbankserverprozess zurück. Werte werden in Sekunden angegeben. Dies schließt die Menge an CPU-Zeit aus, die der Datenbankserver im Betriebssystem-Kernel verbracht hat. Diese Eigenschaft wird unter Windows und Unix unterstützt. Diese Eigenschaft wird unter Windows Mobile nicht unterstützt.</p> <p>Der für diese Eigenschaft zurückgegebene Wert ist kumulativ seit dem Start des Datenbankservers. Der Wert stimmt nicht mit dem Momentanwert überein, der von Anwendungen wie dem Windows-Task-Manager oder Systemmonitor zurückgegeben wird.</p>
<b>ProcessID</b>	Gibt die Prozesskennung des Datenbankserver-Prozesses zurück.

Eigenschaftsname	Beschreibung
<b>ProcessorAffinity</b>	Gibt die vom Datenbankserver genutzten logischen Prozessoren zurück, wie durch die Option -gta oder durch die sa_server_option-Systemprozedur und die ProcessorAffinity-Option angegeben. Siehe „ <a href="#">Datenbankserveroption -gta</a> “ auf Seite 252 und ProcessorAffinity-Option: „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>ProcessorArchitecture</b>	<p>Gibt eine Zeichenfolge zurück, die den Prozessortyp identifiziert, für den die aktuelle Software entwickelt wurde. Werte sind:</p> <ul style="list-style-type: none"> <li>• Windows (außer Windows Mobile) - X86 oder X86_64</li> <li>• Windows Mobile - ARM</li> <li>• Solaris - SPARC oder X86_64</li> <li>• AIX - PPC</li> <li>• MAC OS - X86_64</li> <li>• HP - IA64</li> <li>• Linux - X86 oder X86_64</li> </ul> <p>X86 stellt einen 32-Bit-Datenbankserver dar. X86_64 stellt einen 64-Bit-Datenbankserver dar.</p> <p>Siehe <a href="#">NativeProcessorArchitecture-Servereigenschaft</a> auf Seite 755.</p>
<b>ProductName</b>	Gibt den Namen der Software zurück.
<b>ProductVersion</b>	Gibt die Version der ausgeführten Software zurück.
<b>ProfileFilterConn</b>	Gibt die ID der Verbindung zurück, die überwacht wird, wenn Prozedurprofilerstellung für eine bestimmte Verbindung aktiviert ist. Anderenfalls wird eine leere Zeichenfolge zurückgegeben. Sie steuern die Prozedurprofilerstellung einzelner Benutzer mit der sa_server_option-Prozedur. Siehe „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>ProfileFilterUser</b>	Gibt die ID des überwachten Benutzers zurück, wenn Prozedurprofilerstellung für einen bestimmten Benutzer aktiviert ist. Anderenfalls wird eine leere Zeichenfolge zurückgegeben. Sie steuern die Prozedurprofilerstellung einzelner Benutzer mit der sa_server_option-Prozedur. Siehe „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>QueryHeapPages</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Cacheseiten zurück.
<b>QueryMemActiveCurr</b>	Gibt die Anzahl der Anforderungen zurück, die den Abfragespeicher aktiv nutzen.

Eigenschaftsname	Beschreibung
<b>QueryMemActiveEst</b>	Gibt die Schätzung des Datenbankservers zum Steadystate-Mittelwert der Anzahl der Anforderungen zurück, die aktiv den Abfragespeicher nutzen.
<b>QueryMemActiveMax</b>	Gibt die maximale Anzahl von Anforderungen zurück, denen die Verwendung des Abfragespeichers explizit erlaubt wurde.
<b>QueryMemExtraAvail</b>	Gibt die Speichermenge zurück, die zusätzlich zur grundlegenden speicherintensiven Bereitstellung verfügbar ist.
<b>QueryMemGrantBase</b>	Gibt die Mindestmenge des Speichers zurück, der für alle Abfragen zugeteilt wird.
<b>QueryMemGrantBase-MI</b>	Gibt die Mindestmenge des Speichers zurück, der für speicherintensive Abfragen zugeteilt wird.
<b>QueryMemGrantExtra</b>	Gibt die Anzahl der Abfragespeicherseiten zurück, die über QueryMemGrantBaseMI hinaus an aktive speicherintensive Anforderungen verteilt werden können.
<b>QueryMemGrantFailed</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Zuweisung von Abfragespeicher gewartet, aber nicht erhalten hat.
<b>QueryMemGrantGranted</b>	Gibt die Anzahl der Seiten zurück, die derzeit für Anforderungen bereitgestellt sind.
<b>QueryMemGrantRequested</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt versucht hat, Abfragespeicher zu erhalten.
<b>QueryMemGrantWaiting</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Speicherzuordnung gewartet hat.
<b>QueryMemGrantWaiting</b>	Gibt die aktuelle Anzahl der Anforderungen zurück, die auf Zuweisung von Abfragespeicher warten.
<b>QueryMemPages</b>	Gibt die Menge an Speicher zurück, der für Algorithmen zur Abfrageausführung verfügbar ist, ausgedrückt als eine Seitenanzahl.
<b>QueryMemPercentOf-Cache</b>	Gibt die Menge an Speicher zurück, der für Algorithmen zur Abfrageausführung verfügbar ist, ausgedrückt als Prozentsatz der maximalen Cachegröße.
<b>QuittingTime</b>	Gibt die Uhrzeit zum Herunterfahren des Servers zurück. Wenn keine angegeben ist, ist der Wert "none".

Eigenschaftsname	Beschreibung
<b>RememberLastPlan</b>	Gibt "Yes" zurück, wenn der Server den letzten vom Optimierer zurückgegebenen Abfrageplan aufzeichnet. Siehe „ <a href="#">Datenbankserveroption -zp</a> “ auf Seite 316.
<b>RememberLastState-ment</b>	Gibt "Yes" zurück, wenn der Server die letzte für die jeweilige Verbindung vorbereitete Anweisung aufzeichnet. Anderenfalls wird "No" zurückgegeben. Siehe „ <a href="#">Datenbankserveroption -zl</a> “ auf Seite 313.
<b>RemoteCapability</b>	Gibt den entfernten Funktionsnamen zurück, der mit einer bestimmten Funktionalitäts-ID verknüpft ist.
<b>RemoteputWait</b>	Gibt die Häufigkeit zurück, mit der der Server beim Senden eines Kommunikationspakets blockieren musste. Normalerweise tritt eine Blockierung nur auf, wenn der Datenbankserver Daten schneller sendet, als der Client oder das Netzwerk sie empfangen kann. Es ist kein Hinweis auf eine Fehlerbedingung.
<b>Req</b>	Gibt die Anzahl der Einstiege in den Server zurück, damit er eine neue Anforderung verarbeiten oder die Verarbeitung einer laufenden Anforderung fortsetzen kann.
<b>ReqCountActive</b>	Gibt die Anzahl der Einstiege in den Server zurück, damit er eine neue Anforderung verarbeiten oder die Verarbeitung einer laufenden Anforderung fortsetzen kann.
<b>ReqCountBlockCon-tention</b>	Gibt zurück, wie oft eine beliebige Verbindung aufgrund von Konflikten um eine interne Serverressource blockiert hat.
<b>ReqCountBlockIO</b>	Gibt zurück, wie oft eine beliebige Verbindung beim Warten auf den Abschluss einer I/O-Anforderung blockiert hat.
<b>ReqCountBlockLock</b>	Gibt zurück, wie oft eine beliebige Verbindung beim Warten auf eine von einer anderen Verbindung gesetzten Zeilensperre blockiert hat.
<b>ReqCountUnscheduled</b>	Gibt zurück, wie oft eine beliebige Verbindung beim Warten auf die Verarbeitung durch einen Server-Thread blockiert hat.
<b>ReqTimeActive</b>	Gibt die gesamte Zeit zurück, die der Server direkt für die Bearbeitung von Anforderungen benötigt hat.
<b>ReqTimeBlockConten-tion</b>	Gibt die gesamte Zeit zurück, die eine beliebige Verbindung aufgrund von Konflikten um eine interne Serverressource blockiert hat.
<b>ReqTimeBlockIO</b>	Gibt die gesamte Zeit zurück, die eine beliebige Verbindung beim Warten auf den Abschluss einer I/O-Anforderung blockiert hat.

Eigenschaftsname	Beschreibung
<b>ReqTimeBlockLock</b>	Gibt die gesamte Zeit zurück, die eine beliebige Verbindung beim Warten auf eine von einer anderen Verbindung gesetzte Zeilensperre blockiert hat.
<b>ReqTimeUnscheduled</b>	Gibt die gesamte Zeit zurück, die eine beliebige Verbindung beim Warten auf die Verarbeitung durch einen Server-Thread blockiert hat.
<b>RequestFilterConn</b>	Gibt die ID der Verbindung zurück, deren Protokollierungsinformationen gefiltert werden. Anderenfalls wird "-1" zurückgegeben.
<b>RequestFilterDB</b>	Gibt die ID der Datenbank zurück, deren Protokollierungsinformationen gefiltert werden. Anderenfalls wird "-1" zurückgegeben.
<b>RequestLogFile</b>	Gibt den Namen der Datei für die Anforderungsprotokollierung zurück. Eine leere Zeichenfolge wird zurückgegeben, wenn es keine Anforderungsprotokollierung gibt. Siehe „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>RequestLogging</b>	Gibt einen der Werte SQL, PLAN, HOSTVARS, PROCEDURES, TRIGGERS, OTHER, BLOCKS, REPLACE, ALL oder NONE zurück, der die aktuelle Einstellung für die Anforderungsprotokollierung angibt. Siehe „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>RequestLogMaxSize</b>	Gibt die maximale Größe der Anforderungs-Logdatei zurück. Siehe „Datenbankserveroption -zs“ auf Seite 319.
<b>RequestLogNumFiles</b>	Gibt die Anzahl der aufbewahrten Anforderungs-Logdateien zurück. Siehe „sa_server_option-Systemprozedur“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>RequestsReceived</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationsanforderungen oder Roundtrips zurück. Dies unterscheidet sich von PacketsReceived, da Mehrfachpaketanforderungen als eine Anforderung zählen und Verfügbarkeitspakete nicht aufgenommen werden.
<b>RequestTiming</b>	Gibt "Yes" zurück, wenn Anforderungszeit aktiviert ist. Anderenfalls wird "No" zurückgegeben. Anforderungszeit wird mit der Serveroption -zt aktiviert. Siehe „Datenbankserveroption -zt“ auf Seite 319.
<b>Rlbk</b>	Gibt die Anzahl der Rollback-Anforderungen zurück, die verarbeitet wurden.
<b>SendFail</b>	Gibt die Häufigkeit zurück, mit der die zugrunde liegenden Kommunikationsprotokolle Pakete nicht senden konnten.

Eigenschaftsname	Beschreibung
<b>ServerEdition</b>	<p>Gibt eine mit Leerschritten getrennte Liste von Wörtern zurück, die den Datenbankservertyp beschreiben. Werte sind:</p> <ul style="list-style-type: none"> <li>• Evaluation</li> <li>• Developer</li> <li>• Web</li> <li>• Educational</li> <li>• Standard</li> <li>• Advanced</li> <li>• Workgroup</li> <li>• OEM</li> <li>• Authenticated</li> </ul> <p>Wenn Sie eine separate Lizenz für die folgenden Funktionen haben, werden die entsprechenden Zeichenfolgen der zurückgegebenen Lizenzzeichenfolge hinzugefügt:</p> <ul style="list-style-type: none"> <li>• HighAvailability</li> <li>• InMemory</li> <li>• FIPS</li> </ul> <p>Siehe „Getrennt lizenzierbare Komponenten“ [<a href="#">SQL Anywhere 16 - Einführung</a>].</p>
<b>ServerName</b>	Gibt den echten Servernamen zurück (niemals einen alternativen Servernamen). Anhand dieses Werts können Sie bestimmen, welcher der betriebsbereiten Server als Primärserver in einer Datenbankspiegelungs-Konfiguration agiert. Siehe „ <a href="#">Datenbankspiegelung</a> “ auf Seite 1467.
<b>StartDBPermission</b>	Gibt die Einstellung der Serveroption -gd zurück, die "DBA", "all" oder "none" sein kann. Siehe „ <a href="#">Datenbankserveroption -gd</a> “ auf Seite 240.
<b>StartTime</b>	Gibt den Datums-/Zeitwert des Serverstarts zurück.
<b>StreamsUsed</b>	Gibt die Anzahl der zu verwendenden Datenbankserver-Datenströme zurück.
<b>TcpIpAddresses</b>	<p>Gibt eine durch Semikola getrennte Liste der TCP/IP-Adressen zurück, die der Datenbankserver bei Befehlssequenz- und TDS-Verbindungen abhört. Zum Beispiel:</p> <p>(::1):2638;127.0.0.1:2638</p>
<b>TempDir</b>	Gibt das Verzeichnis zurück, in dem vom Server temporäre Dateien gespeichert werden.

Eigenschaftsname	Beschreibung
<b>ThreadDeadlocksAvoided</b>	<p>Gibt die Häufigkeit zurück, mit der ein Thread-Deadlock-Fehler erkannt, aber nicht an Clientanwendungen gemeldet wurde. Wenn der Datenbankserver gestartet wird, ist der Wert für diese Eigenschaft 0.</p> <p>Um die Rückgabe von Thread-Deadlock-Fehlern zu vermeiden, erhöht die Datenbank dynamisch die Multiprogramming-Stufe. Wenn die Multiprogramming-Stufe nicht erhöht werden kann, wird ein Thread-Deadlock-Fehler an die Clientanwendung gemeldet und die ThreadDeadlocksReported-Eigenschaft wird erhöht. Die ThreadDeadlocksAvoided-Eigenschaft ist immer 0 auf dem Personal Server, weil die dynamische Abstimmung der Multiprogramming-Stufe standardmäßig deaktiviert ist.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Datenbankserverkonfiguration der Multiprogramming-Stufe</a>“ auf Seite 175.</p>
<b>ThreadDeadlocksReported</b>	Gibt die Häufigkeit zurück, mit der ein Thread-Deadlock-Fehler an Clientanwendungen gemeldet wurde. Wenn der Datenbankserver startet, ist der Wert für diese Eigenschaft 0.
<b>TimeZoneAdjustment</b>	Gibt die Anzahl der Minuten zurück, die der Coordinated Universal Time (UTC) hinzugefügt werden müssen, um die für den Server lokale Uhrzeit anzuzeigen.
<b>TotalBuffers</b>	Gibt die Gesamtanzahl der Netzwerkpuffer zurück.
<b>UniqueClientAddresses</b>	Gibt die Anzahl der mit einem Server verbundenen eindeutigen Client-Netzwerkadressen zurück.
<b>UnschReq</b>	Gibt die Anzahl der Anforderungen zurück, die derzeit in einer Warteschlange auf einen verfügbaren Server-Worker warten.
<b>UserDefinedCounterRate01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounter-Rate02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Rate03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Rate04</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Rate05</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Raw01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounter-Raw02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounter-Raw03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounter-Raw04</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>UserDefinedCounter-Raw05</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Benutzerdefinierte Eigenschaften</a>“ auf Seite 789.</p>
<b>WebClientLogFile</b>	Gibt den Namen der Client-Logdatei des Webdiensts zurück. Siehe „ <a href="#">Datenbankserveroption -zoc</a> “ auf Seite 315.
<b>WebClientLogging</b>	Gibt einen Wert zurück, der angibt, ob Webdienst-Clientinformationen in einer Datei protokolliert werden. Siehe „ <a href="#">Datenbankserveroption -zoc</a> “ auf Seite 315.

## Zugreifen auf Werte von Datenbankeigenschaften

Datenbankeigenschaften sind für jede Datenbank auf dem Datenbankserver verfügbar. Sie können die DB\_PROPERTY-Systemfunktion verwenden, um den Wert für eine einzelne Eigenschaft abzurufen, oder die sa\_db\_properties-Systemprozedur, um die Werte aller Datenbankseigenschaften abzurufen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Bei Eigenschaftsnamen wird die Groß- und Kleinschreibung nicht berücksichtigt.

### Aufgabe

- Verwenden Sie eine der folgenden Methoden, um auf Werte von Datenbankeigenschaften zuzugreifen:

Option	Aktion
Wert einer Datenbankeigenschaft abrufen	Verwenden Sie die DB_PROPERTY-Systemfunktion.
Werte aller Datenbankeigenschaften abrufen	Verwenden Sie die sa_db_properties-Systemprozedur.

### Ergebnisse

Der Wert der Datenbankeigenschaft wird zurückgegeben.

### Beispiel

Die folgende Anweisung gibt die Seitengröße der aktuellen Datenbank zurück:

```
SELECT DB_PROPERTY ( 'PageSize' );
```

Verwenden Sie die sa\_db\_properties-Systemprozedur, um die Werte aller Datenbankeigenschaften abzurufen:

```
CALL sa_db_properties;
```

### Siehe auch

- „DB\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_db\_properties-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DB\_EXTENDED\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Liste der Datenbankeigenschaften“ auf Seite 767
- „Liste der Datenbankseigenschaften“ auf Seite 745
- „Liste der Verbindungseigenschaften“ auf Seite 711

## Liste der Datenbankeigenschaften

### Datenbankeigenschaften

Eigenschaftsname	Beschreibung
<b>AccentSensitive</b>	Gibt den Status der Akzent-Berücksichtigungsfunktion zurück. Gibt "On" zurück, wenn die Datenbank Akzente berücksichtigt, "Off", wenn das nicht der Fall ist, und "FRENCH", wenn die französischen Regeln zur Akzent-Berücksichtigung verwendet werden.
<b>Alias</b>	Gibt den Datenbanknamen zurück.
<b>AlternateMirrorServerName</b>	Gibt den der Datenbank zugeordneten alternativen Spiegelservernamen zurück, falls einer angegeben wurde. Siehe „ <a href="#">Datenbankoption -sm (nicht mehr empfohlen)</a> “ auf Seite 331.
<b>AlternateServerName</b>	Gibt den der Datenbank zugeordneten alternativen Servernamen zurück, falls einer angegeben wurde. Siehe „ <a href="#">Datenbankoption -sn</a> “ auf Seite 332.
<b>ApproximateCPUTime</b>	Gibt eine Schätzung der CPU-Zeit in Sekunden zurück, die von der Datenbank genutzt wurde. Der zurückgegebene Wert kann sich vom tatsächlichen Wert um bis zu 50% unterscheiden, auch wenn übliche Abweichungen im Bereich von 5 - 10 % liegen. Auf Mehrprozessorcomputern akkumuliert jede CPU (bzw. jeder Hyperthread oder Kern) Zeit, daher kann die Summe der akkumulierten Zeit größer als die verstrichene Zeit sein. Diese Eigenschaft wird unter Windows und Linux unterstützt.
<b>ArbiterState</b>	Gibt einen der folgenden Werte zurück: <ul style="list-style-type: none"> <li>• <b>NULL</b> Sie sind mit einer Datenbank verbunden, die nicht gespiegelt wird.</li> <li>• <b>connected</b> Der Arbiterserver ist mit dem Primärserver verbunden.</li> <li>• <b>disconnected</b> Der Arbiterserver ist nicht mit dem Primärserver verbunden.</li> </ul> <p>Siehe „<a href="#">Datenbankspiegelung</a>“ auf Seite 1467.</p>
<b>AuditingTypes</b>	Gibt die derzeit aktivierten Auditingtypen zurück. Siehe „ <a href="#">auditing-Option</a> “ auf Seite 582.
<b>Authenticated</b>	Gibt "Yes" zurück, wenn die Datenbank authentifiziert wurde, und "No", wenn die Datenbank nicht authentifiziert wurde.
<b>BlankPadding</b>	Gibt "On" zurück, wenn für die Datenbank die Leerzeichenauffüllung aktiviert ist. Anderenfalls wird "Off" zurückgegeben.

Eigenschaftsname	Beschreibung
<b>BytesReceived</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesReceivedUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. Dieser Wert ist derselbe wie für "BytesReceived", wenn die Komprimierung deaktiviert ist.
<b>BytesSent</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet wurden. Dieser Wert wird für HTTP- und HTTPS-Verbindungen aktualisiert.
<b>BytesSentUncomp</b>	Gibt die Anzahl von Bytes zurück, die während der Client/Server-Kommunikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. Dieser Wert ist derselbe wie für "BytesSent", wenn die Komprimierung deaktiviert ist.
<b>CacheHits</b>	Gibt die Anzahl der Suchvorgänge nach Datenbankseiten zurück, die durch eine im Cache gefundene Seite belohnt wurden.
<b>CacheRead</b>	Gibt die Anzahl der Datenbankseiten zurück, die im Cache nachgeschlagen wurden.
<b>CacheReadIndInt</b>	Gibt die Anzahl der internen Knotenseiten des Indexes zurück, die aus dem Cache gelesen wurden.
<b>CacheReadIndLeaf</b>	Gibt die Anzahl der Indexblattseiten zurück, die aus dem Cache gelesen wurden.
<b>CacheReadTable</b>	Gibt die Anzahl der Tabellenseiten zurück, die aus dem Cache gelesen wurden.
<b>CacheReadWorkTable</b>	Gibt die Anzahl der Cache-Arbeitstabellen-Lesevorgänge zurück.
<b>Capabilities</b>	Gibt die für die Datenbank aktivierten Funktionalitätsbits zurück. Diese Eigenschaft ist hauptsächlich für die Verwendung durch den technischen Support bestimmt.
<b>CarverHeapPages</b>	Gibt die Anzahl der Blattseiten zurück, die für kurzzeitige Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.

Eigenschaftsname	Beschreibung
<b>CaseSensitive</b>	Gibt den Status der Berücksichtigungsfunktion für Groß- und Kleinschreibung zurück. Gibt "On" zurück, wenn die Datenbank die Groß- und Kleinschreibung berücksichtigt. Anderenfalls wird "Off" zurückgegeben. In Datenbanken, die die Groß- und Kleinschreibung berücksichtigen, berücksichtigen Datenvergleiche die Groß- und Kleinschreibung. Diese Einstellung wirkt sich nicht auf die Berücksichtigung von Groß- und Kleinschreibung bei Bezeichnern aus. Kennwörter unterscheiden immer zwischen Groß- und Kleinschreibung. Siehe „Groß-/Kleinschreibung“ [ <a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a> ].
<b>CatalogCollation</b>	Gibt den im Katalog verwendeten Bezeichner für die Kollation zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „DB_EXTENDED_PROPERTY-Funktion [System]“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>CharSet</b>	Gibt den CHAR-Zeichensatz der Datenbank zurück.  Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „DB_EXTENDED_PROPERTY-Funktion [System]“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>CheckpointLogCommitToDisk</b>	Gibt die Anzahl der Checkpoint-Log-Festschreibungen auf Festplatte zurück.
<b>CheckpointLogPagesInUse</b>	Gibt die Anzahl der verwendeten Checkpoint-Log-Seiten zurück.
<b>CheckpointLogPagesRelocated</b>	Gibt die Anzahl der verschobenen Checkpoint-Log-Seiten zurück.
<b>CheckpointLogPagesWritten</b>	Gibt die Anzahl der geschriebenen Checkpoint-Log-Seiten zurück.
<b>CheckpointLogSavePreimage</b>	Gibt die Anzahl von Pre-Images von Datenbankseiten zurück, die dem Checkpoint-Log hinzugefügt werden.
<b>CheckpointLogSize</b>	Gibt die Größe des Checkpoint-Logs zurück, in Seiten.
<b>CheckpointLogWrites</b>	Gibt die Anzahl der Schreibvorgänge in das Checkpoint-Log zurück.
<b>CheckpointUrgency</b>	Gibt die Zeit, die seit dem letzten Checkpoint verstrichen ist, als einen Prozentsatz der Checkpoint-Zeiteinstellung der Datenbank zurück.

Eigenschaftsname	Beschreibung
<b>Checksum</b>	Gibt On zurück, wenn globale Prüfsummen für die Datenbank aktiviert sind (eine Prüfsumme wird für jede Datenbankseite erstellt). Anderenfalls wird "Off" zurückgegeben. Prüfsummen sind bei kritischen Seiten immer aktiviert.
<b>Chkpt</b>	Gibt die Anzahl der Checkpoints zurück, die durchgeführt wurden.
<b>ChkptFlush</b>	Gibt die Anzahl der Bereiche benachbarter Seiten zurück, die während eines Checkpoints ausgelesen werden.
<b>ChkptPage</b>	Gibt die Anzahl der Transaktionslog-Checkpoints zurück.
<b>CleanablePagesAdded</b>	Gibt die Anzahl der Seiten zurück, die seit dem Datenbankserver-Start zum Bereinigen markiert wurden.
<b>CleanablePagesCleaned</b>	Gibt die Anzahl der Datenbankseiten zurück, die seit dem Datenbankserver-Start bereinigt wurden.
<b>CleanableRowsAdded</b>	Gibt die Anzahl der Zeilen zurück, die seit dem Datenbankserver-Start zum Löschen markiert wurden.
<b>CleanableRowsCleaned</b>	Gibt die Anzahl der Schattentabellenzeilen zurück, die seit dem Datenbankserver-Start gelöscht wurden.
<b>ClientStmtCacheHits</b>	Gibt die Anzahl der Vorbereitungen zurück, die aufgrund des Clientanweisungscache für diese Datenbank nicht erforderlich waren. Dies ist die Anzahl der Vorbereitungen, die erforderlich wären, wenn das clientseitige Caching von Anweisungen deaktiviert wäre. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>ClientStmtCacheMisses</b>	Gibt die Anzahl der Anweisungen im Clientanweisungscache dieser Datenbank zurück, die erneut vorbereitet wurden. Dies ist die Angabe, wie oft eine zwischengespeicherte Anweisung für die Wiederverwendung in Frage kam, aber aufgrund einer Schemaänderung, einer Datenbank-Optionseinstellung oder einer DROP VARIABLE-Anweisung nicht wieder verwendet werden konnte. Siehe „ <a href="#">max_client_statements_cached-Option</a> “ auf Seite 629.
<b>Collation</b>	<p>Gibt die von der Datenbank verwendete Kollation zurück. Eine Liste der verfügbaren Kollationen finden Sie unter „<a href="#">Alternative Kollationen</a>“ auf Seite 518.</p> <p>Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>

Eigenschaftsname	Beschreibung
<b>Commit</b>	Gibt die Häufigkeit zurück, mit der der Server eine Leerung des Festplattencaches erzwungen hat. Unter Windows ist ein Leeren des Caches nicht erforderlich, da ungepufferte (direkte) I/O-Vorgänge verwendet werden.
<b>CommitFile</b>	Gibt die Häufigkeit zurück, mit der der Server eine Leerung des Festplattencaches erzwungen hat. Unter Windows ist ein Leeren des Caches nicht erforderlich, da ungepufferte (direkte) I/O-Vorgänge verwendet werden.
<b>ConnCount</b>	<p>Gibt die Anzahl der Verbindungen zur Datenbank zurück. Der Eigenschaftswert enthält keine Verbindungen, die zum Auslösen von internen Vorgängen verwendet werden. Verbindungen für Ereignisse und externe Umgebungen sind hingegen enthalten.</p> <p>Wenn Sie die genaue Anzahl genutzter lizenzierter Verbindungen abrufen möchten, führen Sie folgende Anweisung aus:</p> <pre>SELECT COUNT( * ) FROM sa_conn_info( ) WHERE number &lt; 100000000;</pre>
<b>ConnectedTime</b>	<p>Gibt in Sekunden an, wie lange alle Verbindungen mit der Datenbank aktiv waren.</p> <p>Der Wert wird nur aktualisiert, wenn eine Anforderung abgeschlossen für eine Verbindung wird oder wenn eine Verbindung getrennt wird. Daher kann der Wert für Verbindungen, die inaktiv sind oder seit längerer Zeit im Datenbankserver ausgeführt werden, nicht aktuell sein. Der Wert beinhaltet die Zeit, die sich von beliebigen Verbindungen angesammelt hat, einschließlich Datenbankereignissen und Hintergrundserververbindungen (z.B. Datenbankaufräumvorgang).</p>
<b>ConnPoolCached-Count</b>	Gibt die Anzahl von Verbindungen zurück, die von der Anwendung getrennt, aber für den Verbindungspool im Cache zwischengespeichert wurden.
<b>ConnPoolHits</b>	Gibt die Anzahl der wiederbenutzten Verbindungen im Pool zurück.
<b>ConnPoolMisses</b>	Gibt die Anzahl von Verbindungen im Pool zurück, die zwischengespeichert, aber nicht wiederverwendet werden konnten.
<b>ConnsDisabled</b>	Gibt "On" zurück, wenn Verbindungen zur aktuellen Datenbank deaktiviert sind. Anderenfalls wird "Off" zurückgegeben.
<b>CopyNodeParent</b>	Gibt den Namen des aktuellen übergeordneten Servers für einen Kopieknoten in einem Scale-Out-System mit Schreibschutz zurück.
<b>CurrentRedoPos</b>	Gibt das aktuelle Offset in der Transaktionslogdatei zurück, an dem der nächste Datenbankvorgang protokolliert werden soll.

Eigenschaftsname	Beschreibung
<b>CurrIO</b>	Gibt die aktuelle Anzahl von Datei-I/O-Vorgängen zurück, die vom Server ausgegeben, aber noch nicht abgeschlossen wurden.
<b>CurrRead</b>	Gibt die aktuelle Anzahl von Datei-Lesevorgängen zurück, die vom Server ausgegeben, aber noch nicht abgeschlossen wurden.
<b>CurrWrite</b>	Gibt die aktuelle Anzahl von Datei-Schreibvorgängen zurück, die vom Server ausgegeben, aber noch nicht abgeschlossen wurden.
<b>Cursor</b>	Gibt die Häufigkeit zurück, mit der der Server eine Leerung des Festplattencaches erzwungen hat. Unter Windows ist ein Leeren des Caches nicht erforderlich, da ungepufferte (direkte) I/O-Vorgänge verwendet werden.
<b>CursorOpen</b>	Gibt die Häufigkeit zurück, mit der der Server eine Leerung des Festplattencaches erzwungen hat. Unter Windows ist ein Leeren des Caches nicht erforderlich, da ungepufferte (direkte) I/O-Vorgänge verwendet werden.
<b>DatabaseCleaner</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob der Datenbankaufräuvorgang aktiviert ist.
<b>DBFileFragments</b>	Gibt die Anzahl der Datenbankdateifragmente zurück. Diese Eigenschaft wird unter Windows unterstützt.
<b>DiskRead</b>	Gibt die Anzahl der Seiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadHint</b>	Gibt die Anzahl der Hints für Festplattenlesevorgänge zurück.
<b>DiskReadHintPages</b>	Gibt die Anzahl der Hintseiten für Festplattenlesevorgänge zurück.
<b>DiskReadIndInt</b>	Gibt die Anzahl der internen Knotenseiten des Indexes zurück, die von der Festplatte gelesen wurden.
<b>DiskReadIndLeaf</b>	Gibt die Anzahl der Indexblattseiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadTable</b>	Gibt die Anzahl der Tabellenseiten zurück, die von der Festplatte gelesen wurden.
<b>DiskReadWorkTable</b>	Gibt die Anzahl der Festplatten-Arbeitstabellen-Lesevorgänge zurück.
<b>DiskRetryReadScatter</b>	Gibt die Anzahl der Festplattenlese-Neuersuche für verteilte Lesevorgänge zurück.
<b>DiskSandbox</b>	Gibt "On" oder "Off" zurück, um anzuzeigen, ob Dateivorgänge der Datenbank mit Lese-/Schreibzugriff auf das Verzeichnis beschränkt sind, in dem sich die Hauptdatenbankdatei befindet. Siehe „ <a href="#">Datenbankoption - sbx</a> “ auf Seite 330.

Eigenschaftsname	Beschreibung
<b>DiskSyncRead</b>	Gibt die Anzahl der synchron ausgegebenen Festplattenlesevorgänge zurück.
<b>DiskSyncWrite</b>	Gibt die Anzahl der synchron ausgegebenen Schreibvorgänge zurück.
<b>DiskWaitRead</b>	Gibt zurück, wie oft der Datenbankserver auf einen asynchronen Lesevorgang gewartet hat.
<b>DiskWaitWrite</b>	Gibt zurück, wie oft der Datenbankserver auf einen asynchronen Schreibvorgang gewartet hat.
<b>DiskWrite</b>	Gibt die Anzahl der geänderten Seiten zurück, die auf die Festplatte geschrieben wurden.
<b>DiskWriteHint</b>	Gibt die Anzahl der Hints für Festplattenschreibvorgänge zurück.
<b>DiskWriteHintPages</b>	Gibt die Anzahl der Hints für Festplatten-Sammelschreibvorgänge zurück.
<b>DriveBus</b>	<p>Gibt den Typ des Busses zurück, mit dem die Datenbankdatei verbunden ist. Der Wert ist einer der folgenden:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• SCSI</li> <li>• ATAPI</li> <li>• ATA</li> <li>• 1394</li> <li>• SSA</li> <li>• Fibre</li> <li>• USB</li> <li>• RAID</li> <li>• iSCSI</li> <li>• SAS</li> <li>• SATA</li> <li>• SD</li> <li>• MMC</li> <li>• Virtual</li> <li>• FileBackedVirtual</li> </ul> <p>Wenn der Bustyp nicht ermittelt werden kann, gibt diese Eigenschaft NULL zurück.</p> <p>Der Wert dieser Eigenschaft für den primären DBSpace ist in der SYS-HISTORY-Ansicht registriert. Siehe „SYSHISTORY-Systemansicht“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>

Eigenschaftsname	Beschreibung
<b>DriveModel</b>	<p>Gibt die Modellnummer des Laufwerks zurück, auf dem die Datenbankdatei untergebracht ist. Der Wert dieser Eigenschaft für den primären DBSpace ist in der SYSHISTORY-Ansicht registriert. Siehe „<a href="#">SYSHISTORY-Systemansicht</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p> <p>Wenn das Laufwerkmodell nicht ermittelt werden kann, gibt diese Eigenschaft NULL zurück.</p>
<b>DriveType</b>	<p>Gibt das Speichermedium zurück, auf dem die Datenbankdatei untergebracht ist. Der Wert ist einer der folgenden:</p> <ul style="list-style-type: none"> <li>• CD</li> <li>• FIXED</li> <li>• RAMDISK</li> <li>• REMOTE</li> <li>• REMOVABLE</li> <li>• UNKNOWN</li> </ul> <p>Unter Unix ist es, abhängig von der Unix-Version und dem Speichermedium, möglicherweise nicht möglich, das Speichermedium zu bestimmen. In diesen Fällen wird UNKNOWN zurückgegeben.</p> <p>Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>
<b>Encryption</b>	Gibt den für Datenbank- oder Tabellenverschlüsselung verwendeten Verschlüsselungstyp zurück: None, Simple, AES, AES256, AES_FIPS oder AES256_FIPS.
<b>EncryptionScope</b>	<p>Gibt den Teil der Datenbank zurück, der verschlüsselt werden kann (falls vorhanden). Der Wert ist einer der folgenden: TABLE, DATABASE oder NONE.</p> <p>TABLE gibt an, dass die Tabellenverschlüsselung aktiviert ist. DATABASE gibt an, dass die gesamte Datenbank verschlüsselt ist. NONE gibt an, dass die Tabellenverschlüsselung nicht aktiviert und die Datenbank nicht verschlüsselt ist.</p>
<b>ExprCacheAbandons</b>	Gibt zurück, wie oft der Ausdruckcache vollständig aufgegeben wurde, weil die Trefferrate zu niedrig war.
<b>ExprCacheDropsTo-ReadOnly</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache auf den schreibgeschützten Status zurückfiel, weil die Trefferrate niedrig war.
<b>ExprCacheEvicts</b>	Gibt die Anzahl der aus dem Ausdruckcache entfernten Einträge zurück.

Eigenschaftsname	Beschreibung
<b>ExprCacheHits</b>	Gibt die Anzahl der Treffer im Ausdruckcache zurück.
<b>ExprCacheInserts</b>	Gibt die Anzahl der in den Ausdruckcache eingetragenen Werte zurück.
<b>ExprCacheLookups</b>	Gibt die Anzahl der Suchvorgänge im Ausdruckcache zurück.
<b>ExprCacheResume-OfReadWrite</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache in den schreibgeschützten Status wechselte, weil die Trefferrate zunahm.
<b>ExprCacheStarts</b>	Gibt die Häufigkeit zurück, mit der der Ausdruckcache gestartet wurde.
<b>ExtendDB</b>	Gibt die Anzahl der Seiten zurück, um die die Datenbankdatei erweitert wurde.
<b>ExtendTempWrite</b>	Gibt die Anzahl der Seiten zurück, um die temporäre Dateien erweitert wurden.
<b>File</b>	<p>Gibt den Dateinamen der Datenbank-Stammdatei einschließlich des Pfads zurück.</p> <p>Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>
<b>FileSize</b>	Gibt die Dateigröße des System-DBSpace (in Seiten) zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „ <a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>FreePages</b>	<p>Gibt die Anzahl der freien Seiten im System-DBSpace zurück. Die Eigenschaft FreePages wird nur in Datenbanken unterstützt, die mit Version 8.0.0 oder höher erstellt wurden.</p> <p>Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „<a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>
<b>FullCompare</b>	Gibt die Anzahl der Vergleiche zurück, die über den Hash-Wert hinaus in einem Index durchgeführt wurden.
<b>GetData</b>	Gibt die Anzahl der GETDATA-Anforderungen zurück.
<b>GlobalDBID</b>	Gibt den Wert der Option global_database_id zurück, mit der eindeutige Primärschlüsselwerte in einer Replikationsumgebung generiert werden können.

Eigenschaftsname	Beschreibung
<b>HasCollationTailoring</b>	Gibt einen Wert zurück, der angibt, ob bei der Datenbankerstellung Optionen der Kollationsanpassung angegeben wurden. Mögliche Werte sind "On" oder "Off".
<b>HasEndianSwapFix</b>	Gibt einen Wert zurück, der angibt, ob die Datenbank Big-endian und Little-endian UTF-16-Kodierung auf allen Plattformen unterstützt, unabhängig von der Endianness der Plattform. Mögliche Werte sind "On" oder "Off".
<b>HashForcedPartitions</b>	Gibt die Häufigkeit zurück, mit der ein Hash-Operator zur Teilung gezwungen war, weil um Speicher konkurriert wurde.
<b>HashRowsFiltered</b>	Gibt die Anzahl der von Bitvektorfiltren zurückgewiesenen Suchzeilen zurück.
<b>HashRowsPartitioned</b>	Gibt die Anzahl der in Hash-Arbeitstabellen geschriebenen Zeilen zurück.
<b>HashWorkTables</b>	Gibt die Anzahl der für Hash-basierte Vorgänge erstellten Arbeitstabellen zurück.
<b>HasNCHARLegacy-CollationFix</b>	<p>Gibt einen der folgenden Werte zurück:</p> <ul style="list-style-type: none"><li>● <b>ON</b> Für alle Datenbanken, die ab Version 11 erstellt wurden, sowie Datenbanken, die von einem Datenbankserver der Version 10 mit der Fehlerbehebung für veraltete Kollationen erstellt wurden und eine veraltete NCHAR-Kollation verwenden.</li><li>● <b>OFF</b> Für Datenbanken, die von einem Datenbankserver der Version 10 ohne Reparaturprogramm für veraltete Kollationen erstellt wurden, oder Datenbanken, die mit einem Datenbankserver der Version 10 erstellt wurden und keine veraltete NCHAR-Kollation verwenden.</li></ul>
<b>HasTornWriteFix</b>	Gibt einen Wert zurück der angibt, ob die Datenbank ein festes Dateiformat hat, um eine Wiederherstellung nach teilweisen Schreibvorgängen zu ermöglichen.
<b>HeapsCarver</b>	Gibt die Anzahl der Heaps zurück, die für kurzzeitige Zwecke, wie z.B. Abfrageoptimierung, verwendet wurden.
<b>HeapsLocked</b>	Gibt die Anzahl von neu positionierbaren, derzeit im Cache gesperrten Heaps zurück.
<b>HeapsQuery</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Heaps zurück.
<b>HeapsRelocatable</b>	Gibt die Anzahl von neu positionierbaren Heaps zurück.

Eigenschaftsname	Beschreibung
<b>HttpConnPoolCached-Count</b>	Gibt die absolute Anzahl der im Cache gespeicherten Datenbankverbindungen in allen Pools zurück.
<b>HttpConnPoolHits</b>	Gibt die Rate der Verbindungen zurück, die von demselben Dienst wieder verwendet werden.
<b>HttpConnPoolMisses</b>	Gibt die Rate der neue Verbindungen zurück, die zugewiesen wurden, als auf eine Verbindung nicht aus einem Pool zugegriffen werden konnte. Diese Eigenschaft zählt nur HTTP-Anforderungen auf Dienste, die Verbindungspools verwenden. Zum Zeitpunkt des Zugriffs war möglicherweise keine Verbindung verfügbar, weil der Pool zu klein war und die älteste Verbindung die Kriterien für eine Übernahme nicht erfüllte.
<b>HttpConnPoolSteals</b>	<p>Gibt zurück, wie viele Verbindungen von Diensten übernommen werden, wobei die Verbindung zu einem anderen Dienst gehörte.</p> <p>Der Dienst übernimmt eine Verbindung von einem anderen Dienst, wenn die Kriterien erfüllt sind, dass eine HTTP-Anforderung für einen Dienst vorliegt, der keine direkt verwendbaren Verbindungen hat, die Poolgröße klein ist und die zuletzt benutzte Verbindung alt ist.</p> <p>Eine Verbindung wird für den Dienst zugewiesen und der Wert für HttpConnPoolMisses wird stattdessen erhöht, wenn die Poolkriterien nicht erfüllt sind.</p>
<b>IdentitySignature</b>	Diese Eigenschaft ist nur für den internen Gebrauch gedacht.
<b>IdleCheck</b>	Gibt die Häufigkeit zurück, mit der der Leerlauf-Thread des Datenbankservers aktiv wurde, um Leerlauf-Schreibvorgänge, Leerlauf-Checkpoints etc. auszuführen.
<b>IdleChkpt</b>	Gibt die Anzahl der Checkpoints zurück, die vom Leerlauf-Thread des Datenbankservers gesetzt wurden. Ein Leerlauf-Checkpoint kommt vor, wenn der Leerlauf-Thread die letzte noch nicht abgeschlossene Seite im Cache ausliest.
<b>IdleChkTime</b>	Gibt die Zeit in Hundertstelsekunden zurück, die zur Checkpointsetzung während inaktiver I/O-Vorgänge genutzt wurde.
<b>IdleWrite</b>	Gibt die Anzahl der Schreibvorgänge auf Festplatte zurück, die vom Leerlauf-Thread des Servers ausgegeben wurden.
<b>IndAdd</b>	Gibt die Anzahl der Einträge zurück, die Indizes hinzugefügt wurden.
<b>IndLookup</b>	Gibt die Anzahl der Einträge zurück, nach denen in Indizes gesucht wurde.

Eigenschaftsname	Beschreibung
<b>IOParallelism</b>	Gibt die geschätzte Anzahl der simultanen, vom DBSpace unterstützten I/O-Vorgänge zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „ <a href="#">DB_EXTEN-DED_PROPERTY-Funktion [System]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>IOTorecover</b>	Gibt die geschätzte Anzahl der I/O-Vorgänge zurück, die zum Wiederherstellen der Datenbank erforderlich sind.
<b>IQStore</b>	Diese Eigenschaft ist nur für den internen Gebrauch gedacht.
<b>JavaVM</b>	Gibt die Java VM zurück, die der Datenbankserver zum Ausführen von Java in der Datenbank verwendet
<b>Language</b>	Gibt eine eine durch Kommas getrennte Liste von Sprachen zurück, die bekanntermaßen von der Datenbankkollation unterstützt werden. Die Sprachen sind im Zwei-Buchstaben-ISO-Format. Wenn die Sprache unbekannt ist, ist der Rückgabewert NULL. Eine Liste der Sprachennamen im Zwei-Buchstaben-ISO-Format und der Sprachen, auf die sie sich beziehen, finden Sie unter „ <a href="#">Sprache der Sprachumgebung</a> “ auf Seite 510.
<b>LastCheckpointTime</b>	Gibt das Datum und die Zeit in Millisekunden für den letzten Checkpoint zurück.
<b>LastCommitRedoPos</b>	Gibt die Wiederherstellungslog-Position zurück, nachdem der letzte COMMIT-Vorgang von der Datenbank in das Transaktionslog geschrieben wurde.
<b>LastSyncedRedoPos</b>	Gibt die letzte Wiederherstellungsposition zurück, für die ein Schreibvorgang auf die Festplatte ausgegeben wurde und die Daten auf dem physischen Medium synchronisiert wurden. Es wird erwartet, dass Daten vor dieser Position auch im Fall eines Stromausfalls auf der Festplatte vorhanden sind.
<b>LastWrittenRedoPos</b>	Gibt die letzte Wiederherstellungsposition zurück, für die ein Schreibvorgang auf die Festplatte ausgegeben wurde. Der Schreibvorgang ist nicht unbedingt auf dem physischen Medium synchronisiert, da er möglicherweise noch von Betriebssystem, Platten-Controller oder Festplattenlaufwerk zwischengespeichert wird.
<b>LockCount</b>	Gibt die Anzahl der von der Datenbank gehaltenen Sperren zurück.
<b>LockTablePages</b>	Gibt die Anzahl der Seiten zurück, die zum Speichern von Sperrendaten verwendet werden.

Eigenschaftsname	Beschreibung
<b>LogFileFragments</b>	Gibt die Anzahl der Logdateifragmente zurück. Diese Eigenschaft wird unter Windows unterstützt.
<b>LogFreeCommit</b>	Gibt die Anzahl der Redo Free Commits zurück. Ein Redo Free Commit tritt auf, wenn das Festschreiben des Transaktionslogs verlangt wurde, das Log aber schon geschrieben ist (das Festschreiben war daher umsonst).
<b>LogMirrorName</b>	Gibt den Dateinamen des Transaktionslog-Spiegels einschließlich des Pfads zurück.
<b>LogName</b>	Gibt den Dateinamen des Transaktionslogs einschließlich des Pfads zurück.
<b>LogWrite</b>	Gibt die Anzahl der Seiten zurück, die in das Transaktionslog geschrieben wurden.
<b>LTMGeneration</b>	Diese Eigenschaft ist nur für den internen Gebrauch gedacht.
<b>LMTTrunc</b>	Diese Eigenschaft ist nur für den internen Gebrauch gedacht.
<b>MaxIO</b>	Gibt den Höchstwert zurück, den "CurrIO" erreicht hat.
<b>MaxRead</b>	Gibt den Höchstwert zurück, den "CurrRead" erreicht hat.
<b>MaxWrite</b>	Gibt den Höchstwert zurück, den "CurrWrite" erreicht hat.
<b>MirrorMode</b>	Gibt "NULL" zurück, wenn keine Datenbankspiegelung verwendet wird, und "synchron", wenn der Spiegelmodus mit der -xp-Option angegeben ist. Ansonsten wird "asynchron" zurückgegeben.
<b>MirrorRole</b>	<p>Gibt einen der folgenden Werte zurück:</p> <ul style="list-style-type: none"> <li>• <b>primary</b> Der primäre Datenbankserver oder Spiegelserver.</li> <li>• <b>mirror</b> Der Spiegelserver.</li> <li>• <b>copy</b> Ein schreibgeschützter Spiegelserver, der seine Logseiten vom aktuellen Primärserver, dem aktuellen Spiegelserver oder einem anderen schreibgeschützten Knoten erhält. Ein Kopieknoten kann nicht der Primärserver werden. Ein Kopieknoten kann auch als untergeordneter Knoten bezeichnet werden, weil er einen übergeordneten Knoten hat, von dem er Seiten erhält.</li> </ul> <p>Siehe „<a href="#">Datenbankspiegelung</a>“ auf Seite 1467.</p>

Eigenschaftsname	Beschreibung
<b>MirrorServerState</b>	<p>Gibt nun einen der folgenden Werte zurück, wenn sie mit der DB_EXTENDED_PROPERTY-Funktion verwendet wird:</p> <ul style="list-style-type: none"> <li>• <b>NULL</b> Die Datenbank wird nicht gespiegelt.</li> <li>• <b>connected</b> Es gibt eine Verbindung dieses Servers mit einem angegebenen Server und eine Verbindung des angegebenen Servers mit diesem Server.</li> <li>• <b>disconnected</b> Es gibt keine Verbindungen zwischen diesem Server und dem angegebenen Server.</li> <li>• <b>incoming only</b> Es gibt eine Verbindung vom angegebenen Server zu diesem Server.</li> <li>• <b>outgoing only</b> Es gibt eine Verbindung von diesem Server zum angegebenen Server.</li> </ul> <p>Siehe „Datenbankspiegelung“ auf Seite 1467 und „DB_EXTENDED_PROPERTY-Funktion [System]“ [SQL Anywhere Server - SQL-Referenzhandbuch].</p>
<b>MirrorServerWaits</b>	Gibt zurück, wie oft der Datenbankserver länger als 500 ms warten musste, um Logseiten an Kopierserver zu senden.
<b>MirrorState</b>	<p>Gibt einen der folgenden Werte zurück:</p> <ul style="list-style-type: none"> <li>• <b>NULL</b> Sie sind mit einer Datenbank verbunden, die nicht gespiegelt wird.</li> <li>• <b>Synchronisation läuft</b> Der Spiegelserver ist nicht verbunden oder hat noch nicht alle Logseiten des Primärservers gelesen. Dieser Wert wird auch zurückgegeben, wenn der Synchronisationsmodus asynchron ist.</li> <li>• <b>Synchronisiert</b> Der Spiegelserver ist verbunden und hat alle Änderungen übernommen, die auf dem Primärserver festgeschrieben wurden.</li> </ul> <p>Siehe „Datenbankspiegelung“ auf Seite 1467.</p>
<b>MultiByteCharSet</b>	Gibt "On" zurück, wenn die Datenbank einen Mehrbyte-Zeichensatz wie UTF-8 verwendet. Anderenfalls wird "Off" zurückgegeben. Weitere Hinweise finden Sie unter „Mehrbyte-Zeichensätze“ auf Seite 500.
<b>Name</b>	Gibt den Datenbanknamen zurück (mit Alias identisch). Siehe <a href="#">Alias-Datenbankeigenschaft auf Seite 767</a> .

Eigenschaftsname	Beschreibung
<b>NcharCharSet</b>	Gibt den NCHAR-Zeichensatz der Datenbank zurück.
<b>NcharCollation</b>	Gibt den Namen der für NCHAR-Daten verwendeten Kollation zurück. Diese Eigenschaft hat Erweiterungen, die Sie angeben können, wenn Sie den Eigenschaftswert abfragen. Siehe „ <a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>NextScheduleTime</b>	Gibt den nächsten geplanten Ausführungszeitpunkt für ein angegebenes Ereignis zurück. Sie fragen diese Eigenschaft mit der DB_EXTEN-DED_PROPERTY-Funktion ab. Siehe „ <a href="#">DB_EXTENDED_PROPERTY-Funktion [System]</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>OptionWatchAction</b>	Gibt die Aktion zurück, die durchgeführt wird, wenn ein Versuch unter- nommen wird, eine Datenbankoption zu setzen, die in der Eigenschaft OptionWatchList enthalten ist. Siehe „ <a href="#">sa_server_option-Systemprozedur</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>OptionWatchList</b>	Gibt die Liste der Datenbankoptionen zurück, die vom Datenbankserver überwacht werden. Siehe „ <a href="#">sa_server_option-Systemprozedur</a> “ [ <i>SQL Any- where Server - SQL-Referenzhandbuch</i> ].
<b>PacketsReceived</b>	Gibt die Anzahl der empfangenen Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsReceivedUn- comp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommu- nikation empfangen worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsReceived", wenn die Komprimierung deaktiviert ist.)
<b>PacketsSent</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationspakete zurück. Dieser Wert wird für HTTP- oder HTTPS-Verbindungen nicht aktualisiert.
<b>PacketsSentUncomp</b>	Gibt die Anzahl der Pakete zurück, die während der Client/Server-Kommu- nikation gesendet worden wären, wenn die Komprimierung deaktiviert gewesen wäre. (Dieser Wert ist derselbe wie für "PacketsSent", wenn die Komprimierung deaktiviert ist.)
<b>PageRelocations</b>	Gibt die Anzahl der verlegbaren Heap-Seiten zurück, die von der temporä- ren Datei gelesen wurden.
<b>PageSize</b>	Gibt die Seitengröße der Datenbank (in Byte) zurück

Eigenschaftsname	Beschreibung
<b>PartnerState</b>	<p>Gibt einen der folgenden Werte zurück:</p> <ul style="list-style-type: none"> <li>• <b>NULL</b> Der Datenbankserver ist kein Partner.</li> <li>• <b>connected</b> Es besteht eine Verbindung von diesem Server zu einem Partnerserver und eine Verbindung vom Partnerserver zu diesem Server.</li> <li>• <b>disconnected</b> Es gibt keine Verbindungen zwischen diesem Server und dem Partnerserver.</li> <li>• <b>incoming only</b> Es gibt eine Verbindung vom Partnerserver zu diesem Server.</li> <li>• <b>outgoing only</b> Es gibt eine Verbindung von diesem Server zum Partnerserver.</li> </ul> <p>Siehe „Datenbankspiegelung“ auf Seite 1467.</p>
<b>Prepares</b>	Gibt die Anzahl der die Datenbank durchgeführten Anweisungsvorbereitungen zurück.
<b>PrepStmt</b>	Gibt die Anzahl der vorbereiteten Anweisungen zurück, die derzeit vom Datenbankserver aufrechterhalten werden.
<b>ProcedurePages</b>	Gibt die Anzahl der verlegbaren Heap-Seiten zurück, die für Prozeduren verwendet wurden.
<b>ProcedureProfiling</b>	Gibt "On" zurück, wenn die Prozedur-Profilerstellung für die Datenbank aktiviert ist. Anderenfalls wird "Off" zurückgegeben.
<b>QueryBypassed</b>	Gibt die Anzahl der Anforderungen zurück, die aus dem Plan-Cache wieder verwendet werden.
<b>QueryBypassedCosted</b>	Gibt die Anzahl von Anforderungen zurück, die vom Optimierer-Bypass mit Kostenermittlung verarbeitet wurden.
<b>QueryBypassedHeuristic</b>	Gibt die Anzahl von Anforderungen zurück, die vom Optimierer-Bypass mit Heuristik verarbeitet wurden.
<b>QueryBypassedOptimized</b>	Gibt die Anzahl von Anforderungen zurück, die ursprünglich vom Optimierer-Bypass verarbeitet und danach vom SQL Anywhere-Optimierer voll optimiert wurden.
<b>QueryCachedPlans</b>	Gibt die Anzahl der im Cache gespeicherten Ausführungspläne für alle Verbindungen zurück.

Eigenschaftsname	Beschreibung
<b>QueryCachePages</b>	Gibt die Anzahl der Seiten zurück, die benutzt wurden, um Ausführungspläne im Cache zu halten.
<b>QueryDescribedBypass</b>	Gibt die Anzahl der Anforderungen zurück, die vom Optimierer-Bypass verarbeitet wurden.
<b>QueryDescribedOptimizer</b>	Gibt die Anzahl der Anforderungen zurück, die vom Optimierer verarbeitet wurden.
<b>QueryHeapPages</b>	Gibt die Anzahl der für die Abfrageverarbeitung (Hash- und Sort-Vorgänge) benutzten Cacheseiten zurück.
<b>QueryJHToJNLOptUsed</b>	Gibt die Häufigkeit zurück, mit der ein Hash-Join in einen Nested Loops Join umgewandelt wurde.
<b>QueryLowMemoryStrategy</b>	Gibt die Häufigkeit zurück, mit der der Server wegen Speichermangels seinen Ausführungsplan geändert hat. Die Strategie kann sich ändern, weil weniger Speicher als vom Optimierer geschätzt verfügbar ist, oder weil der Ausführungsplan mehr Speicher beansprucht, als der Optimierer geschätzt hat.
<b>QueryMemActiveCurr</b>	Gibt die Anzahl der Anforderungen zurück, die den Abfragespeicher aktiv nutzen.
<b>QueryMemGrantFailed</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Zuweisung von Abfragespeicher gewartet, aber nicht erhalten hat.
<b>QueryMemGrantGranted</b>	Gibt die Anzahl der Seiten zurück, die derzeit für Anforderungen bereitgestellt sind.
<b>QueryMemGrantRequested</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt versucht hat, Abfragespeicher zu erhalten.
<b>QueryMemGrantWait</b>	Gibt einen Wert zurück, der angibt, wie viele Male eine Anforderung insgesamt auf Speicherzuweisung gewartet hat.
<b>QueryMemGrantWaiting</b>	Gibt die aktuelle Anzahl der Anforderungen zurück, die auf Zuweisung von Abfragespeicher warten.
<b>QueryOpened</b>	Gibt die Anzahl der OPEN-Anforderungen für die Ausführung zurück.
<b>QueryOptimized</b>	Gibt die Anzahl der vollständig optimierten Anforderungen zurück.
<b>QueryReused</b>	Gibt die Anzahl der wiederverwendeten Abfragepläne zurück.

Eigenschaftsname	Beschreibung
<b>QueryRowsFetched</b>	Gibt die Anzahl der Zeilen zurück, die aus den Basistabellen über einen sequenziellen Scan oder einen Index-Scan für diese Datenbank gelesen wurden.
<b>QueryRowsMaterialized</b>	Gibt die Anzahl der Zeilen zurück, die während der Abfrageverarbeitung in Arbeitstabellen geschrieben werden.
<b>ReadOnly</b>	Gibt "On" zurück, wenn die Datenbank im schreibgeschützten Modus ausgeführt wird. Anderenfalls wird "Off" zurückgegeben.
<b>ReceivingTracingFrom</b>	Gibt den Namen der Datenbank zurück, von der die Protokollierungsdaten stammen. Gibt eine leere Zeichenfolge zurück, wenn keine Protokollierung angehängt ist.
<b>RecoveryUrgency</b>	Gibt eine Schätzung der Zeitmenge zurück, die erforderlich ist, um die Datenbank wiederherzustellen, und zwar als einen Prozentsatz der Wiederherstellungszeit-Einstellung der Datenbank. Siehe <a href="#">„Datenbankserveroption -gr“ auf Seite 249</a> und <a href="#">„So entscheidet die Datenbank, wann ein Check-point auszuführen ist“ auf Seite 1077</a> .
<b>RecursiveIterations</b>	Gibt die Anzahl von Wiederholungen für rekursive Vereinigungen zurück.
<b>RecursiveIterations-Hash</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join eine Hash-Strategie verwendet hat.
<b>RecursiveIterations-Nested</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join eine Nested Loops-Strategie verwendet hat.
<b>RecursiveJNLMisses</b>	Gibt die Anzahl der Indextest-Cachefehlschläge für rekursive Hash-Joins zurück.
<b>RecursiveJNLProbes</b>	Gibt die Häufigkeit zurück, mit der ein rekursiver Hash-Join einen Indextest versucht hat.
<b>RelocatableHeapPages</b>	Gibt die Anzahl der Seiten zurück, die für verlegbare Heaps (Cursor, Anweisungen, Prozeduren, Trigger, Ansichten, etc.) verfügbar sind.
<b>RemoteTrunc</b>	Gibt das niedrigste bestätigte Log-Offset für den SQL Remote-Nachrichtenagenten zurück.
<b>ReqCountActive</b>	Gibt die Anzahl der verarbeiteten Anforderungen zurück, oder NULL, wenn die Servereigenschaft RequestTiming auf "Off" gesetzt ist. Siehe <a href="#">„Datenbankserveroption -zt“ auf Seite 319</a> .

Eigenschaftsname	Beschreibung
<b>ReqCountBlockContention</b>	Gibt zurück, wie oft Verbindungen mit der Datenbank auf einen unteilbaren Zugriff gewartet haben, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountBlockIO</b>	Gibt zurück, wie oft Verbindungen mit der Datenbank auf den Abschluss von I/O-Vorgängen gewartet haben, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountBlockLock</b>	Gibt zurück, wie oft Verbindungen mit der Datenbank auf eine Sperre gewartet haben, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqCountUnscheduled</b>	Gibt zurück, wie oft Verbindungen mit der Datenbank auf einen Zeitplan gewartet haben, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqTimeActive</b>	Gibt die Menge der verstrichenen Zeit bei der Verarbeitung von Anforderungen zurück, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqTimeBlockContention</b>	Gibt die Menge der verstrichenen Zeit beim Warten auf einen unteilbaren Zugriff zurück, oder NULL, wenn die Servereigenschaft RequestTiming auf "Off" gesetzt ist. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqTimeBlockIO</b>	Gibt die Menge der verstrichenen Zeit beim Warten auf den Abschluss von I/O-Vorgängen zurück, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqTimeBlockLock</b>	Gibt die Menge der verstrichenen Zeit beim Warten auf eine Sperre zurück, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>ReqTimeUnscheduled</b>	Gibt die Menge der Wartezeit ohne Zeitplanung zurück, oder NULL, wenn die Option -zt nicht angegeben wurde. Siehe „ <a href="#">Datenbankserveroption -zt</a> “ auf Seite 319.
<b>RequestsReceived</b>	Gibt die Anzahl der gesendeten Client/Server-Kommunikationsanforderungen oder Roundtrips zurück. Dies unterscheidet sich von PacketsReceived, da Mehrfachpaketaanforderungen als eine Anforderung zählen und Verfügbarkeitspakete nicht enthalten sind.
<b>Rlbk</b>	Gibt die Anzahl der Rollback-Anforderungen zurück, die verarbeitet wurden.
<b>RollbackLogPages</b>	Gibt die Anzahl der Seiten im Rollback-Log zurück.

Eigenschaftsname	Beschreibung
<b>SendingTracingTo</b>	Gibt die Verbindungszeichenfolge zurück, an die die Protokollierungsdaten gesendet werden. Gibt eine leere Zeichenfolge zurück, wenn keine Protokollierung angehängt ist.
<b>SnapshotCount</b>	Gibt die Anzahl der der Datenbank zugeordneten Snapshots zurück.
<b>SnapshotIsolationState</b>	<p>Gibt einen der folgenden Werte zurück:</p> <ul style="list-style-type: none"> <li>• <b>On</b> Snapshot-Isolation ist für die Datenbank aktiviert.</li> <li>• <b>Off</b> Snapshot-Isolation ist für die Datenbank deaktiviert.</li> <li>• <b>in_transition_to_on</b> Snapshot-Isolation wird aktiviert, sobald die aktuellen Transaktionen abgeschlossen sind.</li> <li>• <b>in_transition_to_off</b> Snapshot-Isolation wird deaktiviert, sobald die aktuellen Transaktionen abgeschlossen sind.</li> </ul> <p>Siehe „<a href="#">allow_snapshot_isolation-Option</a>“ auf Seite 574.</p>
<b>SortMergePasses</b>	Gibt die Anzahl der Zusammenführungsdurchgänge zurück, die während des Sortierens benutzt wurden.
<b>SortRowsMaterialized</b>	Gibt die Anzahl der Zeilen zurück, die in Arbeitstabellen sortiert werden.
<b>SortRunsWritten</b>	Gibt die Anzahl sortierter Folgen zurück, die während des Sortierens geschrieben wurden.
<b>SortSortedRuns</b>	Gibt die Anzahl sortierter Folgen zurück, die während der Folgenbildung erstellt wurden.
<b>SortWorkTables</b>	Gibt die Anzahl der für Sortierungen erstellten Arbeitstabellen zurück.
<b>StatementDescribes</b>	Gibt die Gesamtanzahl von Anweisungen zurück, die von DESCRIBE-Anforderungen verarbeitet werden.
<b>StatementPostAnnotations</b>	Gibt die Anzahl von Anweisungen zurück, die von der semantischen Abfragetransformationsphase verarbeitet werden.
<b>StatementPostAnnotationsSimple</b>	Gibt die Anzahl von Anweisungen zurück, die von der semantischen Abfragetransformationsphase verarbeitet wurden, wobei aber einige semantische Transformationen übersprungen wurden.
<b>StatementPostAnnotationsSkipped</b>	Gibt die Anzahl von Anweisungen zurück, die die semantische Abfragetransformationsphase komplett übersprungen haben.

Eigenschaftsname	Beschreibung
<b>SynchronizationSchemaChangeActive</b>	Gibt On zurück, wenn eine aktive Verbindung eine START SYNCHRONIZATION SCHEMA CHANGE-Anweisung ausgegeben hat, aber keine STOP SYNCHRONIZATION SCHEMA CHANGE-Anweisung. Siehe „START SYNCHRONIZATION SCHEMA CHANGE-Anweisung [MobiLink]“ [SQL Anywhere Server - SQL-Referenzhandbuch] und „STOP SYNCHRONIZATION SCHEMA CHANGE-Anweisung [MobiLink]“ [SQL Anywhere Server - SQL-Referenzhandbuch].
<b>SyncTrunc</b>	Gibt das niedrigste bestätigte Log-Offset für das MobiLink-Client-Programm dbmlsync zurück.
<b>TempFileName</b>	Gibt den Dateinamen der temporären Datei der Datenbank einschließlich des Pfads zurück.
<b>TempTablePages</b>	Gibt die Anzahl der Seiten in der temporären Datei zurück, die für temporäre Tabellen verwendet werden.
<b>TriggerPages</b>	Gibt die Anzahl der verlegbaren Heap-Seiten zurück, die für Trigger verwendet werden.
<b>UserDefinedCounterRate01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter „Benutzerdefinierte Eigenschaften“ auf Seite 789.</p>
<b>UserDefinedCounterRate02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter „Benutzerdefinierte Eigenschaften“ auf Seite 789.</p>
<b>UserDefinedCounterRate03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter „Benutzerdefinierte Eigenschaften“ auf Seite 789.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounter-Rate04</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Rate05</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor zeigt die Änderung im Wert des Indikators im Laufe der Zeit.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Raw01</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Raw02</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>
<b>UserDefinedCounter-Raw03</b>	<p>Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Benutzerdefinierte Eigenschaften“ auf Seite 789</a>.</p>

Eigenschaftsname	Beschreibung
<b>UserDefinedCounterRaw04</b>	Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.  Weitere Hinweise finden Sie unter „ <a href="#">Benutzerdefinierte Eigenschaften</a> “ auf Seite 789.
<b>UserDefinedCounterRaw05</b>	Gibt den aktuellen Wert für den benutzerdefinierten Leistungsindikator zurück. Die Semantik dieser Eigenschaft wird von der Clientanwendung definiert. Auf diesen Indikator kann auch vom Systemmonitor aus zugegriffen werden. Der Systemmonitor gibt den absoluten Wert des Indikators an.  Weitere Hinweise finden Sie unter „ <a href="#">Benutzerdefinierte Eigenschaften</a> “ auf Seite 789.
<b>UTCTimestampCatalog</b>	Gibt "On" zurück, wenn die Datenbank UTC-Zeitstempel in den Systemtabellen speichert.
<b>VersionStorePages</b>	Gibt die Anzahl der Seiten in der temporären Datei zurück, die zur Zeilenversionsspeicherung verwendet werden, wenn die Snapshot-Isolation aktiviert ist.
<b>ViewPages</b>	Gibt die Anzahl der verlegbaren Heap-Seiten zurück, die für Ansichten verwendet werden.
<b>WriteChecksum</b>	Gibt On zurück, wenn der Datenbankserver Prüfsummen zu Seiten hinzufügt, bevor sie ausgeschrieben werden, sonst Off. Siehe „ <a href="#">Erkennung von Beschädigungen mithilfe von Prüfsummen</a> “ auf Seite 1084.
<b>XPathCompiles</b>	Gibt zurück, wie viel Mal eine XPath-Abfrage (unter Verwendung des OPENXML-Operators) vom Datenbankserver seit seinem Start kompiliert wurde. Siehe „ <a href="#">OPENXML-Operator</a> “ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].

## Benutzerdefinierte Eigenschaften

SQL Anywhere unterstützt einen Satz von benutzerdefinierten Eigenschaften. Ihre Anwendung muss die Semantik für jede benutzerdefinierte Eigenschaft definieren und die zurückgegebenen Werte festlegen. Die Eigenschaftswerte können mit der sa\_user\_defined\_counter\_set-Systemprozedur auf einen absoluten 32-Bit-Wert vom Typ UNSIGNED INTEGER festgelegt oder mit der sa\_user\_defined\_counter\_add-Systemprozedur schrittweise erhöht werden. Die sa\_user\_defined\_counter\_add-Systemprozedur kann

auch dazu verwendet werden, die Eigenschaftswerte durch Addieren eines negativen Werts zu verringern. Die benutzerdefinierten Zähler sind:

- UserDefinedCounterRaw01
- UserDefinedCounterRaw02
- UserDefinedCounterRaw03
- UserDefinedCounterRaw04
- UserDefinedCounterRaw05
- UserDefinedCounterRate01
- UserDefinedCounterRate02
- UserDefinedCounterRate03
- UserDefinedCounterRate04
- UserDefinedCounterRate05

Die Werte für benutzerdefinierte Eigenschaften werden für jede Verbindung, jede Datenbank und jeden Server getrennt verwaltet. Der aktuelle Wert der Eigenschaften kann mit den CONNECTION\_PROPERTY-, DB\_PROPERTY- und PROPERTY-Funktionen abgerufen werden. Sie können auf diese Eigenschaften auch vom Systemmonitor aus zugreifen. Der Systemmonitor zeigt den aktuellen Wert einer UserDefinedCounterRaw-Eigenschaft als einen absoluten Wert und die Rate der Änderung einer UserDefinedCounterRate in einem Messwertintervall als Rate an.

Ein Beispiel für die Verwendung dieser Eigenschaften wäre eine Raw-Eigenschaft, die die aktuelle Anzahl von in einem Schlüsselpool verbleibenden Schlüsseln anzeigt. Der Wert der Eigenschaft schwankt im Laufe der Zeit. Gleichzeitig kann eine Rate-Eigenschaft anzeigen, wie schnell Schlüssel aus dem Schlüsselpool genutzt werden. Der Wert wird im Laufe der Zeit erhöht, wenn Schlüssel verwendet werden, und der Systemmonitor zeigt die Rate, mit der Schlüssel pro Sekunde verwendet werden.

### Siehe auch

- [UserDefinedCounterRaw01-Verbindungseigenschaft auf Seite 742](#)
- [UserDefinedCounterRate01-Verbindungseigenschaft auf Seite 741](#)
- [UserDefinedCounterRaw01 Datenbankeigenschaft auf Seite 788](#)
- [UserDefinedCounterRate01 Datenbankeigenschaft auf Seite 787](#)
- [UserDefinedCounterRaw01-Servereigenschaft auf Seite 764](#)
- [UserDefinedCounterRate01-Servereigenschaft auf Seite 763](#)
- [„sa\\_user\\_defined\\_counter\\_add-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„sa\\_user\\_defined\\_counter\\_set-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Benutzerdefinierte Statistiken“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„SQL-Funktionen zum Überwachen von Statistiken“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)
- [„Optionen des Windows-Systemmonitors“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#)

## SQL Anywhere-Einschränkungen von Größe und Anzahl

Die folgende Tabelle listet die physikalischen Einschränkungen von Größe und Anzahl der Objekte in einer SQL Anywhere-Datenbank auf. In der Regel sind der Speicher, die CPU und die Festplatte des Computers die Faktoren mit den größten Einschränkungen.

Element	Beschränkung
Datenbankgröße	13 Dateien pro Datenbank. Für jede Datei die größte vom Betriebs- und Dateisystem zugelassene Datei
DBSpace-Größe	2 <sup>28</sup> x Seitengröße
Größe der temporären Datei	2 <sup>28</sup> x Seitengröße
Feldgröße	2 GB
Dateigröße (FAT 12)	16 MB
Dateigröße (FAT 16)	2 GB
Dateigröße (FAT 32)	4 GB
Dateigröße für NTFS, HP-UX 11.0 und höher, Solaris 2.6 und höher, Linux 2.4 und höher, AIX und Mac OS X	<ul style="list-style-type: none"> <li>• 512 GB für 2-kB-Seiten</li> <li>• 1 TByte für 2-kB-Seiten</li> <li>• 2 TByte für 8-kB-Seiten</li> </ul>
Dateigröße (alle übrigen Plattformen und Dateisysteme)	2 GB
Maximale Cachegröße (Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2008, Windows Server 2008 R2, Windows 7)	1,8 GB
Maximale Cachegröße (Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Business, Windows Vista Home Premium, Windows Vista Home Basic)	2,7 GB
Maximale Cachegröße (Windows Mobile)	Begrenzt durch den verfügbaren Speicher auf dem Gerät

Element	Beschränkung
Maximale Cachegröße (Unix-Solaris, x86 Linux, IBM AIX, HP)	2 GB für 32-Bit-Server
Maximale Cachegröße (Win 64)	Begrenzt durch physischen Speicher auf 64-Bit-Servern
Maximale Cachegröße (Itanium HP-UX)	Begrenzt durch physischen Speicher auf 64-Bit-Servern
Maximale Größe der Indexeinträge	Keine Grenze
Anzahl der Datenbanken pro Server	255
Spaltenanzahl pro Tabelle	45000  Hinweis: Eine übermäßige Spaltenanzahl - obwohl zulässig - hat negative Auswirkungen auf die Performance.
Anzahl von nullwertfähigen Spalten pro Tabelle	$\min(45000, (\text{Seitengröße} - \text{Overhead}) * 8)$
Anzahl von Spalten in einer Prozedur-Ergebnismenge	45000
Anzahl von Spalten in einer SELECT-Liste	100000
Anzahl von Spalten in einer GROUP BY-Liste	100000
Anzahl von Spalten in einem GROUP BY mit Gruppierungskombinationen	64
Anzahl von Spalten in einem CUBE	15
Anzahl von unterschiedlichen Gruppierungskombinationen	32768
Länge von DEFAULT bei einer Spalte	32768
Länge von COMPUTE bei einer Spalte	32768
Länge von DEFAULT bei Prozedurparametern	32768
Länge von DEFAULT bei einer benutzerdefinierten Domäne	32768
Länge von Prüf-Integritätsregeln	2 GB
Anzahl der Indizes pro Tabelle	$2^{32}$

Element	Beschränkung
Anzahl der Zeilen pro Datenbank	$4096 \times 2^{28} \times 13$
Anzahl von Zeilen pro Tabelle	$4096 \times 2^{28}$
Anzahl der Tabellen pro Datenbank	$2^{32} - 2^{20} - 1 = 4293918719$
Anzahl temporärer Tabellen pro Verbindung	$2^{20} = 1048576$
Anzahl der pro Transaktion referenzierten Tabellen	Keine Grenze
Anzahl von gespeicherten Prozeduren pro Datenbank	$2^{32} - 1 = 4294967295$
Anzahl gleichzeitiger Anweisungen pro Datenbank-server	$20 \times \text{Anzahl der Datenbankverbindungen} + 65534$
Anzahl der Ereignisse pro Datenbank	$2^{31} - 1 = 2147483647$
Anzahl der Trigger pro Datenbank	$2^{32} - 1 = 4294967295$
Zeilenlänge	Begrenzt durch die Dateigröße
Tabellengröße	Maximale Dateigröße. Vom Benutzer für die Tabelle erstellte Indizes können getrennt von der Tabelle gespeichert werden.
Zeichendatentypen	$2^{31} - 1 = 2147483647$
Binärdatentypen	$2^{31} - 1 = 2147483647$
Zeilenlänge	45000 Felder
Arraygröße	6,4 Mio. Elemente
Bezeichner (Benutzer-IDs, Tabellennamen und Spaltennamen)	128 Byte
Kennwörter	255 Byte
Datenbankservernamen	250 Byte (TCP/IP und Shared Memory)  Siehe „Datenbankserveroption -n“ auf Seite 266 und „Verbindungsparameter ServerName (Server)“ auf Seite 383.
Datenbanknamen	250 Byte  Siehe „Datenbankoption -n“ auf Seite 328.

Element	Beschränkung
Anzahl der Schlüssel für gesicherte Funktionen pro Datenbank	1000

## Hardwareanforderungen für SQL Anywhere

Weitere Informationen zu Hardwareanforderungen finden Sie unter [www.sybase.com/detail?id=1069662](http://www.sybase.com/detail?id=1069662).

---

# Datenbankadministration

Dieser Abschnitt beschreibt, wie Sie Tools, die in SQL Anywhere enthalten sind, verwenden, um Ihre Datenbank zu verwalten.

## SQL Anywhere - Grafische Administrationstools

### Sybase Central

Sybase Central ist eine grafische Benutzeroberfläche für die Verwaltung Ihrer Datenbankserver, Datenbanken und Datenbankobjekte.

#### Sybase Central-Kernfunktionen

- **Einfache Zugriff über Befehle** Das Menü **Datei** von Sybase Central wird automatisch aktualisiert, wenn Sie ein Objekt wählen, sofern sich die Befehle direkt auf das betreffende Objekt beziehen. Sie können auch auf ein Objekt rechtsklicken, um auf diese Befehle zuzugreifen.
- **Aufgabenassistenten** Wenn Sie ein neues Objekt hinzufügen möchten, finden Sie in Sybase Central Assistenten, die Sie Schritt für Schritt durch die Aufgabe führen.
- **Drag-Drop-Funktionen** In Sybase Central können viele Vorgängen mithilfe von Drag-Drop-Funktionen mit der Maus ausgeführt werden. Wenn Sie beispielsweise Tabellen in eine andere Datenbank kopieren möchten, können Sie sie mit der Maus an den neuen Speicherort ziehen.

Beim Kopieren eines Datenbankobjekts wird der SQL-Code für das Objekt in die Zwischenablage kopiert und Sie können ihn in andere Anwendungen einfügen, z.B. in Interactive SQL oder einen Texteditor. Wenn Sie beispielsweise einen Index in Sybase Central kopieren und in einen Texteditor einfügen, wird die CREATE INDEX-Anweisung für diesen Index angezeigt.

- **Tastenkürzel** Für viele gängige Befehle gibt es Tastenkürzel, die neben den Befehlen in den Menüs aufgeführt werden. Siehe „[Sybase Central-Tastenkürzel](#)“ auf Seite 799.
- **Plug-In-Unterstützung** Eine Reihe von Datenbankprodukten und -Tools können Sie über Plug-Ins verwalten. Klicken Sie in Sybase Central auf **Hilfe** und anschließend auf einen Plug-In-Namen, um zusätzliche Informationen zur Verwendung und Konfiguration des betreffenden Plug-Ins abzurufen. Siehe „[Plug-In-Architektur von Sybase Central](#)“ auf Seite 806.

#### Inhalte aktualisieren

Sybase Central speichert Informationen zur Datenbank im Cache. Wenn Sie Änderungen an der Datenbank über eine andere Verbindung vornehmen, erkennt Sybase Central die Änderungen erst, wenn Sie die Datenbank in Sybase Central aktualisieren. Beispiel: Von Sybase Central verwaltete Produkte können einen gleichzeitigen Zugriff unterstützen. Das bedeutet, dass ein anderer Benutzer die Struktur der Ordnerliste ändern könnte, während Sie sie in Sybase Central anzeigen.

Damit gewährleistet ist, dass Sie immer die aktuellsten Informationen sehen, bietet Sybase Central die folgenden Aktualisierungsbefehle im Menü **Ansicht**:

- **Ordner aktualisieren** Aktualisiert Ihre Ansicht des derzeit erweiterten Behälters. Sie können auch F5 drücken, um den Ordner zu aktualisieren.
- **Alles aktualisieren** Aktualisiert Ihre Ansicht aller erweiterten Behälter.

Diese Befehle rufen bei Sybase Central und den Plug-Ins die aktuellen Informationen ab.

## Deployment von Sybase Central

Abhängig von Ihrer Lizenzvereinbarung können Sie das Deployment der SQL Anywhere-Verwaltungstools, einschließlich Sybase Central, vornehmen.

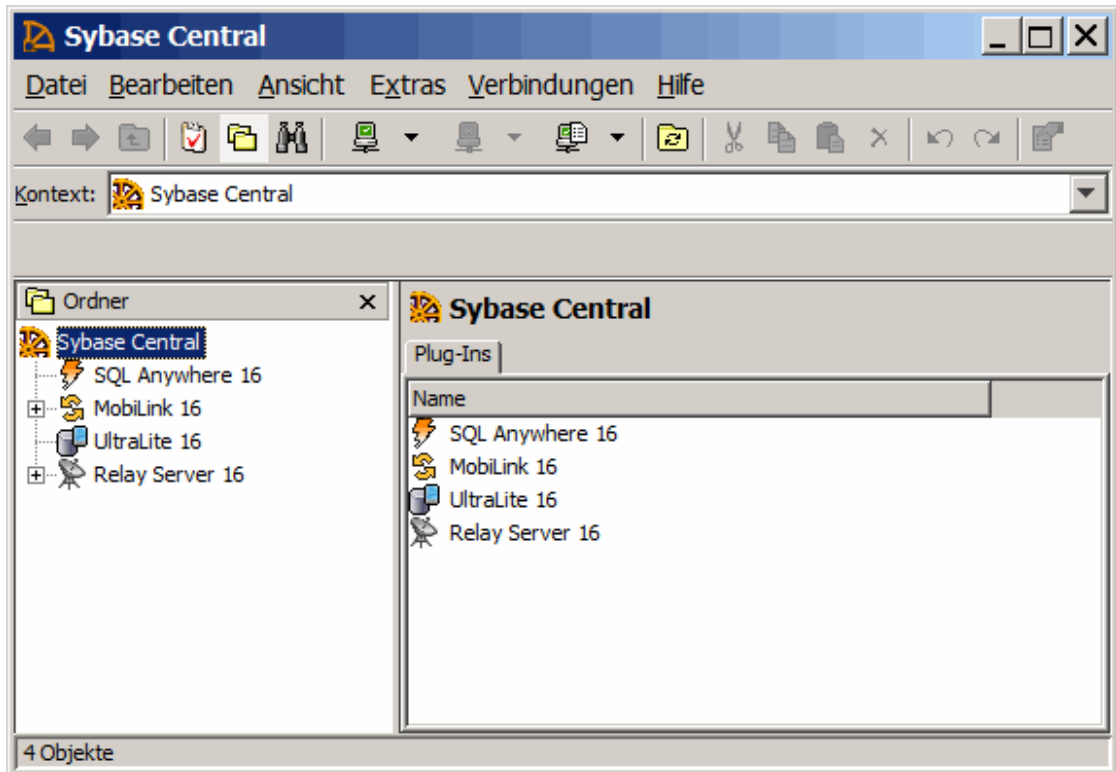
Weitere Hinweise zum Deployment von Sybase Central mit Ihrer Anwendung finden Sie unter „Deployment von Administrationstools“ [[SQL Anywhere Server - Programmierung](#)].

## Siehe auch

- SQL Anywhere: „SQL Anywhere 16-Plug-In“ auf Seite 808
- MobiLink: „MobiLink-Plug-In für Sybase Central“ [[MobiLink - Erste Orientierung](#)]
- UltraLite: „Erstellen einer UltraLite-Datenbank mit dem Assistenten Datenbank erstellen“ [[UltraLite - Datenbankverwaltung](#)]
- Relay Server: „Relay Server-Plug-In für Sybase Central“ [[Relay Server](#)]
- „Verbinden mit der Beispieldatenbank (Sybase Central)“ auf Seite 5

## Sybase Central-Navigation

Das Fenster von Sybase Central ist in zwei vertikale Fensterausschnitte unterteilt.



### Linker Fensterausschnitt

Sie können im Menü **Ansicht** auswählen, was im linken Fensterausschnitt angezeigt wird:

- **Ordner** Dieser Fensterausschnitt enthält eine hierarchische Ansicht der Datenbankobjekte.

**Ordner** im linken Fensterausschnitt enthalten nur die Behälter der Objekt-Strukturdarstellung, aber keine Objekte, die nicht Behälter anderer Objekte sind. Im linken Fensterausschnitt kann z.B. ein Ordner "Spalten" erscheinen (ein Behälter), jedoch nicht die Spalten selbst, weil sie Elemente sind und deshalb im rechten Fensterausschnitt erscheinen.

Sie können konfigurieren, welche Datenbankobjekte im Fensterausschnitt **Ordner** angezeigt werden, indem Sie auf die Datenbank rechtsklicken, auf **Typfilter konfigurieren** klicken und die Objekttypen auswählen, die in Sybase Central im linken Fensterausschnitt angezeigt werden sollen. Klicken Sie anschließend auf **OK**. Optional können Sie auf **Dies soll der Standardfilter für neue Datenbanken werden** klicken, um den konfigurierten Filter als Standardtypfilter festzulegen. Der Standardtypfilter wird verwendet, wenn Sie eine Verbindung mit einer Datenbank herstellen, die nicht über einen festgelegten Typfilter verfügt.

- **Aufgaben** Dieser Fensterausschnitt enthält eine Aufgabenliste für das ausgewählte Datenbankobjekt.
- **Suchen** In diesem Fensterausschnitt können Sie nach Objekten in einem Plug-In suchen.

## Rechter Fensterausschnitt

Im rechten Fensterausschnitt erscheint der Inhalt des derzeit markierten Behälters. Der rechte Fensterausschnitt enthält Registerkarten, die den Inhalt des Behälters anzeigen, der im linken Fensterausschnitt ausgewählt ist, sowie weitere Informationen über den ausgewählten Behälter.

Sie können konfigurieren, welche Spalten auf einer Registerkarte im rechten Fensterausschnitt angezeigt werden, indem Sie auf **Ansicht » Spalten auswählen** klicken.

Sie können das Erscheinungsbild des rechten Fensterausschnitts ändern, indem Sie auf **Extras » Optionen** klicken.

Wenn eine Verbindung mit einem Datenbankserver oder einer Datenbank besteht, wird ihr Symbol im Hauptfenster von Sybase Central angezeigt.

## Symbolleiste

Das Hauptfenster enthält Schaltflächen für häufig verwendete Befehle. Um die Symbolleiste anzuzeigen bzw. auszublenden, klicken Sie auf **Ansicht » Symbolleisten » Standardsymbolleisten**. Die Haupt-Symbolleiste bietet folgende Funktionen:

- Durch die Objektordner navigieren
- Die Verbindung mit einer Datenbank, einem Datenbankserver oder einem Produkt-Plug-In herstellen bzw. beenden
- Die Fensterausschnitt **Aufgaben**, **Ordner** oder **Suchen** anzeigen
- Das Fenster **Verbindungsprofile** aufrufen (kann auch über das Menü **Extras** geöffnet werden)
- Die Ansicht des aktuellen Ordners aktualisieren
- Objekte ausschneiden, kopieren, einfügen oder löschen
- Änderungen rückgängig machen und wiederherstellen
- Das Eigenschaftsfenster eines markierten Objekts aufrufen

## Dropdown-Liste Kontext

Mithilfe der Dropdown-Liste **Kontext**, die unterhalb der Symbolleiste angezeigt wird, können Sie durch die Objektordner zu einem Plug-In navigieren.

## Statusleiste

Während Sie durch die einzelnen Menüs navigieren, erscheint in der Statusleiste am unteren Rand des Hauptfensters eine kurze Zusammenfassung der Menübefehle. Um die Statusleiste anzuzeigen bzw. auszublenden, klicken Sie auf **Ansicht » Statusleiste**.

## Siehe auch

- „Nach Datenbankobjekten suchen“ auf Seite 799

## Nach Datenbankobjekten suchen

Über Sybase Central können Sie nach einem bestimmten Datenbankobjekt in einer Datenbank oder nach einer Zeichenfolge im SQL-Code eines Datenbankobjekts suchen.

### Voraussetzungen

Wenn Sie nicht die erforderlichen Privilegien haben, um den Ordner **Login-Zuordnungen**, den Ordner **Wartungspläne** bzw. die Registerkarte **Seitennutzung** oder **Sperren** für eine Datenbank anzuzeigen, werden diese Ordner bzw. Registerkarten bei jeder von Ihnen durchgeführten Suche übersprungen.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zu einer Datenbank mithilfe des **SQL Anywhere 16-Plug-Ins** her.
2. Klicken Sie auf **Ansicht » Suchbereich**.

Der Bereich **Suchen** erscheint im linken Fensterausschnitt.

3. Konfigurieren Sie die Optionen für die Suche.

Option	Aktion
<b>SQL Anywhere 16-Plug-In</b>	<ul style="list-style-type: none"> <li>• <b>In SQL suchen</b> Wählen Sie diese Option, um den SQL-Code von Prozeduren, Ereignissen, Funktionen und Triggern in die Suche einzubeziehen.</li> <li>• <b>Nach dynamischen Eigenschaften suchen (Verbindungen, Statistiken, Sperren)</b> Wählen Sie diese Option, um dynamische Eigenschaften wie verbundene Benutzer, SQL Remote-Statistiken, Tabellensperren und Tabellenseitennutzungsinformationen in die Suche einzubeziehen.</li> </ul>
<b>MobiLink 16-Plug-In</b>	<ul style="list-style-type: none"> <li>• <b>Suche in Skripten</b> Wählen Sie diese Option aus, um Synchronisationskripten in die Suche aufzunehmen.</li> </ul>

4. Klicken Sie auf **Suchen**.

### Ergebnisse

Die Suchergebnisse werden im linken Fensterausschnitt unter **Ergebnisse** angezeigt. Doppelklicken Sie auf ein Ergebnis, um es im rechten Fensterausschnitt zu öffnen.

## Sybase Central-Tastenkürzel

In Sybase Central gibt es die folgenden Tastenkürzel:

Funktionstaste	Beschreibung
Alt+Eingabe	Öffnet das Eigenschaftsfenster für das markierte Element.

Funktionstaste	Beschreibung
Strg+C	Kopiert die Markierung in die Zwischenablage
Strg+V	Fügt den Inhalt der Zwischenablage ein
Strg+X	Schneidet die Markierung aus und speichert sie in der Zwischenablage
Entf	Löscht die Markierung
F1	Öffnet die Hilfe für Sybase Central
F5	Aktualisiert den Inhalt des markierten Ordners
F9	Öffnet das Fenster <b>Verbindungsprofile</b> .
F11	Öffnet das Menü <b>Verbindung</b> , wenn mehrere Plug-Ins geladen sind. Wenn nur ein Plug-In geladen ist, wird mit F11 das Fenster <b>Verbinden</b> dieses Plug-Ins geöffnet.
F12	Trennt die Verbindung, wenn in Sybase Central nur eine Verbindung vorhanden ist. Wenn es mehr als eine Verbindung gibt, wird mit F12 das Fenster <b>Trennen</b> geöffnet. Dort können Sie die zu trennende Verbindung auswählen.
Umschalt+F10	Öffnet das Einblendmenü für das markierte Objekt.

## Code-Editor

Der Code-Editor erscheint als Registerkarte **SQL** im rechten Fensterausschnitt von Sybase Central, als separates Fenster in Sybase Central und als Fensterausschnitt **SQL-Anweisungen** in Interactive SQL. Um den Code-Editor in einem separaten Fenster in Sybase Central zu öffnen, wählen Sie im linken Fensterausschnitt ein Datenbankobjekt aus und klicken dann auf **Datei » In neuem Fenster bearbeiten**.

Neben der standardmäßigen Textbearbeitung stehen im Code-Editor die folgenden Funktionen zur Verfügung:

- Eine Symbolleiste und eine Statusleiste
- Automatische Syntax-Hervorhebung.
- Berücksichtigung der Sprache beim Einrücken
- Die Möglichkeit, Text zu suchen und zu ersetzen
- Die Möglichkeit, Dateien zu öffnen und zu speichern (ob diese Funktion verfügbar ist, hängt davon ab, welche Plug-Ins Sie benutzen)

- Die Möglichkeit, Code auszudrucken
- Textvervollständigung bei Eingabe von Code

## Tastenkürzel im Code-Editor

Sybase Central bietet die folgenden Tastenkürzel für den Code-Editor.

Funktionstaste	Beschreibung
Alt+F4	Schließt den Code-Editor (falls er ein separates Fenster ist) oder schließt Sybase Central (wenn Sie Text im rechten Fens- terrausschnitt von Sybase Central bearbeiten)
Rücktaste	Löscht die Markierung Falls nichts markiert ist, werden mit der Rücktaste die Zeichen links vom Cursor gelöscht.
Strg+]	Verschiebt den Cursor zur schließenden eckigen Klammer. Verwenden Sie dieses Tastenkürzel, um nach übereinstimm- enden runden, geschweiften, eckigen und spitzen Klammern zu suchen.
Strg+A	Markiert den gesamten Inhalt des Code-Editor-Fensters
Strg+Rückschritt	Löscht das Wort links vom Cursor
Strg+C	Kopiert den markierten Text in die Zwischenablage
Strg+Entf	Löscht das Wort rechts vom Cursor
Strg+Ende	Verschiebt den Cursor zum Anfang des Code-Editor-Fensters.
Strg+F	Öffnet das Fenster <b>Suchen/Ersetzen</b> , mit dem Sie nach dem angegebenen Text suchen und ihn ersetzen können, wenn Sie im aktuellen Fenster noch nicht nach Text gesucht haben. Ansonsten wird nach dem nächsten Vorkommen des angege- benen Textes gesucht.
Strg+F3	Sucht das nächste Vorkommen des derzeit markierten Textes
Strg+G	Öffnet das Fenster <b>Gehe zu</b> , in dem Sie eine Zeilennummer eingeben können, zu der Sie im Code-Editor-Fenster springen möchten.
Strg+Pos1	Verschiebt den Cursor zum Anfang des Code-Editor-Fensters
Strg+L	Löscht die aktuelle Zeile.
Strg+Pfeil nach links	Verschiebt den Cursor ein Wort zurück

<b>Funktionstaste</b>	<b>Beschreibung</b>
Strg+N	Löscht den Inhalt des Code-Editor-Fensters und schließt die aktuelle Datei (falls vorhanden). Dieses Tastenkürzel kann über die <b>SQL</b> -Registerkarte im rechten Fensterausschnitt von Sybase Central aus nicht verwendet werden.
Strg+O	Öffnet eine Datei, wenn der Code-Editor als separates Fenster geöffnet ist. Dieses Tastenkürzel kann über die <b>SQL</b> -Registerkarte im rechten Fensterausschnitt von Sybase Central aus nicht verwendet werden.
Strg+P	Druckt den Inhalt des Code-Editor-Fensters. Sie können das Erscheinungsbild des gedruckten Textes konfigurieren, indem Sie auf <b>Extras » Optionen » Drucken</b> klicken.
Strg+Pfeil nach rechts	Verschiebt den Cursor ein Wort vorwärts
Strg+S	Speichert den Inhalt des Code-Editor-Fensters.
Strg+Umschalt+]	Erweitert die Markierung bis zur schließenden eckigen Klammer. Verwenden Sie dieses Tastenkürzel, um nach übereinstimmenden runden, geschweiften, eckigen und spitzen Klammern zu suchen.
Strg+Umschalt+Ende	Erweitert die Markierung bis zum Ende des Codes
Strg+Umschalt+F3	Sucht das vorige Vorkommen des derzeit markierten Textes
Strg+Umschalt+Pos1	Erweitert die Markierung bis zum Anfang des Codes
Strg+Umschalt+L	Löscht die aktuelle Zeile
Strg+Umschalt+Pfeil nach links	Erweitert die Markierung um ein Wort rückwärts
Strg+Umschalt+Pfeil nach rechts	Erweitert die Markierung um ein Wort vorwärts
Strg+Umschalt+U	Ändert den markierten Text auf Großbuchstaben
STRG+Umschalt+Punkt (.)	Erhöht den Zeileneinzug des markierten Zextes im Code-Editor-Fenster. Wenn kein Text ausgewählt wurde, wird der Einzug auf die aktuelle Zeile angewendet.
STRG+Umschalt+Komma (,)	Verringert den Zeileneinzug des markierten Zextes im Code-Editor-Fenster. Wenn kein Text ausgewählt wurde, wird der Einzug auf die aktuelle Zeile angewendet.
Strg+U	Ändert den markierten Text auf Kleinbuchstaben

Funktionstaste	Beschreibung
Strg+V	Fügt den Inhalt der Zwischenablage an der aktuellen Cursorposition ein
Strg+X	Schneidet den markierten Text aus.
Strg+Y	Stellt die zuletzt rückgängig gemachte Aktion wieder her
Strg+Z	Setzt die letzte Aktion zurück
STRG+Minuszeichen (-)	<p>Fügt den Doppel-Bindestrich (--) als SQL-Kommentarindikator hinzu oder entfernt ihn.</p> <p>Um vorhandenen Text in Kommentar zu verwandeln, markieren Sie den Text im Code Editor-Fenster und drücken STRG+Minuszeichen. Das SQL-Kommentarzeichen in Form eines doppelten Bindestrichs wird an den Beginn der Zeilen des markierten Texts gesetzt.</p> <p>Wenn kein Text markiert wurde, wird das Kommentarzeichen am Beginn der aktuellen Zeile eingefügt.</p> <p>Um einen Kommentarindikator zu entfernen, wählen Sie den Text aus und drücken dann STRG+Minuszeichen.</p> <p>Siehe „Kommentare“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>
STRG+Schrägstrich (/)	<p>Fügt den Doppel-Schrägstrich (//) als SQL-Kommentarindikator hinzu oder entfernt ihn.</p> <p>Um vorhandenen Text in Kommentar zu verwandeln, markieren Sie den Text im Code Editor-Fenster und drücken STRG+Schrägstrich. Das SQL-Kommentarzeichen in Form eines doppelten Schrägstrichs wird an den Beginn der Zeilen des markierten Texts gesetzt.</p> <p>Wenn kein Text markiert wurde, wird das Kommentarzeichen am Beginn der aktuellen Zeile eingefügt.</p> <p>Um einen Kommentarindikator zu entfernen, wählen Sie den Text aus und drücken dann STRG+Schrägstrich.</p> <p>Siehe „Kommentare“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>
Entf	Löscht die Markierung

<b>Funktionstaste</b>	<b>Beschreibung</b>
Abwärtspfeil	Verschiebt den Cursor eine Zeile nach unten
Ende	Verschiebt den Cursor zum Ende der aktuellen Zeile
F3	Öffnet das Fenster <b>Suchen/Ersetzen</b> , mit dem Sie nach dem angegebenen Text suchen und ihn ersetzen können, wenn Sie im aktuellen Fenster noch nicht nach Text gesucht haben. Ansonsten wird nach dem nächsten Vorkommen des angegebenen Textes gesucht.
Pos1	Verschiebt den Cursor an den Anfang der aktuellen Zeile oder an den Textanfang in der aktuellen Zeile.
Pfeil nach links	Verschiebt den Cursor ein Zeichen nach links
Seite nach unten	Verschiebt den Cursor zum Ende der aktuellen Seite
Seite nach oben	Verschiebt den Cursor zum Anfang der aktuellen Seite
Pfeil nach rechts	Verschiebt den Cursor ein Zeichen nach rechts
Umschalt+Abwärtspfeil	Erweitert die Markierung um eine Zeile nach unten
Umschalt+Ende	Markiert die aktuelle Zeile
Umschalt+F3	Öffnet das Fenster <b>Suchen/Ersetzen</b> , mit dem Sie nach dem angegebenen Text suchen und ihn ersetzen können, wenn kein Text markiert ist. Wenn Text markiert ist, wird das vorige Vorkommen des markierten Textes gesucht.
Umschalt+F10	Zeigt das Einblendmenü für den aktiven Bereich an.  Dieses Tastenkürzel ist eine Alternative zum Rechtsklicken auf einen Bereich.
Umschalt+Pos1	Erweitert die Markierung bis zum Textbeginn in der aktuellen Zeile.
Umschalt+Pfeil nach links	Erweitert die Markierung ausgehend von den derzeit markierten Zeichen um ein Zeichen nach links
Umschalt+Seite nach unten	Erweitert die Markierung um eine Seite nach unten
Umschalt+Seite nach oben	Erweitert die Markierung um eine Seite nach oben
Umschalt+Pfeil nach rechts	Erweitert die Markierung ausgehend von den derzeit markierten Zeichen um ein Zeichen nach rechts

Funktionstaste	Beschreibung
Umschalt+Aufwärtspfeil	Erweitert die Markierung um eine Zeile nach oben
Aufwärtspfeil	Verschiebt den Cursor um eine Zeile nach oben

## Log-Viewer

Der Log-Viewer ist ein Fenster in Sybase Central, das Produktmeldungen speichert und anzeigt.

Dabei handelt es sich um folgende Meldungstypen:

- **Information** Hier werden Basisinformationen über die aktuelle Sitzung angezeigt.
- **Warnung** Hier werden Warnungen über aufgetretene Vorgänge angezeigt.
- **Fehler** Hier werden Fehlermeldungen über fehlgeschlagene Vorgänge angezeigt.

Verwenden Sie das Menü **Ansicht**, um diese Meldungen so zu filtern, dass nur ein bestimmter Typ, eine bestimmte Anzahl oder nur Meldungen aus einem bestimmten Plug-In angezeigt werden. Außerdem können Sie Meldungen in einer Datei speichern oder alle Meldungen aus der Liste löschen.

Um den Log-Viewer zu öffnen und die aktuellen Meldungen, sofern vorhanden, anzuzeigen, klicken Sie auf **Extras » Log-Viewer**.

### Einzelne Meldungsdetails im Log-Viewer

Wenn die Spalte **Kurzmeldung** des Log-Viewers nicht genügend Informationen zu einer bestimmten Meldung enthält, können Sie zusätzliche Details anzeigen, indem Sie die Meldung im Log-Viewer auswählen und dann auf **Ansicht » Detail** klicken.

### Im Log-Viewer nach Logeinträgen suchen

Verwenden Sie die Suchfunktion im Log-Viewer, um nach bestimmten Meldungen zu suchen. Wählen Sie im Log-Viewer **Ansicht » Suchen**.

### Siehe auch

- „Log-Viewer“ auf Seite 805
- „Meldungsliste des Log-Viewers konfigurieren“ auf Seite 805

## Meldungsliste des Log-Viewers konfigurieren

Konfigurieren Sie die Reihenfolge der Meldungen im Log-Viewer, beschränken Sie die Anzahl der angezeigten Meldungen oder filtern Sie die angezeigten Meldungen. Sie können auch alle Meldungen aus der Liste löschen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Aufgabe

- Klicken Sie in Sybase Central auf **Extras » Log-Viewer**, um den Log-Viewer zu öffnen.

Option	Aktion
Alle Meldungen anzeigen	Im Log-Viewer wählen Sie <b>Ansicht→Alle Ereignisse</b> .
Alle Meldungen löschen	Im Log-Viewer wählen Sie <b>Log→Alle Ereignisse löschen</b> .
Reihenfolge der Meldungen festlegen	Wählen Sie im Log-Viewer im Menü <b>Ansicht</b> eine der folgenden Optionen: <ul style="list-style-type: none"> <li>• <b>Neueste zuerst</b>, wenn die neuesten Nachrichten an erster Stelle stehen sollen.</li> <li>• <b>Älteste zuerst</b>, wenn die neuesten Nachrichten an letzter Stelle stehen sollen.</li> </ul>
Meldungen filtern	<p>a. Im Log-Viewer wählen Sie <b>Ansicht→Ereignisse filtern</b>.</p> <p>Das Fenster <b>Filter</b> wird eingeblendet.</p> <p>b. Konfigurieren Sie die Optionen.</p>

## Ergebnisse

Die Meldungsliste im Log-Viewer wird angepasst.

## Siehe auch

- „Log-Viewer“ auf Seite 805

## Plug-In-Architektur von Sybase Central

Jedes Sybase-Produkt wird von einem eigenen Plug-In in Sybase Central verwaltet. SQL Anywhere enthält Sybase Central-Plug-Ins für die folgenden Produkte:

- SQL Anywhere-Datenbanken
- UltraLite-Datenbanken
- MobiLink-Synchronisation
- Relay Server

Die Plug-Ins für diese Produkte müssen registriert und geladen werden, bevor Sie die jeweiligen Produkte in Sybase Central verwenden können. Zumeist wird das Plug-In bei der Installation des Produkts automatisch registriert und geladen. In besonderen Fällen können Sie die Plug-Ins, die in Sybase Central erscheinen, auch manuell registrieren.

**Tipp**

Sybase Central hat eine eigene Versionsnummer, die sich von der der Plug-Ins unterscheidet. Wenn Sie die Versionsnummer von Sybase Central oder die Versionsnummer eines Plug-Ins anzeigen möchten, wählen Sie **Hilfe » Info über Sybase Central**.

Die Plug-In-Dateien befinden sich am folgenden Standort in Ihrer SQL Anywhere -Installation:

Plug-In	Dateiname und Standort
<b>SQL Anywhere 16</b>	<i>%SQLANY16%\java\sapplugin.jar</i>
<b>MobiLink 16</b>	<i>%SQLANY16%\java\mlplugin.jar</i>
<b>UltraLite 16</b>	<i>%SQLANY16%\java\ulplugin.jar</i>
<b>Relay Server 16</b>	<i>%SQLANY16%\java\rsplugin.jar</i>

**Siehe auch**

- „Plug-In registrieren“ auf Seite 807

**Plug-In registrieren**

Registrieren Sie ein zusätzliches Plug-In, indem Sie die Registrierungsdatei oder die JAR-Datei des Plug-Ins angeben.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Aufgabe**

1. Wählen Sie in Sybase Central **Extras→Plug-Ins**.

Das Fenster **Plug-Ins für Sybase Central** wird aufgerufen.

2. Wählen Sie die Plug-Ins aus, die Sie registrieren wollen und klicken Sie auf **Registrieren**.

Der Assistent **Plug-In registrieren** wird aufgerufen.

3. Befolgen Sie die Anweisungen des Assistenten.

**Ergebnisse**

Das Plug-In wird registriert.

**Siehe auch**

- „Plug-In-Architektur von Sybase Central“ auf Seite 806

## SQL Anywhere 16-Plug-In

Mit dem Plug-In **SQL Anywhere 16** können Sie ein Upgrade einer bestehenden Datenbank durchführen, neue Datenbanken erstellen und Datenbanken verwalten. Sie können den gewünschten Modus im Menü **Modus** auswählen, oder indem Sie auf die Schaltfläche für den Modus in der Symbolleiste klicken.

Das Plug-In **SQL Anywhere 16** kann in einem der folgenden Modi ausgeführt werden:

- **Planungsmodus** Wenn Sie im **Planungsmodus** arbeiten, können Sie Datenbankobjekte wie z.B. Tabellen, Benutzer, Trigger, Indizes, entfernte Datenbankservers etc. erstellen und ändern. Sie können auch Tabellen Daten hinzufügen, neue Datenbanken erstellen und ein Upgrade bestehender Datenbanken durchführen.

Weitere Hinweise zu den Aufgaben, die Sie im Modus **Design** in einer SQL Anywhere-Datenbank ausführen können, finden Sie unter „[Tabellen, Ansichten und Indizes](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

- **Debug-Modus** Wenn Sie im **Debug-Modus** arbeiten, können Sie den SQL Anywhere-Debugger verwenden, um Unterstützung bei der Entwicklung von gespeicherten Prozeduren, Triggern und Event-Handletern in SQL zu erhalten.

Siehe „[SQL Anywhere-Debugger](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

- **Anwendungsprofilerstellung-Modus** Wenn Sie im Modus **Anwendungsprofilerstellung** arbeiten, können Sie die Anwendungsprofilerstellung oder die Diagnoseprotokollierung für Ihre Datenbank konfigurieren. Die generierten Daten unterstützen Sie dabei, das Interagieren der Anwendungen nachzuvollziehen und ggf. Performanceprobleme zu erkennen und zu eliminieren.

Siehe „[Anwendungsprofilerstellung](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].

### Von Assistenten generierte SQL-Anweisungen und Dienstprogrammbefehle anzeigen

Die letzte Seite der meisten **SQL Anywhere**-Plug-In-Assistenten zeigt die SQL-Anweisungen und Dienstprogrammbefehle an, die der jeweilige Assistent basierend auf Ihrer Auswahl ausführt.

Mit dem Klicken auf **Fertig stellen** werden die SQL-Anweisungen bzw. die Dienstprogrammbefehle ausgeführt. Sie können die SQL-Anweisungen auch in die Zwischenablage kopieren, auf **Abbrechen** klicken, um den Assistenten zu verlassen, und danach die SQL-Anweisungen über Interactive SQL ausführen.

Mit dieser Funktion können Sie die Assistenten verwenden, um SQL-Skripten ohne Änderung der Datenbank zu erstellen.

### Siehe auch

- „[Das Fenster Verbinden öffnen \(Sybase Central\)](#)“ auf Seite 14
- „[Tabellen, Ansichten und Indizes](#)“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „[Windows Mobile-Datenbanken erstellen \(Sybase Central\)](#)“ auf Seite 442

## Vergleich von Datenbankschemata

Sie können Sybase Central verwenden, um zwei Datenbanken zu vergleichen.

### Voraussetzungen

Sie müssen in beiden Datenbanken das SELECT ANY TABLE-Systemprivileg haben.

### Kontext und Bemerkungen

Beim Vergleichen von Datenbanken werden übereinstimmende Objekte nicht anhand der Objekt-ID ermittelt, sondern anhand von Name, Name und Eigentümer oder einer Kombination aus Namen und Eigentümern.

### Aufgabe

1. Verwenden Sie in Sybase Central das **SQL Anywhere 16**-Plug-In, um die Verbindung mit den beiden zu vergleichenden Datenbanken herzustellen.
2. Klicken Sie auf **Extras » SQL Anywhere 16 » Datenbankschemata vergleichen**.

Das Fenster **Datenbankschemata vergleichen** wird angezeigt.

3. Geben Sie die beiden Datenbanken, die Sie vergleichen möchten, in den Feldern **Datenbank 1** und **Datenbank 2** an.
4. Klicken Sie auf **Vergleichen**.

Auf der Registerkarte **Objekte** wird die Zusammenfassung der Unterschiede zwischen den Datenbanken angezeigt.

5. Klicken Sie auf der Registerkarte **Objekte** auf ein Element, um die SQL-Anweisungen für das betreffende Objekt anzuzeigen. Ein roter Hintergrund bedeutet SQL für Objekte, die nur in **Datenbank 1** enthalten sind, ein grüner Hintergrund SQL für Objekte, die nur in **Datenbank 2** enthalten sind, und ein blauer Hintergrund SQL für Objekte, die in beiden Datenbanken enthalten sind.

### Ergebnisse

Die Datenbanken werden verglichen.

### Nächste Schritte

Falls Sie das Schema von **Datenbank 1** konvertieren und dadurch an das Schema von **Datenbank 2** angleichen möchten, werden die für die Konvertierung notwendigen SQL-Anweisungen auf der Registerkarte **SQL-Skript** angezeigt.

### Siehe auch

- „SQL-Skriptdateien“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Interactive SQL“ auf Seite 814

## Konvertieren eines Datenbankschemas, um es an ein anderes anzugleichen

Sie können Sybase Central verwenden, um die Schemata zweier Datenbanken zu vergleichen. Die Ausgabe des Vergleichs hat die Form von SQL-Anweisungen, die Sie auf eine Datenbank anwenden können, um sie an eine andere Datenbank anzugleichen.

### Voraussetzungen

Sie müssen in beiden Datenbanken das SELECT ANY TABLE-Systemprivileg haben.

Sie müssen die erforderlichen Privilegien für jede SQL-Anweisung haben, die ausgeführt werden muss, um das Schema von **Datenbank 1** zu konvertieren und an das Schema von **Datenbank 2** anzugleichen.

Das generierte SQL-Skript enthält die notwendigen Anweisungen zum Konvertieren des Schemas von **Datenbank 1** und Angleichen an das Schema von **Datenbank 2**. Sie sollten darauf achten, **Datenbank 1** zu sichern, bevor Sie das Skript ausführen, und sicherstellen, dass keine anderen Verbindungen mit der Datenbank bestehen, während das Skript ausgeführt wird.

### Kontext und Bemerkungen

Die folgenden Vorgänge können nicht mit dieser Funktion für **Datenbank 1** ausgeführt werden und sind daher nicht in der Liste der SQL-Anweisungen enthalten, die während des Vergleichs generiert wird. Wenn einer dieser Vorgänge erforderlich ist, wird am Anfang der generierten Liste von SQL-Anweisungen eine Benachrichtigung angezeigt, in der der Vorgang beschrieben wird.

- Ändern des Dateinamens für einen DBSpace
- Ändern einer Domäne
- Ändern der Schreibschutzeinstellung für einen Fremdserver
- Ändern des DBSpaces für eine Tabelle
- Ändern der COMMIT-Aktion bzw. der SHARE BY ALL-Einstellung für eine globale temporäre Tabelle
- Ändern der Reihenfolge der Spalten in einer Tabelle oder einer globalen temporären Tabelle
- Ändern des Synchronisationstyps für eine Publikation

Beim Vergleichen von Datenbanken werden übereinstimmende Objekte nicht anhand der Objekt-ID ermittelt, sondern anhand von Name, Name und Eigentümer oder einer Kombination aus Namen und Eigentümern. Alle Objekte mit Namen in **Datenbank 1**, die nicht in **Datenbank 2** enthalten sind, einschließlich umbenannter Tabellen und Spalten, werden gelöscht und neu erstellt. Dies kann zu Datenverlust führen.

### Aufgabe

1. Verwenden Sie in Sybase Central das **SQL Anywhere 16**-Plug-In, um die Verbindung mit den beiden zu vergleichenden Datenbanken herzustellen.

2. Klicken Sie auf **Extras » SQL Anywhere 16 » Datenbanken vergleichen**.

Das Fenster **Datenbanken vergleichen** wird angezeigt.

3. Stellen Sie sicher, dass die Datenbank, deren Schema Sie konvertieren möchten, im Feld **Datenbank 1** angegeben ist und die Datenbank, in die Sie das Schema konvertieren möchten, im Feld **Datenbank 2**.
4. Klicken Sie auf **Vergleichen**.

Auf der Registerkarte **Objekte** wird die Liste der Objekte in den Datenbanken angezeigt. Die Registerkarte **SQL-Skript** enthält die generierten SQL-Anweisungen.

5. Klicken Sie auf der Registerkarte **Objekte** auf ein Element, um die Unterschiede in den SQL-Anweisungen für das betreffende Objekt anzuzeigen. Ein roter Hintergrund bedeutet SQL für Objekte, die nur in **Datenbank 1** enthalten sind, ein grüner Hintergrund SQL für Objekte, die nur in **Datenbank 2** enthalten sind, und ein blauer Hintergrund SQL für Objekte, die in beiden Datenbanken enthalten sind.
6. Klicken Sie auf der Registerkarte **SQL-Skript** auf **In Interactive SQL öffnen**, um Interactive SQL zu öffnen und die Anweisungen im Fensterausschnitt **SQL-Anweisungen** anzuzeigen. Sie können weitere Änderungen nach Bedarf vornehmen und die Anweisungen ausführen. Durch Ausführen der SQL-Anweisungen wird **Datenbank 1** an **Datenbank 2** angeglichen.

## Ergebnisse

Das Schema für **Datenbank 1** wird konvertiert und an das Schema für **Datenbank 2** angeglichen.

## Siehe auch

- „SQL-Skriptdateien“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Interactive SQL“ auf Seite 814

## Entity-Relationship-Diagramme anzeigen

Sie können mit Sybase Central ein Entity-Relationship-Diagramm der Tabellen in einer Datenbank anzeigen. Außerdem können Sie das Layout der ER-Diagramme importieren und exportieren.

## Voraussetzungen

Sie müssen die PUBLIC-Systemrolle haben.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zu einer Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Wählen Sie die Datenbank aus und klicken Sie dann im rechten Fensterausschnitt auf die Registerkarte **ER-Diagramm**, um das Diagramm anzuzeigen.

3. Klicken Sie auf **Datei » ER-Diagrammtabellen wählen** und geben Sie an, welche Tabellen im ER-Diagramm angezeigt werden sollen.
4. Klicken Sie auf **OK**.
5. (Optional) Ändern Sie die im Diagramm angezeigten Tabellen, indem Sie die Filtereinstellungen für die Datenbank ändern.

Welche Tabellen im Diagramm angezeigt werden, hängt von den Filtereinstellungen der Datenbank ab. Die Tabellen werden nach ihren Eigentümern gefiltert. Klicken Sie auf **Datei » Eigentümerfilter konfigurieren**.

6. Ordnen Sie die Objekte im Diagramm an. Sie können das Layout durch Ziehen der Objekte ändern. Die Layoutänderungen bleiben zwischen Sybase Central-Sitzungen erhalten. Sie können auch ein Layout importieren, indem Sie auf **Datei » Layout importieren** klicken.
7. (Optional) Doppelklicken Sie auf eine Tabelle, um die Spaltendefinitionen für diese Tabelle anzuzeigen.

## Ergebnisse

Das Entity-Relationship-Diagramm wird geändert.

## Nächste Schritte

Exportieren Sie das ER-Diagramm, indem Sie auf **Datei » Layout exportieren** klicken.

## Siehe auch

- [„Datenbankerstellung“ auf Seite 121](#)

## Zustand und Statistik von Datenbanken

Im Designmodus zeigt die Registerkarte **Übersicht** eine zusammenfassende Ansicht des Datenbankservers und seiner Merkmale. Diese Registerkarte enthält folgende Komponenten:

- **Datenbank** Dieser links oben angeordnete Ausschnitt zeigt allgemeine Informationen über den Datenbankserver.

Um die Software des SQL Anywhere-Datenbankservers zu aktualisieren, klicken Sie auf **Updates suchen**. Siehe [„Software-Updates“ auf Seite 879](#).

- **Funktionen** Links unten in diesem Fensterausschnitt finden Sie eine aktuelle Darstellung der Datenbank und ihrer Produkte und Merkmale. Wenn Sie auf einen Knoten im Diagramm klicken, wird der entsprechende Abschnitt im Ausschnitt **Gesundheit und Statistik** auf der rechten Seite erweitert. Mit einem weiteren Klick wird der Abschnitt wieder reduziert.

### Hinweis

Sie müssen den Abruf von MobiLink-Informationen einleiten, weil diese Knoten sonst als unbekannt angezeigt werden (grau abgeblendet). Siehe [MobiLink und Notifier auf Seite 813](#).

- **Gesundheit und Statistik** Auf der rechten Seite zeigt dieser Fensterausschnitt Statistiken und Informationen zum Gesamtstatus der Datenbank. Die folgenden, reduzierbaren Fensterausschnitte werden angezeigt:
  - **Statistiken** Zeigt allgemeine Statistiken an, wie z.B. die Anzahl der gelesenen Seiten und der Schreibvorgänge auf der Festplatte. Eine Warnung wird angezeigt, wenn nicht geplante Anforderungen vorhanden sind. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **DBSpaces** Zeigt eine Tabelle mit allen DBSpaces an. Eine Warnung wird angezeigt, wenn ein DBSpace weniger als 10% freien Speicher hat oder nicht gefunden werden kann. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **Transaktionslogs** Hier werden Informationen über das Transaktionslog und den Transaktionslog-Spiegel angezeigt, sofern vorhanden. Der Ausschnitt erscheint nur, wenn die Datenbank ein Transaktionslog hat. Eine Warnung wird angezeigt, wenn für eine Logdatei weniger als 10% freier Speicher auf der Festplatte vorhanden ist. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **Verbundene Benutzer** Hier werden verbundene Benutzer und Transaktionsstatistiken angezeigt. Die Anzeige erfolgt in Form einer Tabelle mit den 5 schnellsten Transaktionszeiten, sofern vorhanden. Außerdem wird eine Tabelle aller blockierten Verbindungen angezeigt, sofern vorhanden. Wenn blockierte Verbindungen vorhanden sind, wird eine Warnung angezeigt. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **Datenbankspiegelung** Hier werden Informationen für den Primär-, Arbitr-, Spiegel- und Kopierserver und für eine Datenbankspiegelung oder ein Scale-Out-System mit Schreibschutz angezeigt, wenn Sie mit dem Primärserver für das System verbunden sind. Dieser Fensterausschnitt erscheint nur, wenn die Datenbankspiegelung oder ein Scale-Out-System mit Schreibschutz verwendet wird. Eine Warnung wird angezeigt, wenn der Arbitr- oder Spiegelserver getrennt ist. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **Fremdserver** Hier wird eine Tabelle der von der Datenbank verwendeten Fremdserver angezeigt. Dieser Ausschnitt erscheint nur, wenn ein Fremdserver vorhanden ist. Eine Warnung wird hier angezeigt, wenn ein Fremdserver getrennt ist oder ein Fremdserver keine Verbindung aufnehmen kann. Klicken Sie auf die Warnung, um weitere Details zu erhalten.
  - **MobiLink und Notifier** Hier werden Statistiken für MobiLink und Notifier angezeigt. Dieser Ausschnitt erscheint nur, wenn MobiLink-Tabellen und -Ansichten in der Datenbank vorhanden sind.

#### Hinweis

Sie müssen auf die Schaltfläche **Aktualisieren** klicken, um die Informationen in diesem Ausschnitt zu aktualisieren. Anders als bei den Informationen in den anderen Fensterausschnitten wird dieser Ausschnitt nicht aktualisiert, wenn Sie auf **Ansicht » Aktualisieren** klicken (oder in der Symbolleiste auf das Symbol **Aktualisieren**). Sie müssen diese Informationen getrennt aktualisieren, weil sich die Aktualisierung auf die Performance der Datenbank auswirken könnte.

- **SQL Remote-Benutzer** Hier wird eine Tabelle mit allen SQL Remote-Benutzern und ihren letzten Sende- und Empfangszeiten angezeigt. Der Ausschnitt erscheint nur, wenn in der Datenbank SQL Remote-Benutzer registriert sind.

## Datenbank dokumentieren

Sie können eine HTML-Datei generieren, die die Abhängigkeiten und Referenzen für eine Datenbank mithilfe des **Assistenten zum Erstellen der Datenbankdokumentation** in Sybase Central anzeigt.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Datenbankdokumentation erstellen**.
2. Befolgen Sie die Anweisungen des Assistenten.

### Ergebnisse

Die generierte Dokumentation wird in HTML-Dateien gespeichert, um Navigation und Überprüfung zu erleichtern.

## Interactive SQL

Interactive SQL ist ein Tool, das zum Lieferumfang von SQL Anywhere gehört und mit dem Sie für die folgenden Datenbanken SQL-Anweisungen ausführen, SQL-Skriptdateien ausführen und Datenbankdaten anzeigen können:

- SQL Anywhere-Datenbanken
- SAP HANA-Datenbanken
- SAP Sybase IQ-Datenbanken
- UltraLite-Datenbanken

### Nur von Interactive SQL aus verwendbare SQL-Anweisungen

Interactive SQL unterstützt alle SQL-Anweisungen, die von SQL Anywhere- und UltraLite-Datenbanken unterstützt werden, sowie mehrere SQL-Anweisungen, die nur von Interactive SQL aus verwendbar sind.

### Siehe auch

- [„SQL-Anweisungen für Interactive SQL“ auf Seite 821](#)

## Interactive SQL starten

Sie können Interactive SQL verwenden, um eine Verbindung mit einer SQL Anywhere-Datenbank, einer UltraLite-Datenbank, einer SAP Sybase IQ-Datenbank, einer SAP HANA-Datenbank oder einer generischen ODBC-Datenbank herzustellen.

### Voraussetzungen

**Linux** Sie müssen eine Version von Linux verwenden, die die Linux-Desktop-Symbole unterstützt, und diese müssen bei der Installation von SQL Anywhere installiert worden sein.

**Unix und Mac OS X** Das Sourcen der SQL Anywhere-Dienstprogramme muss bereits abgeschlossen sein. Siehe „[Unix- und Mac OS X-Umgebungsvariablen](#)“ auf Seite 467.

### Aufgabe

- Öffnen Sie Interactive SQL und stellen Sie eine Verbindung mit einer Datenbank her.

Option	Aktion
Befehlszeile bzw. Unix	<p>Führen Sie den folgenden Befehl aus:</p> <pre>dbisql</pre> <p>Wenn Sie nicht die Option -c verwenden, durch die die Verbindungsparameter für die Datenbank festgelegt werden, oder wenn Sie nicht genügend Verbindungsparameter angeben, wird das Fenster <b>Verbinden</b> angezeigt, in dem Sie Verbindungsinformationen für die Datenbank eingeben können.</p>
Windows	<ol style="list-style-type: none"> <li>Klicken Sie auf <b>Start » Programme » SQL Anywhere 16 » Administrations- tools » Interactive SQL</b>.</li> <li>Klicken Sie auf <b>Datenbanktyp ändern</b> und wählen Sie den Typ der Datenbank, mit der eine Verbindung hergestellt werden soll. Sie können sich verbinden mit einer SQL Anywhere-Datenbank, einer UltraLite-Datenbank, einer SAP Sybase IQ-Datenbank, einer SAP HANA-Datenbank oder einer generischen ODBC-Datenbank.</li> </ol> <p>Um beispielsweise eine Verbindung mit einer SQL Anywhere-Datenbank herzustellen, klicken Sie auf <b>Datenbanktyp ändern</b> und anschließend auf <b>SQL Anywhere</b>.</p> <ol style="list-style-type: none"> <li>Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</li> <li>Klicken Sie auf <b>Verbinden</b>.</li> </ol>

Option	Aktion
Sybase Central	<p>a. Klicken Sie auf <b>Extras » SQL Anywhere 16 » Interactive SQL öffnen</b>.</p> <p>b. Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</p> <p>c. Klicken Sie auf <b>Verbinden</b>.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>Tipp</b>          Sie können auch eine der folgenden Methoden verwenden, um Interactive SQL von Sybase Central aus aufzurufen:</p> <ul style="list-style-type: none"> <li>● Eine Datenbank auswählen und auf <b>Datei » Interactive SQL öffnen</b> klicken.</li> <li>● Auf eine Datenbank rechtsklicken und auf <b>Interactive SQL öffnen</b> klicken.</li> <li>● Auf eine gespeicherte Prozedur rechtsklicken und auf <b>Von Interactive SQL aus ausführen</b> klicken. Interactive SQL wird im Fensterausschnitt <b>SQL-Anweisungen</b> mit einem Aufruf der Prozedur geöffnet.</li> <li>● Auf eine Tabelle oder Ansicht rechtsklicken und auf <b>Daten in Interactive SQL anzeigen</b> klicken. Interactive SQL öffnet mit einem <code>SELECT * FROM table-name</code> und führt die Abfrage aus.</li> </ul> </div>
Mac OS X	<p>a. Doppelklicken Sie im Finder auf <b>Interactive SQL</b> in <code>/Applications/SQLAnywhere16</code>.</p> <p>b. Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</p> <p>c. Klicken Sie auf <b>Verbinden</b>.</p>
Linux	<p>a. Klicken Sie auf <b>Anwendungen » SQL Anywhere 16 » Administrations-tools » Interactive SQL</b>.</p> <p>b. Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</p> <p>c. Klicken Sie auf <b>Verbinden</b>.</p>

## Ergebnisse

Interactive SQL wird gestartet und Sie werden mit der Datenbank verbunden.

## Beispiel

Wenn Sie über die Befehlszeile Interactive SQL starten und eine Verbindung mit der Beispieldatenbank herstellen möchten, führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;DSN=SQL Anywhere 16 Demo"
```

**Siehe auch**

- „Das Fenster Verbinden öffnen (Sybase Central)“ auf Seite 14
- „Interactive SQL-Dienstprogramm (dbisql)“ auf Seite 939
- „Verbindungsparameter“ auf Seite 337

## Interactive SQL-Navigation

Das Interactive SQL-Fenster ist in Fensterausschnitte aufgeteilt:

- **SQL-Anweisungen** In diesen Fensterausschnitt geben Sie die SQL-Anweisungen ein, mit denen Sie auf die Daten zugreifen und diese ändern.
- **Ergebnisse** Der Fensterausschnitt **Ergebnisse** enthält zwei Registerkarten, die am unteren Rand des Fensterausschnitts **Ergebnisse** angezeigt werden.

Auf der Registerkarte **Ergebnisse** werden die Ergebnisse der ausgeführten Anweisungen angezeigt. Sie können die Ergebnismenge auf der Registerkarte **Ergebnisse** bearbeiten.

Auf der Registerkarte **Meldungen** werden Meldungen vom Datenbankserver über die SQL-Anweisungen angezeigt, die Sie in Interactive SQL ausführen.

Ergebnisse von grafischen Plänen für SQL Anywhere-Datenbanken und Textplänen für UltraLite-Datenbanken werden in separaten Plananzeige-Fenstern angezeigt.

**Siehe auch**

- „Ergebnismengen in Interactive SQL“ auf Seite 830
- „Grafische Pläne mit detaillierten und Knotenstatistiken erstellen“ auf Seite 839

## Interactive SQL anpassen

Sie können Interactive SQL anpassen, indem Sie konfigurieren, wie Ergebnismengen angezeigt werden, Warnmeldungen deaktivieren und Interactive SQL als Standardeditor für .sql-Dateien festlegen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Mithilfe des Fensters **Optionen** können Sie Einstellungen für die Registerkarten und Fensterausschnitte in Interactive SQL konfigurieren. Beim Deployment von Interactive SQL können Sie im Fenster **Optionen** steuern, welche Funktionen angezeigt oder aktiviert werden.

**Aufgabe**

- Öffnen Sie Interactive SQL und stellen Sie eine Verbindung mit einer Datenbank her.

Option	Aktion
Anzeige von Ergebnismengen anpassen	<p>a. Wählen Sie, ob die Ergebnisse als scrollfähige Tabelle oder als Text angezeigt werden sollen. Klicken Sie auf <b>Daten</b> und wählen Sie dann eine der folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• <b>Ergebnisse als abrollbare Tabelle anzeigen</b> Sie können die Ergebnismenge in diesem Format bearbeiten. Dies ist die Standardeinstellung.</li> <li>• <b>Ergebnisse als Text anzeigen</b> Diese Option zeigt die Ergebnismenge als Text in einer Schrift mit fester Buchstabenbreite an. Die Ergebnismenge ist in diesem Format nicht bearbeitbar.</li> </ul> <p>b. Führen Sie eine Abfrage aus.</p> <p>Sie müssen eine neue Abfrage ausführen, damit die Änderungen der Tabellenbearbeitung wirksam werden.</p> <p>c. Klicken Sie mit der rechten Maustaste innerhalb der Ergebnismenge und wählen Sie eine der folgenden Optionen:</p> <ul style="list-style-type: none"> <li>• <b>Spalten an Daten anpassen</b> Die Tabellenspalten werden so verbreitert, dass die Werte nicht abgeschnitten werden.</li> <li>• <b>Spalten an Fenstergröße anpassen</b> Die Tabellenspalten erhalten jeweils die gleiche Breite, sodass sie alle in das Fenster passen und keine horizontale Bildlaufleiste erforderlich ist.</li> </ul>
Warnmeldungen deaktivieren	<p>Sie können bestimmte Warnmeldungen in Interactive SQL deaktivieren. Beispiel: Sie können die Warnung unterdrücken, die angezeigt wird, wenn im Fens- terausschnitt <b>SQL-Anweisungen</b> nicht gespeicherter Text vorhanden ist und Sie auf <b>Datei » Beenden</b> klicken.</p> <p>a. Klicken Sie auf <b>Extras » Optionen » Meldungen</b>.</p> <p>b. Deaktivieren Sie die Meldungen in der Liste <b>Optionale Meldungen</b>.</p>
Interactive SQL als Standardeditor für .sql-Dateien festlegen	<p>a. Klicken Sie auf <b>Extras » Optionen » Allgemein</b>.</p> <p>b. Klicken Sie auf <b>Interactive SQL als Standardeditor für .SQL-Dateien und Plandateien einrichten</b>.</p> <p>c. Klicken Sie auf <b>OK</b>.</p>

## Ergebnisse

Interactive SQL wird angepasst.

**Siehe auch**

- „Konfiguration der Administrationstools“ [[SQL Anywhere Server - Programmierung](#)]
- „Fehlerbehandlung von unerwarteten Symbolen bei der Anzeige von Daten“ auf Seite 504
- „SQL-Skriptdateien“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SQL-Skriptdateien“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## SQL-Anweisungen in Interactive SQL

In erster Linie wird Interactive SQL dazu verwendet, Tabellendaten zu durchsuchen. Interactive SQL ruft die Daten ab, indem eine Anforderung an Ihren Datenbankserver gesendet wird. Der Datenbankserver sucht die Daten und gibt sie an Interactive SQL zurück.

In Interactive SQL wird die erste Ergebnismenge der zuletzt ausgeführten Anweisung angezeigt. Standardmäßig erscheinen Zeilennummern links von der Ergebnismenge.

**Hinweis**

Der Datenbankserver erstellt Schemasperrungen für Tabellen, die Sie in Interactive SQL anzeigen, auch wenn Sie die Tabelle nicht ändern.

Interactive SQL kann aber auch automatisch versuchen, die Datenbankschemasperrungen freizugeben, die bei der Anzeige Ihrer Ergebnismenge erstellt werden. Klicken Sie dafür in Interactive SQL auf **Extras » Optionen » SQL Anywhere** und anschließend auf **Datenbanksperren automatisch freigeben**.

Nachdem Sie diese Option ausgewählt haben, überprüft Interactive SQL jedes Mal, wenn Sie eine Anweisung mit darauf folgender Rückgabe einer Ergebnismenge ausgeführt haben, ob im Rahmen Ihrer Verbindung nicht festgeschriebene Änderungen in der Datenbank vorhanden sind. Wenn keine gefunden werden, gibt Interactive SQL Ihre Schemasperrungen frei; andernfalls bleiben die Schemasperrungen erhalten. Das heißt, Interactive SQL gibt Ihre Schemasperrungen nicht frei, wenn nicht festgeschriebene Änderungen in der Datenbank vorhanden sind.

## SQL-Anweisungen ausführen (Interactive SQL)

Sie können über Interactive SQL mehrere SQL-Anweisungen ausführen, sofern jede Anweisung mit einem Befehlstrennzeichen endet.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Das Befehlstrennzeichen wird mit der `command_delimiter`-Option festgelegt und ist standardmäßig ein Semikolon (;). Eine Alternative zur Verwendung des Semikolons besteht darin, das Trennzeichen **go** in einer eigenen Zeile am Anfang der Zeile einzugeben.

## Aufgabe

1. Geben Sie in Interactive SQL Ihre Abfragen im Fensterausschnitt **SQL-Anweisungen** ein.
2. Wählen Sie eine der folgenden Optionen, um die SQL-Anweisungen auszuführen:

Option	Aktion
Alle SQL-Anweisungen ausführen	Drücken Sie F5 oder klicken Sie auf <b>SQL » Ausführen</b> , um alle Anweisungen auszuführen.
Ausgewählte SQL-Anweisungen ausführen	Wählen Sie die gewünschten Anweisungen aus und drücken Sie dann F9 oder klicken Sie auf <b>SQL » Markierte Anweisungen ausführen</b> , um die ausgewählten Anweisungen auszuführen.
SQL-Anweisungen einzeln ausführen	Platzieren Sie Ihren Cursor in der Anweisung, die Sie ausführen möchten, und drücken Sie dann Umschalt+F9 oder klicken Sie auf <b>SQL » Einzelschritt</b> , um die Anweisung auszuführen.

## Ergebnisse

Die SQL-Anweisungen werden ausgeführt wie angegeben. Die Ergebnismenge wird auf der Registerkarte **Ergebnisse** des Fensterausschnitts **Ergebnisse** angezeigt. In Interactive SQL wird die erste Ergebnismenge der zuletzt ausgeführten Anweisung angezeigt. Standardmäßig erscheinen Zeilennummern links von der Ergebnismenge.

## Nächste Schritte

Sie können die Symbolleistenschaltfläche zum Ausführen von Anweisungen permanent so konfigurieren, dass alle oder ausgewählte Anweisungen ausgeführt werden.

Klicken Sie auf **Extras » Optionen » Symbolleiste**. Wählen Sie eine der folgenden Optionen:

- Wenn alle SQL-Anweisungen ausgeführt werden sollen, klicken Sie auf **Ausführen**. Dies ist die Standardeinstellung.
- Wenn nur die ausgewählten SQL-Anweisungen ausgeführt werden sollen, klicken Sie auf **Markierte Anweisungen ausführen**.

## Siehe auch

- „command\_delimiter-Option [Interactive SQL]“ auf Seite 854
- „Rückgabe von mehreren Ergebnismengen“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Fehlerbehandlung von unerwarteten Symbolen bei der Anzeige von Daten“ auf Seite 504
- „Konfiguration der Administrationstools“ [*SQL Anywhere Server - Programmierung*]

## SQL-Anweisungen für Interactive SQL

Die folgenden SQL-Anweisungen werden nur von Interactive SQL unterstützt:

- „CLEAR-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CONFIGURE-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CONNECT-Anweisung [ESQL] [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DESCRIBE-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DISCONNECT-Anweisung [ESQL] [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „EXIT-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „HELP-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „INPUT-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „OUTPUT-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „PARAMETERS-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „READ-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET CONNECTION-Anweisung [Interactive SQL] [ESQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „START SERVER-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „START LOGGING-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „STOP LOGGING-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SYSTEM-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

### Siehe auch

- „SQL-Anweisungen“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „UltraLite-SQL-Anweisungen“ [*UltraLite - Datenbankverwaltung*]

## SQL-Skriptdateien in Interactive SQL

SQL-Skriptdateien sind Textdateien, die SQL-Anweisungen enthalten; sie sind dann nützlich, wenn Sie dieselben SQL-Anweisungen wiederholt ausführen möchten. Sie können Interactive SQL verwenden, um Skriptdateien zu öffnen, anzuzeigen, auszuführen und zu speichern.

Es gibt folgende Möglichkeiten, SQL-Skriptdateien über Interactive SQL auszuführen:

- Sie können Skriptdateien mit der READ-Anweisung von Interactive SQL ausführen. Die folgende Anweisung führt zum Beispiel die Datei *temp.sql* aus:

```
READ temp.sql;
```

- Sie können eine Skriptdatei in den Fensterausschnitt **SQL-Anweisungen** laden und direkt von dort ausführen.

Um Skriptdateien in den Fensterausschnitt **SQL-Anweisungen** zu laden, klicken Sie auf **Datei » Öffnen**. Geben Sie nach der Aufforderung den Dateinamen ein, z.B. *temp.sql*.

- Sie können eine Skriptdatei ausführen, ohne sie zu laden, indem Sie auf **Datei » Skript ausführen** klicken.
- Sie können eine Skriptdatei als Befehlszeilenargument für Interactive SQL eingeben.

Wenn Sie eine *.sql*-Datei bearbeiten, speichert Interactive SQL automatisch eine Sicherungskopie, wenn Folgendes geschieht:

- Sie führen eine Anweisung aus.
- Die Datei wurde 30 Sekunden lang nicht verändert.

Wenn Sie eine Datei bearbeiten und Interactive SQL unerwartet geschlossen wird, werden Sie beim nächsten Starten von Interactive SQL aufgefordert, die Datei wiederherzustellen.

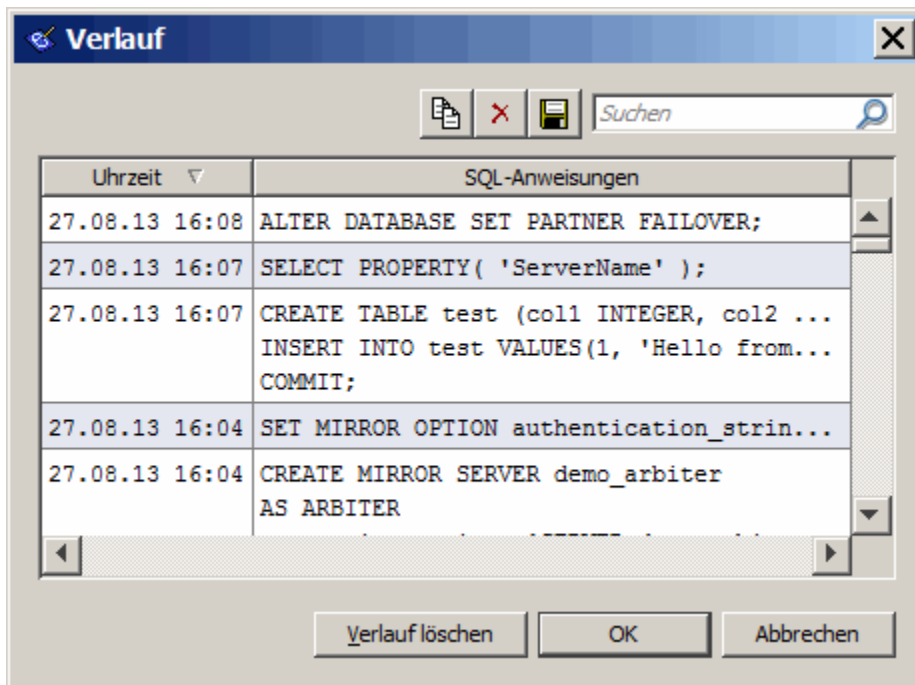
### Siehe auch

- „SQL-Skriptdateien“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „READ-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Favoriten gemeinsam nutzen“ auf Seite 826

## Interactive SQL-Verlauf

Wenn Sie eine Anweisung ausführen, speichert Interactive SQL diese automatisch in einer Verlaufsliste, die auch zwischen Interactive SQL-Sitzungen erhalten bleibt. Interactive SQL speichert im Verlauf maximal die 50 zuletzt ausgeführten Anweisungen.

Im Fenster **Verlauf** können Sie die gesamte Liste der Anweisungen anzeigen. Um auf das Fenster **Verlauf** zuzugreifen, drücken Sie Strg+H oder klicken Sie in der Symbolleiste auf **SQL » Verlauf**.



Die zuletzt ausgeführten Anweisungen werden in der Liste unten angezeigt. Wenn Sie einen Befehl erneut aufrufen möchten, wählen Sie ihn aus und klicken Sie dann auf **OK**. Er erscheint im Fensterausschnitt **SQL-Anweisungen** von Interactive SQL. Sie können im Fenster **Verlauf** mehrere Anweisungen auswählen.

Sie können Anweisungen aus dem Fenster **Verlauf** kopieren, um sie an anderer Stelle zu verwenden, indem Sie die Anweisungen im Fenster **Verlauf** auswählen und dann Strg+C drücken oder auf **Kopieren** klicken. Klicken Sie auf **OK**, um die ausgewählten Anweisungen in den Fensterausschnitt **SQL-Anweisungen** von Interactive SQL zu kopieren. Wenn Sie mehrere Anweisungen kopieren, werden diese durch das Anweisungstrennzeichen voneinander getrennt (standardmäßig ein Semikolon).

Sie können Ihre Anweisungen in Textdateien speichern, um sie in einer späteren Interactive SQL-Sitzung zu verwenden, indem Sie Strg+S drücken oder auf **Verlauf als .SQL-Datei speichern** klicken, einen Speicherort und einen Namen für die .sql-Datei angeben und dann auf **Speichern** klicken. Außerdem können Sie SQL-Skriptdateien in der Liste **Favoriten** speichern.

Der Inhalt des Fensters **Verlauf** bleibt zwischen Interactive SQL-Sitzungen erhalten. Sie können die ausgewählten Anweisungen aus dem Verlauf entfernen, indem Sie auf **Löschen** klicken. Sie können alle Anweisungen aus dem Verlauf entfernen, indem Sie auf **Verlauf löschen** klicken. Beide Aktionen können nicht rückgängig gemacht werden.

Sie können Anweisungen auch ohne das Fenster **Verlauf** erneut aufrufen. Klicken Sie in der Symbolleiste auf die Symbole **Vorherige SQL-Anweisung wieder aufrufen** bzw. **Nächste SQL-Anweisung wieder aufrufen**, um durch ihre Anweisungen zu navigieren, oder drücken Sie Alt+Pfeil nach rechts bzw. Alt+Pfeil nach links.

**Hinweis**

Wenn Sie eine SQL-Anweisung ausführen, die Kennwortinformationen enthält (CREATE USER, CONNECT oder CREATE EXTERNLOGIN), erscheinen die Kennwortinformationen für die Dauer der aktuellen Interactive SQL-Sitzung im Fenster **Verlauf**.

Wenn Sie den Anweisungsverlauf in nachfolgenden Interactive SQL-Sitzungen anzeigen, werden die Kennwörter in allen Anweisungen mit Kennwortinformationen durch ... ersetzt. Sie führen z.B. folgende Anweisung in Interactive SQL aus:

```
CREATE USER testuser
  IDENTIFIED BY testpassword;
```

In nachfolgenden Interactive SQL-Sitzungen erscheint die folgende Anweisung im Fenster **Verlauf**:

```
CREATE USER testuser
  IDENTIFIED BY ...;
```

Siehe auch

- [„SQL-Skriptdateien, SQL-Anweisungen und Verbindungen zu den Favoriten hinzufügen“ auf Seite 824](#)

SQL-Skriptdateien, SQL-Anweisungen und Verbindungen zu den Favoriten hinzufügen

In Interactive SQL können Sie häufig verwendete SQL-Skriptdateien, SQL-Anweisungen und Verbindungen in einer Favoritenliste speichern. Eine Favoritenliste wird für einen bestimmten Benutzer eingerichtet und kann von anderen Benutzern nicht gesehen werden.

Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

Aufgabe

1. Klicken Sie auf **Favoriten » Zu Favoriten hinzufügen**.

Option	Aktion
SQL-Skriptdateien	<div>a. Öffnen Sie die SQL-Skriptdatei, die Sie zu Ihren Favoriten hinzufügen möchten.</div> <div>b. Klicken Sie auf <b>Die geöffnete Datei 'Dateiname' hinzufügen</b>. Geben Sie im Feld <b>Name</b> einen Namen für die .sql-Datei ein.</div>
SQL-Anweisungen	Klicken Sie auf <b>SQL-Anweisungen hinzufügen</b> . Im Feld <b>Name</b> geben Sie einen Namen für den Favoriten ein.

Option	Aktion
Verbindungen	Klicken Sie auf <b>Das Verbindungskennwort speichern</b> . Im Feld <b>Name</b> geben Sie einen Namen für die Verbindung ein.

2. Klicken Sie auf **OK**.

## Ergebnisse

Die SQL-Skriptdatei, SQL-Anweisung bzw. Verbindung wird in Ihrer Favoritenliste gespeichert.

## Nächste Schritte

Sie können Ihre Favoriten öffnen, indem Sie auf **Favoriten** klicken und den gewünschten Favoriten auswählen. Sie können auch Ihre Favoriten in einer Seitenleiste anzeigen, indem Sie auf **Favoriten » Favoriten anzeigen** klicken.

Außerdem können Sie Ihre Favoriten bearbeiten, gemeinsam nutzen oder sichern.

## Siehe auch

- „Konfiguration der Administrationstools“ [[SQL Anywhere Server - Programmierung](#)]
- „Favoriten bearbeiten“ auf Seite 825
- „Favoriten gemeinsam nutzen“ auf Seite 826

## Favoriten bearbeiten

In Interactive SQL können Sie die Einträge in Ihrer Favoritenliste bearbeiten.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Aufgabe

1. Klicken Sie auf **Favoriten » Favoriten anzeigen**.

Das Fenster **Favoriten** erscheint links neben dem Interactive SQL-Fenster.

2. Rechtsklicken Sie auf einen Favoriten und klicken Sie dann auf "Bearbeiten".

3. Befolgen Sie die Anweisungen im Fenster.

4. Klicken Sie auf **Speichern**.

## Ergebnisse

Ihre Favoritenliste wird bearbeitet.

## Nächste Schritte

Sie können Ihre Favoriten gemeinsam nutzen.

## Siehe auch

- „SQL-Skriptdateien, SQL-Anweisungen und Verbindungen zu den Favoriten hinzufügen“ auf Seite 824
- „Favoriten gemeinsam nutzen“ auf Seite 826

## Favoriten gemeinsam nutzen

In Interactive SQL können Sie alle Ihre Favoriten in eine *.fav*-Datei exportieren. Sie können die Favoriten auf einen anderen Computer kopieren oder die Datei als Sicherung speichern.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

- Klicken Sie in Interactive SQL auf **Favoriten**.

Option	Aktion
Favoriten exportieren	Klicken Sie auf <b>Favoriten exportieren</b> .  Geben Sie einen Dateinamen für die <i>.fav</i> -Datei an und klicken Sie dann auf <b>Exportieren</b> .
Favoriten importieren	Klicken Sie auf <b>Favoriten importieren</b> .  Navigieren Sie zur Datei <i>Dateiname.fav</i> und klicken Sie dann auf <b>Importieren</b> .

### Ergebnisse

Die Datei wird exportiert bzw. importiert.

## Anweisungen in Interactive SQL protokollieren

Die Protokollierungsfunktion von Interactive SQL erfasst SQL-Anweisungen während der Ausführung. Anweisungen werden erfasst, bis Sie den Protokollierungsprozess stoppen oder die aktuelle Sitzung beenden.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Zum Starten oder Stoppen der Protokollierung können Sie entweder das Menü **SQL** oder SQL-Anweisungen verwenden.

Die aufgezeichneten Anweisungen werden in einer Logdatei zur weiteren Verwendung gespeichert.

Sobald Sie die Protokollierung starten, werden alle ausgeführten Anweisungen protokolliert, einschließlich derjenigen, die nicht korrekt ausgeführt werden können.

## Aufgabe

1. Öffnen Sie Interactive SQL.
2. So starten Sie die Protokollierung:

Option	Aktion
Menü <b>SQL</b>	<ol style="list-style-type: none"> <li>a. Klicken Sie auf <b>SQL » Protokollierung starten</b>.</li> <li>b. Geben Sie im Fenster <b>Speichern unter</b> einen Speicherort und einen Namen für die Logdatei ein. Benennen Sie die Datei z.B. <i>mylogs.sql</i>.</li> <li>c. Klicken Sie auf <b>Speichern</b>, wenn Sie die Eingaben vorgenommen haben.</li> </ol>
START LOGGING-Anweisung	<p>Führen Sie eine START LOGGING-Anweisung aus.</p> <p>Um beispielsweise die Protokollierung in einer Datei namens <i>c:\mylogs.sql</i> zu starten, führen Sie die folgende Anweisung aus:</p> <pre>START LOGGING "c:\mylogs.sql";</pre>

3. So stoppen Sie die Protokollierung:

Option	Aktion
Menü <b>SQL</b>	Klicken Sie auf <b>SQL » Protokollierung stoppen</b> .
STOP LOGGING-Anweisung	<p>Führen Sie die folgende Anweisung aus:</p> <pre>STOP LOGGING;</pre>

## Ergebnisse

Die Protokollierung von Anweisungen in Interactive SQL wird gestartet bzw. gestoppt.

**Siehe auch**

- „START LOGGING-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „STOP LOGGING-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SQL-Anweisungen protokollieren“ auf Seite 164
- „isql\_command\_timing-Option [Interactive SQL]“ auf Seite 859

# Abbrechen von Anweisungen in Interactive SQL

Ein Abbruchbefehl bricht die aktuelle Prozessverarbeitung ab und wartet auf den nächsten Befehl. Mit der Schaltfläche **Stopp** in der Symbolleiste von Interactive SQL können Sie eine Anweisung abbrechen.

Wenn eine SQL-Skriptdatei verarbeitet wurde, werden Sie aufgefordert, eine Aktion auszuführen (**Befehlsdatei stoppen**, **Fortsetzen** oder **Interactive SQL beenden**). Diese Aktionen können durch die Interactive SQL-Option `on_error` gesteuert werden.

**Siehe auch**

- „on\_error-Option [Interactive SQL]“ auf Seite 865

# Suchen nach Tabellen, Spalten und Prozeduren in Interactive SQL

Beim Eingeben von Anweisungen in Interactive SQL können Sie die Namen von Tabellen, Spalten oder Prozeduren nachschlagen, die in der aktuellen Datenbank gespeichert sind, und sie an der Cursorposition einfügen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Aufgabe**

1. Klicken Sie in Interactive SQL auf **Extras** und wählen Sie dann eine der folgenden Optionen:

Option	Aktion
Tabellennamen nachschlagen	Klicken Sie auf <b>Tabellennamen nachschlagen</b> oder drücken Sie F7.  Suchen Sie die Tabelle und wählen Sie sie aus.
Spaltennamen nachschlagen	Klicken Sie auf <b>Tabellennamen nachschlagen</b> oder drücken Sie F7.  Suchen Sie die Tabelle, die die Spalte enthält, und wählen Sie diese aus.  Klicken Sie auf <b>Spalten anzeigen</b> .

Option	Aktion
Prozedurnamen nachschlagen	Klicken Sie auf <b>Prozedurnamen nachschlagen</b> oder drücken Sie F8. Suchen Sie die Prozedur und wählen Sie sie aus.

**Tipp**

- Geben Sie die ersten Zeichen eines Tabellen- oder Prozedurnamens ein, um die Liste der Elemente einzugrenzen.
- Verwenden Sie die SQL-Platzhalterzeichen "%" (Prozentzeichen) für Übereinstimmungen mit einer beliebigen Zeichenfolge mit null oder mehr Zeichen und "\_" (Unterstrich) für Übereinstimmungen mit einem beliebigen Zeichen.
- Suchen Sie nach einem Wildcard-Zeichen in einem Tabellennamen, indem Sie ihm ein Escapezeichen voranstellen. Das Escapezeichen für SQL Anywhere-ODBC-Treiber und SQL Anywhere-JDBC-Treiber ist "~" (Tilde).

2. Klicken Sie auf **OK**, um den Namen im Fensterausschnitt **SQL-Anweisungen** an der Cursorposition einzufügen.

**Ergebnisse**

Der Tabellen-, Spalten- bzw. Prozedurname wird gefunden und in den Fensterausschnitt **SQL-Anweisungen** eingefügt.

**Siehe auch**

- „Textvervollständigung“ auf Seite 873

## SQL-Anweisungen aus Interactive SQL Ergebnismengen generieren

Sie können INSERT-, DELETE- und UPDATE-Anweisungen für ausgewählte Zeilen in einer Ergebnismenge generieren.

**Voraussetzungen**

Sie müssen eine Abfrage ausgeführt haben, um eine Ergebnismenge zu erhalten, auf die Sie die Aufgabe anwenden können.

**Aufgabe**

1. Wählen Sie die Zeile(n) aus, für die Sie eine Anweisung generieren möchten.
2. Rechtsklicken Sie auf die ausgewählten Zeilen, klicken Sie auf **Generieren** und anschließend auf **INSERT-Anweisung**, **DELETE-Anweisung** oder **UPDATE-Anweisung**.

## Ergebnisse

Die Anweisung wird in die Zwischenablage kopiert.

## Nächste Schritte

Führen Sie die generierte Anweisung aus. Sie müssen die erforderlichen Privilegien zum Ausführen der INSERT-, DELETE- oder UPDATE-Anweisung haben.

## Ergebnismengen in Interactive SQL

Wenn Sie eine Abfrage in Interactive SQL ausgeführt haben, können Sie die Ergebnismenge sortieren und bearbeiten, um die Datenbank zu ändern.

Um eine Ergebnismenge zu sortieren, klicken Sie auf der Registerkarte **Ergebnisse** auf einen Spaltentitel, um die Ergebnisse nach der betreffenden Spalte zu sortieren. Wenn die Registerkarte **Ergebnisse** nicht die gesamte Ergebnismenge enthält, werden Sie aufgefordert, die übrigen Ergebnisse abzurufen. Andernfalls werden nur die aktuell abgerufenen Ergebnisse sortiert.

Sie können auch Zeilen aus der Ergebnismenge auswählen und diese in eine andere Anwendung kopieren. Feldbegrenzer, Anführungszeichen und Escapezeichen für die Ergebnisse können Sie mit den Optionen `isql_field_separator`, `isql_quote` und `isql_escape_character` steuern. Die Optionen können Sie im Fenster **Optionen** in Interactive SQL oder durch Ausführen der SET OPTION-Anweisung anzeigen und ändern.

In Interactive SQL können Zeilen bearbeitet, eingefügt und gelöscht werden. Das Bearbeiten der Ergebnismenge hat dieselbe Wirkung wie UPDATE-, INSERT- oder DELETE-Anweisungen. Nach dem Bearbeiten der Ergebnismenge werden die entsprechenden INSERT-, UPDATE- und DELETE-Anweisungen dem Befehlsverlauf von Interactive SQL hinzugefügt.

Um eine Zeile oder einen Wert in der Ergebnismenge zu bearbeiten, müssen Sie die entsprechenden Privilegien für die Tabelle bzw. Spalte haben, in der Sie die Werte ändern möchten. Wenn Sie beispielsweise eine Zeile löschen möchten, müssen Sie das DELETE-Privileg für die Tabelle haben, zu der die Zeile gehört.

Unter folgenden Bedingungen können Sie eine Ergebnismenge nicht bearbeiten:

- Wenn Sie Spalten aus einer Tabelle mit einem Primärschlüssel auswählen, aber nicht alle Primärschlüsselspalten markieren.
- Wenn Sie versuchen, die Ergebnismenge eines JOINS (z.B. bei Daten aus mehr als einer Tabelle in der Ergebnismenge) zu bearbeiten.
- Wenn Sie versuchen, eine Tabelle zu bearbeiten, deren Bearbeitung deaktiviert ist.

Unter folgenden Voraussetzungen können Sie die Ergebnismenge eventuell nicht bearbeiten:

- Wenn Sie versuchen, eine Zeile bzw. Spalte zu bearbeiten, für die Sie keine Privilegien haben.
- Wenn Sie einen ungültigen Wert eingeben (z.B. eine Zeichenfolge in einer numerischen Spalte oder NULL in einer Spalte, die NULL nicht zulässt).

Falls der Bearbeitungsvorgang fehlschlägt, wird eine Interactive SQL-Fehlermeldung mit einer Beschreibung des Fehlers angezeigt, und die Werte der Datenbanktabelle werden nicht geändert.

**Siehe auch**

- „Interactive SQL-Optionen“ auf Seite 851
- „Interactive SQL-Verlauf“ auf Seite 822
- „Tabellenbearbeitung in Interactive SQL deaktivieren“ auf Seite 832

**Zeilen in Interactive SQL-Ergebnismengen bearbeiten**

Über Interactive SQL können Sie Werte in vorhandenen Zeilen von Datenbanktabellen ändern.

**Voraussetzungen**

Sie müssen das UPDATE-Privileg für die zu ändernden Spalten haben. Bei SQL Anywhere- und UltraLite-Datenbanken darf die Tabellenbearbeitung nicht deaktiviert sein.

**Kontext und Bemerkungen**

Beim Bearbeiten einer Ergebnismenge können Sie jeweils nur Änderungen an den Werten in einer Zeile vornehmen.

**Aufgabe**

1. Führen Sie eine Abfrage in Interactive SQL aus.
2. Auf der Registerkarte **Ergebnisse** klicken Sie auf den Wert, den Sie ändern möchten.
3. Rechtsklicken Sie auf den Wert und klicken Sie auf **Zeile bearbeiten** oder drücken Sie F2.

In der Tabellenzelle, in der sich der Wert befindet, erscheint die Schaltfläche ...

4. Klicken Sie auf ... und wählen Sie eine der folgenden Optionen:
  - **In Fenster bearbeiten** Öffnet ein Fenster, in dem Sie einen neuen Wert eingeben können (nur Zeichendatenfelder).
  - **Auf NULL setzen** Wenn die Spalte nicht nullwertfähig ist, wird diese Menüoption nicht angezeigt.
  - **Auf DEFAULT setzen** Dieses Menüelement erscheint, wenn einer Tabelle eine neue Zeile hinzugefügt wird, vorausgesetzt für die Spalte ist ein Standardwert definiert.
  - **Aus Datei laden** Sie können nach einer Datei suchen und den Inhalt der Zelle aus der Datei laden.

Geben Sie den neuen Wert ein. Wenn Sie andere Werte in der Zeile ändern möchten, drücken Sie die Tabulatortaste oder die Kombination Umschalt+Tabulator, um zu den anderen Werten zu springen.

5. Wenn Sie die Bearbeitung der Werte in der Zeile abgeschlossen haben, drücken Sie die Eingabetaste, um die Datenbank zu aktualisieren.

Sie können Esc drücken, um die am ausgewählten Wert vorgenommene Änderung abzubrechen.

6. Führen Sie eine COMMIT-Anweisung aus, um die Änderungen an der Tabelle permanent zu speichern.

### Ergebnisse

Die Zeile in der Ergebnismenge wird bearbeitet.

### Siehe auch

- „Konfiguration der Administrationstools“ [[SQL Anywhere Server - Programmierung](#)]

## Tabellenbearbeitung in Interactive SQL deaktivieren

Sie können die Tabellenbearbeitung über das Fenster **Optionen** in Interactive SQL deaktivieren. Beim Deployment von Interactive SQL können Sie ebenfalls die Tabellenbearbeitung deaktivieren.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Klicken Sie auf **Extras » Optionen** und anschließend entweder auf **SQL Anywhere** oder auf **UltraLite**.
2. Vergewissern Sie sich, dass **Abrollbare Tabelle** ausgewählt ist, und klicken Sie auf **Bearbeitung deaktivieren**.
3. Klicken Sie auf **OK**.
4. Führen Sie eine Abfrage aus.

Sie müssen eine neue Abfrage ausführen, damit die Änderungen der Tabellenbearbeitung wirksam werden.

### Ergebnisse

Die Tabellenbearbeitung wird deaktiviert.

## Neue Zeilen in Interactive SQL-Ergebnismengen einfügen

Interactive SQL ermöglicht das Hinzufügen neuer Zeilen in eine Tabelle. Mit der Tabulatortaste können Sie in der Ergebnismenge von einer Spalte zur anderen springen, um Werte in die Zeile einzufügen.

### Voraussetzungen

Um neue Zeilen hinzuzufügen, müssen Sie das INSERT-Privileg für die Tabelle haben.

Sie müssen eine Abfrage ausgeführt haben, um eine Ergebnismenge zu erhalten.

## Kontext und Bemerkungen

Sie können in eine Spalte keine ungültigen Datentypen eingeben. Beispielsweise können Sie in eine Spalte, die nur den Datentyp INT zulässt, keine Zeichenfolge eingeben.

## Aufgabe

1. Rechtsklicken Sie in Interactive SQL auf die Ergebnismenge und klicken Sie auf **Zeile hinzufügen**.

Eine neue leere Zeile wird angezeigt, wobei der Cursor im ersten Wert der Zeile blinkt.

2. Geben Sie den neuen Wert ein und drücken Sie die Tabulatortaste, um in die nächste Spalte zu springen.

Option	Aktion
Werte in Spalten mit Standardwerten einfügen	Beim Hinzufügen eines Werts in einer Spalte mit Standardwert enthält der Zelleneditor eine Liste mit dem Eintrag <b>(Standard)</b> . Klicken Sie auf <b>(Standard)</b> , wenn Sie den Standardwert einfügen möchten. Auf gleiche Weise wird <b>(NULL)</b> angezeigt, wenn eine Spalte NULL akzeptiert. Wenn eine Spalte nicht NULL sein kann und keinen Standardwert hat, müssen Sie einen Wert eingeben.
Werte in berechnete Spalten einfügen	Wenn die Ergebnismenge eine berechnete Spalte enthält und Sie keinen Wert für die berechnete Spalte eingeben, wird der Wert beim Aktualisieren der Datenbank berechnet. Wenn Sie jedoch einen Wert für die berechnete Spalte angeben, wird die Datenbank mit dem angegebenen Wert aktualisiert, und es wird kein Wert für die berechnete Spalte errechnet.

Wiederholen Sie diesen Schritt, bis Sie alle Spaltenwerte hinzugefügt haben.

3. Drücken Sie Eingabe, um die Datenbank zu aktualisieren.
4. Führen Sie eine COMMIT-Anweisung aus, um die Änderungen an der Datenbank permanent zu speichern.

## Ergebnisse

Sie haben eine neue Zeile in die Datenbank eingefügt.

## Siehe auch

- „INPUT-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „input\_format-Option [Interactive SQL]“ auf Seite 857

## Zeilen aus Interactive SQL-Ergebnismengen löschen

Sie können eine Zeile aus einer Ergebnismenge in Interactive SQL löschen.

## Voraussetzungen

Um Zeilen zu löschen, müssen Sie das DELETE-Privileg für die Tabelle haben.

Sie müssen eine Abfrage ausgeführt haben, um eine Ergebnismenge zu erhalten.

## Aufgabe

1. Wählen Sie in Interactive SQL die zu löschende(n) Zeile(n) aus. So markieren Sie eine bzw. mehrere Zeilen:

- Klicken Sie auf die Zeilen, während Sie die Umschalttaste drücken.
- Markieren Sie die Zeilen mit den Auf- und Abpfeilen, während Sie die Umschalttaste drücken.

Wenn Sie nicht aufeinanderfolgende Zeilen löschen möchten, müssen Sie jede Zeile einzeln löschen.

2. Drücken Sie auf "Entfernen".

Die ausgewählte(n) Zeile(n) werden aus der Datenbanktabelle entfernt.

3. Führen Sie ein COMMIT aus, um die Änderungen permanent zu speichern.

## Ergebnisse

Die Zeile wird aus der Ergebnismenge gelöscht.

## Spalten, Zeilen und Zellen aus Interactive SQL-Ergebnismengen kopieren

Sie können Zellen, Zeilen und Spalten direkt aus der Ergebnismenge in Interactive SQL kopieren und dann in andere Anwendungen einfügen. Durch Kopieren von Zeilen und Spalten kopieren Sie sowohl die Spaltentitel als auch die Tabellendaten in die Zwischenablage.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

Sie müssen eine Abfrage ausgeführt haben, um eine Ergebnismenge zu erhalten.

## Kontext und Bemerkungen

Die kopierten Daten werden gemäß den folgenden Interactive SQL-Optionen formatiert:

- „isql\_escape\_character-Option [Interactive SQL]“
- „isql\_field\_separator-Option [Interactive SQL]“
- „isql\_quote-Option [Interactive SQL]“

Außerdem können Sie diese Optionen in Interactive SQL ändern, indem Sie auf **Optionen » Import/Export** klicken.

Wenn diese Optionen auf ihre Standardwerte gesetzt sind, werden die kopierten Daten durch Kommata getrennt und alle Zeichenfolgen werden in Apostrophe eingeschlossen.

### Aufgabe

- Rufen Sie in Interactive SQL die Ergebnismenge ab, die Sie kopieren möchten.

Option	Aktion
Eine Zeile kopieren	Rechtsklicken Sie auf eine Zelle in der Zeile und klicken Sie auf <b>Daten kopieren » Zeilen</b> .
Mehrere Zeilen kopieren	Halten Sie die Strg-Taste gedrückt, während Sie auf Zellen in den Zeilen klicken, rechtsklicken Sie und klicken Sie dann auf <b>Daten kopieren » Zeilen</b> .  Die ausgewählten Zeilen werden einschließlich des entsprechenden Spaltentitels in die Zwischenablage kopiert.
Eine Spalte kopieren	Rechtsklicken Sie auf eine Zelle in der Spalte und klicken Sie auf <b>Daten kopieren » Spalten</b> .
Mehrere Spalten kopieren	Halten Sie die Strg-Taste gedrückt, während Sie auf Zellen in den Spalten klicken, rechtsklicken Sie und klicken Sie dann auf <b>Daten kopieren » Spalten</b> .  Wenn der Fensterausschnitt <b>Ergebnisse</b> nicht die gesamte Ergebnismenge enthält, werden Sie aufgefordert, die übrigen Ergebnisse abzurufen, bevor Sie sie auswählen. Sonst werden nur die Ergebnisse ausgewählt, die bisher abgerufen wurden.
Eine Zelle kopieren	Rechtsklicken Sie auf die Zelle, die Sie kopieren möchten, und klicken Sie auf <b>Daten kopieren » Zellen</b> .
Mehrere Zellen kopieren	Halten Sie die Strg-Taste gedrückt, während Sie auf Zellen klicken, rechtsklicken Sie und klicken Sie dann auf <b>Daten kopieren » Zellen</b> .  Bei diesem Verfahren werden nur die Daten in die Zwischenablage kopiert, keine Spaltentitel. Außerdem werden keine Apostrophe gesetzt.

### Ergebnisse

Die ausgewählten Daten werden kopiert.

### Nächste Schritte

Sie können die ausgewählten Informationen in andere Anwendungen einfügen.

## Abfrage-Editor in Interactive SQL

Der in Interactive SQL verfügbare Abfrage-Editor unterstützt Sie beim Erstellen von SELECT-Anweisungen. Sie können SQL-Abfragen im Abfrage-Editor erstellen oder Abfragen importieren und

bearbeiten. Wenn Sie Ihre Abfrage erstellt haben, klicken Sie auf **OK**, um sie zur Verarbeitung zurück in Sybase Central oder Interactive SQL zu exportieren.

### SQL-Anweisungen mit dem Abfrage-Editor verwenden

Um mit dem Abfrage-Editor Abfragen zu erstellen, brauchen Sie keine SQL-Anweisungen zu verwenden. Sie können SQL-Anweisungen jedoch auf folgende Weise im Abfrage-Editor verwenden:

- Sie können eine Abfrage in Interactive SQL im Fenster **SQL-Anweisungen** erstellen und sie in den Abfrage-Editor importieren, indem Sie den Code markieren, bevor Sie den Editor öffnen.
- Sie können im Abfrage-Editor jederzeit unten im Fenster auf **SQL** klicken, um die SQL-Anweisungen für die zu erstellende Abfrage anzuzeigen. Sie können den Code direkt bearbeiten, und die Felder werden im Abfrage-Editor automatisch aktualisiert.

### Abfrage-Editor konfigurieren

Sie können den Abfrage-Editor aus Interactive SQL oder Sybase Central so konfigurieren, dass die SQL-Anweisungen vollständig ausgeschrieben sind, d.h., dass alle Tabellen- und Spaltennamen vollständig qualifiziert und Namen in Anführungszeichen gesetzt werden. Diese zusätzliche Formatierung ist gewöhnlich nicht erforderlich, doch sie stellt sicher, dass die SQL-Anweisungen in allen Situationen einwandfrei arbeiten. Sie können auch festlegen, dass beim Start eine Liste mit Tabellen abgerufen wird.

Um den Abfrage-Editor in Interactive SQL zu konfigurieren, klicken Sie auf **Extras » Optionen » SQL Anywhere** und anschließend auf die Registerkarte **Abfrage-Editor**.

### Abfrage-Editor-Registerkarten

Der Abfrage-Editor verfügt über eine Reihe von Registerkarten, die Sie durch die Komponenten einer SQL-Abfrage führen, die zum größten Teil optional sind. Die Registerkarten werden in der Reihenfolge angezeigt, in der SQL-Abfragen gewöhnlich erstellt werden:

Tabulatortaste	Beschreibung
Registerkarte <b>Tabellen</b>	Mit dieser Registerkarte können Sie die Tabellen Ihrer Abfrage festlegen.
Registerkarte <b>Joins</b>	Mit dieser Registerkarte können Sie eine Join-Strategie zur Kombination der Daten in den Tabellen angeben, wenn Sie mehr als eine Tabelle in der Abfrage verwenden. Wenn Sie keine Join-Strategie festlegen, empfiehlt der Abfrage-Editor eine. Wenn es eine Fremdschlüsselbeziehung zwischen den Tabellen gibt, generiert er eine Join-Bedingung basierend auf dieser Beziehung oder empfiehlt ein Kreuzprodukt. Wenn Sie Abfragen öffnen, akzeptiert der Abfrage-Editor genau die Join-Strategie, die Sie angegeben haben (und ein nicht spezifizierter JOIN wird nicht standardmäßig als Key-Join interpretiert, so wie es sonst in SQL Anywhere üblich ist).
Registerkarte <b>Spalten</b>	Mit dieser Registerkarte können Sie die Spalten in Ihrer Ergebnismenge festlegen. Wenn Sie keine Spalten angeben, werden alle Spalten angezeigt.
Registerkarte <b>INTO</b>	Mit dieser Registerkarte können Sie Variablen Ergebnisse zuweisen.

Tabulatortaste	Beschreibung
Registerkarte <b>WHERE</b>	Mit dieser Registerkarte können Sie Bedingungen zur Begrenzung der Zeilen in Ihrer Ergebnismenge festlegen.
Registerkarte <b>GROUP BY</b>	Mit dieser Registerkarte können Sie die Zeilen in Ihrer Ergebnismenge gruppieren.
Registerkarte <b>HAVING</b>	Mit dieser Registerkarte können Sie die Zeilen in Ihrer Ergebnismenge basierend auf Gruppenwerten begrenzen.
Registerkarte <b>ORDER BY</b>	Mit dieser Registerkarte können Sie die Zeilen sortieren.

### Abfrage-Editor-Tools

Der Abfrage-Editor enthält außerdem die folgenden Tools:

Fenster	Beschreibung
Ausdruck-Editor	Mit dem Ausdruck-Editor können Sie Suchbedingungen erstellen oder berechnete Spalten festlegen. Siehe „ <a href="#">Ausdruck-Editor in Interactive SQL</a> “ auf Seite 838.
<b>Abgeleitete Tabelle</b>	Mit diesem Fenster, das nahezu identisch mit dem Hauptfenster des Abfrage-Editors ist, können Sie abgeleitete Tabellen und Unterabfragen erstellen.

Jede Komponente des Abfrage-Editors verfügt über eine kontextsensitive Online-Hilfe, in der die Verwendung der Registerkarten beschrieben wird und die Links zur SQL Anywhere-Dokumentation enthält, wo relevante Konzepte und Syntax erläutert werden.

### Einschränkungen des Abfrage-Editors

Der Abfrage-Editor erstellt SQL Anywhere SELECT-Anweisungen. Er dient nicht zur Erstellung von Ansichten, wenngleich Sie sie in Interactive SQL erstellen und dann im Abfrage-Editor referenzieren können. Auch können damit keine UPDATE-Anweisungen oder andere Anweisungen erstellt werden, bei denen es sich nicht um SQL-SELECT-Anweisungen handelt. Der Editor erstellt eine einzelne SELECT-Anweisung, sodass er keine Unions oder Intersects von SELECT-Anweisungen aufbaut. Der Abfrage-Editor unterstützt außerdem keine Transact-SQL-Syntax.

### Siehe auch

- „Abfragen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SELECT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

### Abfragen mit dem Abfrage-Editor erstellen

Sie können den Abfrage-Editor in Interactive SQL zum Aufbauen von SELECT-Anweisungen verwenden. Sie können SQL-Abfragen im Abfrage-Editor erstellen oder Abfragen importieren und bearbeiten.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Aufgabe

1. Stellen Sie eine Verbindung zu einer Datenbank in Interactive SQL her.
2. Öffnen Sie den Abfrage-Editor.

Klicken Sie auf **Extras » Abfrage bearbeiten**.

Wenn Sie in Interactive SQL eine SQL-Anweisung ausgewählt haben, wird die gewählte Anweisung automatisch in den Abfrage-Editor importiert.

3. Erstellen Sie Ihre Abfrage.

Sie können im Abfrage-Editor jederzeit unten im Fenster auf **SQL** klicken, um die SQL-Anweisung für die zu erstellende Abfrage anzuzeigen. Sie können den Code direkt bearbeiten. Die Felder werden im Fenster des Abfrage-Editors automatisch aktualisiert.

4. Klicken Sie auf **OK**, um die Abfrage in den Fensterausschnitt **SQL-Anweisungen** zu schreiben.

## Ergebnisse

Eine Abfrage wird mit dem Abfrage-Editor erstellt und zur Verarbeitung in Interactive SQL exportiert.

## Ausdruck-Editor in Interactive SQL

Der Ausdruck-Editor unterstützt Sie bei der Erstellung von Suchbedingungen, berechneten Spalten und Unterabfragen. Um vorhandene Ausdrücke zu bearbeiten, markieren Sie den Ausdruck, bevor Sie den Ausdruck-Editor öffnen. Andernfalls wird alles, was Sie im Ausdruck-Editor erstellen, an vorher vorhandene Ausdrücke angehängt, wenn Sie auf **OK** klicken.

## Komponenten

- **Ausdruck** Hier erstellen Sie Ihren Ausdruck.
- **Spalten** Dieses Feld listet die Spalten auf, die in Ihrer Abfrage enthalten sind. Um eine Spalte in Ihren Ausdruck einzufügen, doppelklicken Sie darauf oder geben sie direkt in den Fensterausschnitt **Ausdruck** ein.
- **Funktionen** Funktionen sind vordefinierte Ausdrücke, die zur Rückgabe von Informationen aus der Datenbank verwendet werden. Um eine Funktion in einen Ausdruck einzufügen, wählen Sie ihn auf der Dropdown-Liste aus. Siehe „SQL-Funktionen“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- **Gespeicherte Prozeduren** Dieses Feld listet die gespeicherten Prozeduren auf, die Sie verwenden können.

- **Numerisches Tastenfeld** Das numerische Tastenfeld befindet sich unten links im Fenster. Klicken Sie auf eine Zahl, um sie in den Ausdruck einzufügen. Sie können die Zahlen auch über Ihre Tastatur eingeben.
- **Vergleichsoperatoren** Die arithmetischen Symbole, wie z.B. "=", erscheinen in der Mitte des unteren Bereichs des Fensters. Um ein Symbol in den Ausdruck einzufügen, klicken Sie darauf. Hier werden nur einige häufig verwendete Operatoren angezeigt, doch Sie können weitere Operatoren über die Tastatur eingeben. Siehe „[Vergleichsoperatoren](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- **Logische Operatoren** Logische Operatoren, wie z.B. AND, erscheinen unten rechts im Fenster. Um einen Operator in den Ausdruck einzufügen, klicken Sie darauf. Diese Gruppe ist eine Teilmenge häufig verwendeter logischer Operatoren. Sie können beliebige logische Operatoren über die Tastatur eingeben. Siehe „[Logische Operatoren](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].
- **Unterabfrage bearbeiten und Ergebnisse in den Editor einfügen (Schaltfläche)** Diese Schaltfläche befindet sich bei den logischen Operatoren. Wenn Sie darauf klicken, erscheint ein Fenster, das Sie bei der Erstellung von Unterabfragen anleitet.

### Unterabfrage hinzufügen

Um eine Unterabfrage zu erstellen, öffnen Sie den Ausdrucks-Editor und klicken auf die Schaltfläche **Unterabfrage bearbeiten und Ergebnisse in den Editor einfügen** (neben der Schaltfläche **NOT**). Dies öffnet das Fenster **Unterabfrage**, das so ähnlich aussieht wie das Hauptfenster des Abfrage-Editors, mit dem einzigen Unterschied, dass in der Titelleiste **Unterabfrage** angezeigt wird. Sie erstellen eine Unterabfrage auf die gleiche Art wie eine Hauptabfrage.

### Siehe auch

- „[Abfrage-Editor in Interactive SQL](#)“ auf Seite 835
- „[Suchbedingungen](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „[Unterabfragen in Suchbedingungen](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Grafische Pläne mit detaillierten und Knotenstatistiken erstellen

Die Plananzeige ist ein grafisches Tool zum Anzeigen von grafischen Plänen für SQL Anywhere-Datenbanken und Textplänen für UltraLite-Datenbanken.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Starten Sie Interactive SQL und stellen Sie eine Verbindung mit der Datenbank her.
2. Klicken Sie auf **Extras » Plananzeige** oder drücken Sie Umschalttaste+F5.

Die Plananzeige erscheint in einem separaten Fenster. Das Plananzeige-Fenster ist in folgende Fensterausschnitte aufgeteilt:

- **SQL-Fensterausschnitt** In diesem Fensterausschnitt können Sie SQL-Anweisungen eingeben, für die Pläne erstellt werden sollen.
  - **Ergebnisfenster** Dieser Fensterausschnitt zeigt den grafischen Plan und wird nur für SQL Anywhere-Datenbanken verwendet.
  - **Fensterausschnitt "Details"** Dieser Fensterausschnitt zeigt bei SQL Anywhere-Datenbanken Textdetails zum Plan. Bei UltraLite-Datenbanken zeigt dieser Fensterausschnitt den Textplan.
3. Geben Sie eine Anweisung in den Fensterausschnitt **SQL** ein.
  4. Klicken Sie in der Liste **Statistikebene** auf **Detaillierte und Knotenstatistiken**.
  5. Klicken Sie auf **Plan abrufen**, um einen Plan für die angegebene Abfrage zu generieren.
  6. Klicken Sie auf **Speichern unter**.
  7. Legen Sie fest, wo der Plan gespeichert werden soll, und geben Sie einen Dateinamen ein. Klicken Sie auf **Speichern**.

### Ergebnisse

Ein grafischer Plan mit **detaillierten und Knotenstatistiken** wird erstellt.

### Nächste Schritte

Öffnen Sie den grafischen Plan, indem Sie auf **Extras » Plananzeige** klicken. Klicken Sie auf **Öffnen**. Wählen Sie eine Plandatei (*.saplan*) und klicken Sie auf **Öffnen**.

### Siehe auch

- „Grafische Pläne“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Einen Ausführungsplan anzeigen“ [[UltraLite - Datenbankverwaltung](#)]
- „Anzeigen eines grafischen Plans“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Grafische Pläne anpassen

Nachdem Sie einen grafischen Plan erstellt haben, können Sie das Erscheinungsbild der Elemente im Plan anpassen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Öffnen Sie die Plananzeige. Klicken Sie in Interactive SQL auf **Extras » Plananzeige**.
2. Öffnen Sie einen Plan. Rechtsklicken Sie im linken unteren Ausschnitt der Plananzeige auf den Plan und klicken Sie auf **Anpassen**.

3. Ändern Sie die Einstellungen.
4. Klicken Sie auf **OK**, wenn Sie fertig sind.
5. Klicken Sie auf **Plan abrufen**.

### Ergebnisse

Der angepasste grafische Plan wird erstellt.

## Bilder und SVGs in Interactive SQL anzeigen

Mit Interactive SQL können Sie BLOB-Daten sowie Bilder mit weniger als 5000000 Pixeln anzeigen. Außerdem können Sie SVGs anzeigen und in anderen Formaten speichern.

### Voraussetzungen

Sie müssen die zum Ausführen der Abfrage notwendigen Privilegien haben.

Ihr Bild muss in einem der folgenden Formate vorliegen: BMP (Windows 95-Version), GIF, JPG, PNG, SVG, oder WBMP (Wireless Bitmap).

### Aufgabe

1. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her.
2. Führen Sie eine Abfrage aus, die eine Ergebnismenge mit einem Bild zurückgibt.
3. Klicken Sie in der Ergebnismenge in eine Zelle, die **(BILD)** enthält, klicken Sie auf ... und anschließend auf **In Fenster anzeigen**.

Das Fenster **Wert von Spalte *Spaltenname*** erscheint.

Beim Anzeigen von SVGs können Sie folgende Tastenkürzel verwenden:

Tastenkürzel	Beschreibung
STRG+Linke Maustaste, ziehen	Zieht eine Begrenzung, sodass Sie die Perspektive einstellen können.
STRG+Rechte Maustaste, ziehen	Dreht das Bild um seine Mitte.
Umschalt+Linke Maustaste, ziehen	Verschiebt das Bild an einen neuen Ort.
Umschalt+Rechte Maustaste, ziehen	Vergrößert bzw. verkleinert die Bildanzeige.

4. Klicken Sie auf **OK**, um das Fenster zu schließen.

## Ergebnisse

Das Bild wird angezeigt.

## Beispiel

Stellen Sie eine Verbindung mit der Beispieldatenbank her und führen Sie die folgende Anweisung aus, um JPEG-Bilder zurückzugeben:

```
SELECT * FROM GROUPO.Products;
```

Das folgende Fenster wird angezeigt, wenn Sie auf das JPEG-Bild klicken, das der Baumwollkappe zugeordnet ist:



Stellen Sie eine Verbindung mit der Beispieldatenbank her und führen Sie die folgende Anweisung aus, um ein SVG-Bild zurückzugeben:

```
SELECT '<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">

<svg width="100%" height="100%" version="1.1"
xmlns="http://www.w3.org/2000/svg">

<rect width="99" height="99"
```

```
style="fill:rgb(0,0,255);stroke-width:1;
stroke:rgb(0,0,0)"/>

</svg>' ;
```

### Siehe auch

- „Anzeigen von räumlichen Daten als Bilder (Interactive SQL)“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]
- „Anzeigen von räumlichen Daten als Bilder (Spatial Viewer)“ [[SQL Anywhere Server - Unterstützung für räumliche Daten](#)]

## HTML- und XML-Daten in Interactive SQL anzeigen

In Interactive SQL können Sie HTML- und XML-Daten aus der Ergebnismenge einer Abfrage in einem separaten Fenster anzeigen.

### Voraussetzungen

Sie müssen die zum Ausführen der Abfrage notwendigen Privilegien haben.

### Aufgabe

1. Stellen Sie in Interactive SQL eine Verbindung mit der Datenbank her.
2. Führen Sie eine Abfrage aus, die eine Ergebnismenge mit HTML- und XML-Daten zurückgibt.
3. Wählen Sie in den Ergebnissen eine Zelle mit HTML- oder XML-Inhalt aus, klicken Sie auf ... und anschließend auf **In Fenster anzeigen**.

### Ergebnisse

Das Fenster **Wert von Spalte Spaltenname** erscheint.

### Nächste Schritte

Klicken Sie auf **OK**, um das Fenster zu schließen.

### Beispiel

Führen Sie die folgende Abfrage aus, um eine Beispiel-Ergebnismenge mit HTML-Daten anzuzeigen:

```
SELECT '<html>
<head>
  <meta http-equiv=Content-Type content="text/html; charset=windows-1252">
  <title>Tee Shirt</title>
</head>
<body lang=EN-US>
  <p>
    <span style=font-size:10.0pt;font-family:Arial>
      We have improved the design of this perennial favorite.
      A sleek and technical shirt built for the trail, track, or
      sidewalk. UPF rating of 50+.
    </span>
```

```
</p>
</body>
</html>' ;
```

Führen Sie die folgende Abfrage aus, um eine Beispiel-Ergebnismenge mit einem wohlgeformten XML-Dokument anzuzeigen:

```
SELECT '<?xml version="1.0" encoding="UTF-8"?>
<parent>
  <children>
    <child name="Tim" />
    <child name="Katie" />
  </children>
</parent>';
```

## Header im Fensterausschnitt SQL-Anweisungen hinzufügen

Sie können einen Header oder eine Fußzeile zum Inhalt des Fensterausschnitts **SQL-Anweisungen** hinzufügen und andere Formatierungsoptionen im Interactive SQL-Fenster **Optionen** konfigurieren.

### Voraussetzungen

Sie müssen eine Abfrage ausgeführt haben, damit Inhalt im Fensterausschnitt **SQL-Anweisungen** vorhanden ist.

### Aufgabe

1. Klicken Sie in Interactive SQL auf **Extras » Optionen**.
2. Klicken Sie im linken Fensterausschnitt auf die Registerkarte **Editor**. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Drucken**.
3. Im Feld **Kopfzeile** geben Sie den Text für die Kopfzeile ein. Sie können auch auf den Pfeil rechts daneben klicken und Elemente zum Einfügen in die Kopfzeile auswählen.

### Ergebnisse

Ein Header wird zum Text hinzugefügt.

## Öffnen mehrerer Interactive SQL-Fenster

Sie können mehrere Interactive SQL-Fenster öffnen, die jeweils einer eigenen Datenbankverbindung entsprechen. Sie können sich gleichzeitig mit zwei (oder mehr) verschiedenen Datenbanken auf unterschiedlichen Datenbankservern verbinden oder mehrere parallele Verbindungen zu einer einzelnen Datenbank aufbauen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Aufgabe

1. Klicken Sie in Interactive SQL auf **Fenster » Neues Fenster**.

### Tipp

Wenn die SQLCONNECT-Umgebungsvariable gesetzt ist oder Sie bereits eine Verbindung mit einer SQL Anywhere-Datenbank hergestellt haben, versucht der Datenbankserver, diese Informationen für die Verbindung mit einer Datenbank zu verwenden, bevor Sie aufgefordert werden, Informationen einzugeben. Ebenso gilt: Wenn die SQLCONNECT-Umgebungsvariable gesetzt ist oder Sie bereits eine Verbindung mit einer UltraLite-Datenbank hergestellt haben, versucht der Datenbankserver, diese Informationen für die Verbindung mit einer Datenbank zu verwenden, bevor Sie aufgefordert werden, Informationen einzugeben. Wenn diese Versuche fehlschlagen oder Sie nicht bereits mit der Datenbank verbunden sind, wird das Fenster **Verbinden** angezeigt.

2. Im Fenster **Verbinden** geben Sie die Verbindungsinformationen für Ihre Datenbank ein und klicken auf **Verbinden**.

Sie können eine Verbindung mit einer Datenbank auch herstellen oder trennen, indem Sie auf **SQL » Verbinden** bzw. **SQL » Trennen** klicken.

## Ergebnisse

Die Verbindungsinformationen (einschließlich Datenbankname, Benutzer-ID und Name des Datenbankservers) werden in der Interactive SQL-Titelleiste angezeigt.

## Siehe auch

- „SQLCONNECT-Umgebungsvariable“ auf Seite 479
- „UltraLite-Verbindungsparameter und die Umgebungsvariable ULSQLCONNECT“ [*UltraLite - Datenbankverwaltung*]
- „CONNECT-Anweisung [ESQL] [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DISCONNECT-Anweisung [ESQL] [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Tastenkürzel für Interactive SQL

In Interactive SQL gibt es die folgenden Tastenkürzel:

Taste(n)	Beschreibung
Alt+F4	Beendet Interactive SQL.
Alt+Pfeil nach links  Unter Mac OS X verwenden Sie Steuerungsbefehl +Pfeil nach links.	Zeigt die vorherige SQL-Anweisung der Verlaufsliste an.

<b>Taste(n)</b>	<b>Beschreibung</b>
Alt+Pfeil nach rechts  Unter Mac OS X verwenden Sie Steuerungsbefehl +Pfeil nach rechts.	Zeigt die nächste SQL-Anweisung der Verlaufsliste an.
Strg+Rückschritt	Löscht das Wort links vom Cursor
Strg+Untbr	Unterbricht die SQL-Anweisung, die gerade ausgeführt wird. Dieses Tastenkürzel wird nur unter Windows-Betriebssystemen unterstützt.
Strg+A	Markiert den gesamten Text im aktiven Fensterausschnitt  Wenn es sich bei den Ergebnissen im Fensterausschnitt <b>Ergebnisse</b> nicht um die gesamte Ergebnismenge handelt, werden Sie aufgefordert, die verbleibenden Zeilen abzurufen. Andernfalls werden die aktuell abgerufenen Ergebnisse ausgewählt. Siehe „ <a href="#">Spalten, Zeilen und Zellen aus Inter-active SQL-Ergebnismengen kopieren</a> “ auf Seite 834.
Strg+C	Kopiert im Fensterausschnitt <b>Ergebnisse</b> die markierten Zeilen und Spalten in die Zwischenablage.  Kopiert im Fensterausschnitt <b>SQL-Anweisungen</b> den markierten Text in die Zwischenablage.
Strg+Umschalttaste+C	Führt eine Festschreibe-Anweisung aus.  <b>Hinweis</b> Durch das Ausführen einer COMMIT-Anweisung über das Menü <b>SQL</b> oder ein Tastenkürzel wird der Inhalt des Fensterausschnitts <b>SQL-Anweisungen</b> nicht geändert. Der Inhalt der Registerkarte <b>Ergebnisse</b> im Fensterausschnitt <b>Ergebnisse</b> wird jedoch gelöscht.
Strg+Entf	Löscht das Wort rechts vom Cursor
Strg+Ende	Verschiebt den Cursor zum Anfang der aktuellen Seite.
Strg+F	Öffnet das Fenster <b>Suchen/Ersetzen</b> .
Strg+Umschalttaste+F10	Zeigt ein Einblendmenü für eine Zelle an, die den Fokus auf einer Ergebnismenge auf der Registerkarte <b>Ergebnisse</b> hat.  Dieses Tastenkürzel ist eine Alternative zum Klicken auf ... in einer Tabellenzelle.

<b>Taste(n)</b>	<b>Beschreibung</b>
Strg+G	Bewegt den Cursor zur angegebenen Zeile im Ausschnitt <b>SQL-Anweisungen</b> .
Strg+H  Unter Mac OS X verwenden Sie Steuerungsbefehl +H.	Zeigt den Verlauf der ausgeführten SQL-Anweisungen an.
Strg+Pos1	Verschiebt den Cursor zum Anfang des aktuellen Fensterausschnitts.
Strg+L	Löscht die aktuelle Zeile aus dem Fensterausschnitt <b>SQL-Anweisungen</b> und speichert sie in der Zwischenablage.
Strg+Umschalt+L	Löscht die aktuelle Zeile
Strg+N	Löscht den Inhalt des Interactive SQL-Fensters und schließt die aktuelle Datei (falls vorhanden)
Strg+O	Öffnet eine Datei
Strg+P	Druckt den Inhalt des Fensterausschnitts <b>SQL-Anweisungen</b> . Klicken Sie alternativ auf <b>Extras » Optionen » Editor » Drucken</b> .
Strg+Q	Öffnet den Abfrage-Editor.  Mit dem Abfrage-Editor können Sie SQL-Abfragen erstellen. Wenn Sie die Abfrage erstellt haben, klicken Sie auf <b>OK</b> , um sie in den Fensterausschnitt <b>SQL-Anweisungen</b> einzufügen.
Strg+Umschalttaste+R	Führt eine Zurücksetzungsanweisung aus.  <div> <b>Hinweis</b>  Durch das Ausführen einer ROLLBACK-Anweisung über das Menü <b>SQL</b> oder ein Tastenkürzel wird der Inhalt des Fensterausschnitts <b>SQL-Anweisungen</b> nicht geändert. Der Inhalt der Registerkarte <b>Ergebnisse</b> im Fensterausschnitt <b>Ergebnisse</b> wird jedoch gelöscht. </div>
Strg+S	Speichert den Inhalt des Fensterausschnitts <b>SQL-Anweisungen</b> in der angegebenen Datei.
Strg+U	Ändert den markierten Text auf Kleinbuchstaben
Strg+Umschalt+U	Ändert den markierten Text auf Großbuchstaben
Strg+V	Fügt den markierten Text ein

Taste(n)	Beschreibung
Strg+X	Schneidet den markierten Text aus
Strg+Y	Wiederholt den letzten Vorgang
Strg+Z	Setzt den letzten Vorgang zurück
Strg+]	Verschiebt den Cursor zur schließenden Klammer. Verwenden Sie dieses Tastenkürzel, um nach übereinstimmenden runden, geschweiften, eckigen und spitzen Klammern zu suchen.
Strg+Umschalt+]	Erweitert die Markierung bis zur schließenden Klammer. Verwenden Sie dieses Tastenkürzel, um nach übereinstimmenden runden, geschweiften, eckigen und spitzen Klammern zu suchen.
Strg+Minuszeichen (-)	<p>Fügt den Doppel-Bindestrich (--) als SQL-Kommentarindikator hinzu oder entfernt ihn.</p> <p>Um vorhandenen Text in Kommentar zu verwandeln, wählen Sie den Text im Fensterausschnitt <b>SQL-Anweisungen</b> aus und drücken Strg+Minuszeichen. Das SQL-Kommentarzeichen wird am Anfang jeder Zeile des ausgewählten Textes eingefügt.</p> <p>Wenn kein Text ausgewählt wurde, wird der Kommentarindikator am Anfang der aktuellen Zeile eingefügt.</p> <p>Um einen Kommentarindikator zu entfernen, wählen Sie den Text aus und drücken dann STRG+Minuszeichen.</p> <p>Siehe „Kommentare“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>
Strg+Schrägstrich (/)	<p>Fügt den Doppel-Schrägstrich (//) als SQL-Kommentarindikator hinzu oder entfernt ihn.</p> <p>Um vorhandenen Text in Kommentar zu verwandeln, wählen Sie den Text im Fensterausschnitt <b>SQL-Anweisungen</b> aus und drücken STRG+Schrägstrich. Das SQL-Kommentarzeichen wird am Anfang jeder Zeile des ausgewählten Textes eingefügt.</p> <p>Wenn kein Text ausgewählt wurde, wird der Kommentarindikator am Anfang der aktuellen Zeile eingefügt.</p> <p>Um einen Kommentarindikator zu entfernen, wählen Sie den Text aus und drücken dann STRG+Schrägstrich.</p> <p>Siehe „Kommentare“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>

<b>Taste(n)</b>	<b>Beschreibung</b>
Strg+Pfeil nach oben	Wählt die SQLAnweisung vor der Anweisung aus, in der sich im Ausschnitt <b>SQL-Anweisungen</b> der Cursor befindet.
Strg+Pfeil nach unten	Wählt die SQLAnweisung nach der Anweisung aus, in der sich im Ausschnitt <b>SQL-Anweisungen</b> der Cursor befindet.
Strg+Punkt(.)	Wählt die gesamte SQL-Anweisung aus, in der sich im Fensterausschnitt <b>SQL-Anweisungen</b> der Cursor befindet. Alternativ können Sie auf eine Zeile doppelklicken, um die gesamte SQL-Anweisung auszuwählen.
Strg+Komma (,)	Wählt die Zeile aus, in der sich im Ausschnitt <b>SQL-Anweisungen</b> der Cursor befindet.
Strg+Umschalt+Punkt (.)	Erweitert den Zeileneinzug des im Fensterausschnitt <b>SQL-Anweisungen</b> ausgewählten Textes.  Wenn kein Text ausgewählt wurde, wird der Einzug auf die aktuelle Zeile angewendet.
Strg+Umschalt+Komma (,)	Verringert den Zeileneinzug des im Fensterausschnitt <b>SQL-Anweisungen</b> ausgewählten Textes.  Wenn kein Text ausgewählt wurde, wird der Einzug auf die aktuelle Zeile angewendet.
Esc	Standardmäßig hat die Betätigung der Esc-Taste keine Wirkung.  Sie können aber die Esc-Taste mit dem Löschen des Fensterausschnitts <b>SQL-Anweisungen</b> und dem Schließen geöffneter Ergebnismengen belegen. Klicken Sie auf <b>Extras » Optionen » Kompatibilität</b> und anschließend auf <b>Durch Drücken der Escape-Taste werden die SQL-Anweisungen gelöscht und Ergebnismengen geschlossen</b> .
F1	Öffnet die Online-Hilfe.
F2	Bearbeitet den markierten Wert in der Ergebnismenge. Sie können mit der Tabulatortaste innerhalb der Zeile von einer Spalte zur anderen springen.
F3	Sucht das nächste Vorkommen des angegebenen Textes
Umschalt+F3	Sucht das vorherige Vorkommen des markierten Textes

Taste(n)	Beschreibung
F5	<p>Führt den gesamten, im Fenster <b>SQL-Anweisungen</b> enthaltenen Text aus.</p> <p>Sie können diesen Vorgang auch ausführen, indem Sie in der Symbolleiste auf <b>Alle SQL-Anweisungen ausführen</b> klicken oder indem Sie auf <b>SQL » Ausführen</b> klicken.</p>
Umschalt+F5	<p>Öffnet die Plananzeige für die angegebene Anweisungen im Ausschnitt <b>SQL-Anweisungen</b>. Die angegebene Anweisung wird nicht ausgeführt. Um die Anweisung in der Plananzeige auszuführen, klicken Sie auf <b>Plan abrufen</b>.</p>
F6	<p>Wechselt den Fokus vom Fensterausschnitt <b>SQL-Anweisungen</b> zum Fensterausschnitt <b>Ergebnisse</b> und umgekehrt. Wenn der Fensterausschnitt <b>Favoriten</b> geöffnet wird, wechselt der Fokus zwischen den Fensterausschnitten <b>SQL-Anweisungen</b>, <b>Ergebnisse</b> und <b>Favoriten</b>.</p>
F7	<p>Zeigt das Fenster <b>Tabellennamen nachschlagen</b> an.</p> <p>Mit diesem Fenster können Sie eine Tabelle suchen und auswählen. Wenn Sie dann die Eingabetaste drücken, wird der Tabellename im Fenster <b>SQL-Anweisungen</b> an der Cursorposition eingefügt. Drücken Sie bei markierter Tabelle auf F7, um die Spalten dieser Tabelle anzuzeigen. Sie können danach eine Spalte auswählen. Wenn Sie eine Spalte ausgewählt haben und die Eingabetaste drücken, wird der Spaltenname im Fenster <b>SQL-Anweisungen</b> an der Cursorposition eingefügt.</p>
F8	<p>Zeigt das Fenster <b>Prozedurnamen nachschlagen</b> an.</p> <p>Mit diesem Fenster können Sie eine Prozedur suchen und auswählen. Wenn Sie dann die Eingabetaste drücken, wird der Prozedurname im Fenster <b>SQL-Anweisungen</b> an der Cursorposition eingefügt.</p>
F9	<p>Führt den gesamten, im Fenster <b>SQL-Anweisungen</b> markierten Text aus.</p> <p>Wenn kein Text markiert wurde, wird der gesamte im Fenster enthaltene Text ausgeführt.</p> <p>Sie können diesen Vorgang auch ausführen, indem Sie in der Symbolleiste auf <b>Markierte Anweisungen ausführen</b> klicken oder indem Sie auf <b>SQL » Ausführen</b> klicken.</p>
Umschalt+F9	<p>Führt die ausgewählte SQL-Anweisung aus und wählt dann die nächste Anweisung aus. Mit diesem Tastenkürzel können Sie schrittweise eine Reihe von SQL-Anweisungen ausführen. Siehe „<a href="#">SQL-Anweisungen in Interactive SQL</a>“ auf Seite 819.</p>

Taste(n)	Beschreibung
Umschalt+F10	Zeigt das Kontextmenü für den aktiven Bereich an.  Dieses Tastenkürzel ist eine Alternative zum Rechtsklicken auf einen Bereich.
F11	Öffnet das Fenster <b>Verbinden</b> , wenn Interactive SQL mit keiner Datenbank verbunden ist.
F12	Trennt die Verbindung von Interactive SQL mit der aktuellen Datenbank.
Pos1	Verschiebt den Cursor an den Beginn der aktuellen Zeile oder auf das erste Wort in der aktuellen Zeile
Umschalt+Pos1	Erweitert die Markierung bis zum Textbeginn in der aktuellen Zeile
Bild-ab	Blättert im aktuellen Fenster eine Seite nach unten
Bild-auf	Blättert im aktuellen Fenster eine Seite nach oben

**Siehe auch**

- „Tastenkürzel bei der Textvervollständigung“ auf Seite 875

**Interactive SQL-Optionen**

Verwenden Sie die Anweisung SET OPTION, um die Werte der folgenden Interactive SQL-Optionen zu ändern. Siehe „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

Option	Werte	Standardwert
„auto_commit-Option [Interactive SQL]“	On, Off	Off
„auto_refetch-Option [Interactive SQL]“	On, Off	On
„bell-Option [Interactive SQL]“	On, Off	On
„command_delimiter-Option [Interactive SQL]“	Zeichenfolge	" ; "
„commit_on_exit-Option [Interactive SQL]“	On, Off	On
„default_isql_encoding-Option [Interactive SQL]“	Zeichenfolge	Leere Zeichenfolge
„echo-Option [Interactive SQL]“	On, Off	On

Option	Werte	Standardwert
„input_format-Option [Interactive SQL]“	TEXT, FIXED	TEXT
„isql_allow_read_client_file-Option [Interactive SQL]“	On, Off, Prompt	Prompt
„isql_allow_write_client_file-Option [Interactive SQL]“	On, Off, Prompt	Prompt
„isql_command_timing-Option [Interactive SQL]“	On, Off	On
„isql_escape_character-Option [Interactive SQL]“	Zeichen	" \"
„isql_field_separator-Option [Interactive SQL]“	Zeichenfolge	" , "
„isql_maximum_displayed_rows-Option [Interactive SQL]“	"All" oder eine nicht negative Ganzzahl	500
„isql_print_result_set-Option [Interactive SQL]“	Last, All, None	Last
„isql_quote-Option [Interactive SQL]“	Zeichenfolge	'
„isql_show_multiple_result_sets-Option [Interactive SQL]“	On, Off	Off
„nulls-Option [Interactive SQL]“	Zeichenfolge	"(NULL)"
„on_error-Option [Interactive SQL]“	Stop, Continue, Prompt, Exit, Notify_Continue, Notify_Stop, Notify_Exit	Prompt
„output_format-Option [Interactive SQL]“	TEXT, FIXED, HTML, SQL, XML	TEXT
„output_length-Option [Interactive SQL]“	Ganzzahl	0
„output_nulls-Option [Interactive SQL]“	Zeichenfolge	Leere Zeichenfolge
„truncation_length-Option [Interactive SQL]“	Ganzzahl	256

## auto\_commit-Option [Interactive SQL]

Steuert, ob ein COMMIT nach jeder Anweisung ausgeführt wird

### Zulässige Werte

On, Off

### Standardwert

Off

### Bemerkungen

Wenn auto\_commit auf "On" gesetzt ist, wird ein Datenbank-COMMIT nach jeder erfolgreichen Anweisung ausgeführt.

Standardmäßig wird ein COMMIT oder ROLLBACK nur ausgeführt, wenn der Benutzer eine COMMIT- oder ROLLBACK-Anweisung oder eine SQL-Anweisung verwendet, die eine automatische Festschreibung auslöst (wie die Anweisung CREATE TABLE).

#### Hinweis

In der Standardeinstellung arbeitet ODBC im Autocommit-Modus. Auch wenn Sie die auto\_commit-Option in Interactive SQL auf "Off" gesetzt haben, überschreibt die ODBC-Einstellung die Einstellungen von Interactive SQL. Sie können die ODBC-Einstellung mit dem SQL\_ATTR\_AUTOCOMMIT-Verbindungsattribut ändern. ODBC-Autocommit ist von der Option "chained" unabhängig.

### Siehe auch

- „commit\_on\_exit-Option [Interactive SQL]“ auf Seite 855
- „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „COMMIT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ROLLBACK-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Tastenkürzel für Interactive SQL“ auf Seite 845

## auto\_refetch-Option [Interactive SQL]

Steuert, ob Abfrageergebnisse nach Lösch-, Aktualisierungs- und Einfügvorgängen erneut abgerufen werden.

### Zulässige Werte

On, Off

### Standardwert

On

### Bemerkungen

Wenn auto\_refetch aktiviert ist, werden die aktuellen Abfrageergebnisse, die auf der Registerkarte **Ergebnisse** im Interactive SQL-Fensterabschnitt **Ergebnisse** angezeigt werden, von der Datenbank nach

jeder INSERT-, UPDATE- oder DELETE-Anweisung erneut abgerufen. Abhängig davon, wie kompliziert die Abfrage ist, kann dies einige Zeit dauern. Deshalb kann diese Option ausgeschaltet sein.

**Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**bell-Option [Interactive SQL]**

Steuert, ob beim Auftreten eines Fehlers ein Signalton ertönt

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bemerkungen**

Setzen Sie diese Option nach Wunsch.

**Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**command\_delimiter-Option [Interactive SQL]**

Legt die Zeichenfolge fest, die das Ende einer Anweisung in Interactive SQL anzeigt

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Semikolon ( ; )

**Bemerkungen**

Üblicherweise ist es nicht notwendig, das Befehlstrennzeichen zu ändern. Sie sollten das Semikolon belassen.

Eine Alternative zur Verwendung des Semikolons oder einer anderen Zeichenfolge als Trennzeichen für Anweisungen ist die Eingabe des Trennzeichens **go** in einer eigenen Zeile am Zeilenanfang. Siehe „Batchanweisungen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].

Die Angabe von **go** in einer eigenen Zeile am Beginn der Zeile wird immer als Befehlstrennzeichen erkannt, selbst wenn Sie die Option command\_delimiter auf einen anderen Wert setzen.

Der Wert von command\_delimiter kann eine beliebige Zeichenfolge mit den folgenden Einschränkungen sein:

- Wenn das Trennzeichen eines der folgenden Elemente enthält: & (Ampersand), \* (Stern), @ (at-Zeichen), : (Doppelpunkt), (Punkt), = (ist gleich), ( (linke Klammer), ) (rechte Klammer) oder | (senkrechter Strich), dann darf das Trennzeichen kein weiteres Zeichen enthalten. Zum Beispiel ist \* ein gültiges Trennzeichen, aber \*\* ist keines.
- Sie dürfen kein bestehendes Schlüsselwort als Befehlstrennzeichen verwenden.
- Das Befehlstrennzeichen kann eine beliebige Sequenz von Zeichen sein (einschließlich Zahlen, Buchstaben und Satzzeichen), darf aber keine eingebetteten Leerzeichen enthalten.

Wenn das Befehlstrennzeichen auf eine Zeichenfolge gesetzt ist, die mit einem Zeichen beginnt, das in Bezeichnungen gültig ist, muss dem Befehlstrennzeichen ein Leerzeichen vorangestellt werden. Das Befehlstrennzeichen berücksichtigt die Groß/Kleinschreibung. Sie müssen das neue Befehlstrennzeichen in einer SET OPTION-Anweisung in Apostrophen angeben. Wenn das Befehlstrennzeichen ein Semikolon ist (Standard), ist kein Leerzeichen vor dem Semikolon erforderlich.

### Siehe auch

- „Schlüsselwörter“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Interactive SQL-Dienstprogramm (dbisql)“ auf Seite 939
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

### Beispiele

Das folgende Beispiel setzt eine Tilde als das Befehlstrennzeichen:

```
SET OPTION command_delimiter='~';
MESSAGE 'hello'~
```

Sie können auch die Option -d von Interactive SQL verwenden, um das Befehlstrennzeichen zu setzen, ohne eine SET OPTION command\_delimiter-Anweisung in eine .sql-Datei einzufügen. Wenn Sie beispielsweise eine Skriptdatei *test.sql* benutzen, die Tilden (~) als das Befehlstrennzeichen verwendet, können Sie Folgendes ausführen:

```
dbisql -d "~" test.sql
```

### commit\_on\_exit-Option [Interactive SQL]

Steuert das Verhalten, wenn Interactive SQL getrennt wird oder herunterfährt.

#### Zulässige Werte

On, Off

#### Standardwert

On

#### Bemerkungen

Steuert, ob ein COMMIT oder ROLLBACK ausgeführt wird, wenn Sie Interactive SQL verlassen. Wenn commit\_on\_exit auf On gesetzt ist, wird ein COMMIT ausgeführt.

### Siehe auch

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ROLLBACK-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „COMMIT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Tastenkürzel für Interactive SQL“ auf Seite 845

### default\_isql\_encoding-Option [Interactive SQL]

Gibt die Kodierung an, die von READ-, INPUT- und OUTPUT-Anweisungen verwendet werden soll.

### Zulässige Werte

Bezeichner oder Zeichenfolge

### Standardwert

Systemkodierung verwenden (leere Zeichenfolge)

### Bereich

Kann nur als temporäre Option für die Dauer der aktuellen Verbindung eingestellt werden

### Bemerkungen

Diese Option wird verwendet, um die Kodierung anzugeben, die beim Lesen oder Schreiben von Dateien verwendet werden soll. Diese Option kann nicht permanent gesetzt werden: Die Standardkodierung ist die Codepage für die Plattform, die Sie verwenden. Auf Computern mit englischem Windows ist die Standard-Codepage 1252.

Wenn Interactive SQL ausgeführt wird, wird die verwendete Kodierung von der INPUT-, OUTPUT- oder READ-Anweisung in der folgenden Reihenfolge ermittelt:

- Die durch die ENCODING-Klausel festgelegte Kodierung der INPUT-, OUTPUT- oder READ-Anweisung (wenn diese Klausel angegeben wird).
- Die durch die Option default\_isql\_encoding angegebene Kodierung (sofern diese Option festgelegt wurde).
- Die Standardkodierung für die Plattform, die Sie verwenden. Auf Computern mit englischem Windows ist die Standardkodierung 1252.

Wenn die Eingabedatei mit der OUTPUT-Anweisung erstellt und eine Kodierung angegeben wurde, muss dieselbe ENCODING-Klausel in der INPUT-Anweisung angegeben werden.

Weitere Informationen zu Codepages und Zeichensätzen finden Sie unter „[Internationale Sprachen und Zeichensätze](#)“ auf Seite 491.

**Siehe auch**

- „OUTPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „READ-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „INPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Zeichensätze“ auf Seite 497
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**Beispiel**

Setzen Sie die Kodierung auf UTF-16 (zum Lesen von Unicode-Dateien):

```
SET TEMPORARY OPTION default_isql_encoding = 'UTF-16';
```

Setzen Sie die Kodierung auf cp437 I (Windows Englisch OEM):

```
SET TEMPORARY OPTION default_isql_encoding = 'cp437';
```

**echo-Option [Interactive SQL]**

Steuert, ob Anweisungen in der Logdatei erfasst werden sollen, bevor sie ausgeführt werden.

**Zulässige Werte**

On, Off

**Standardwert**

On

**Bemerkungen**

Diese Option ist besonders nützlich, wenn Sie die READ-Anweisung verwenden, um eine SQL-Skriptdatei auszuführen, oder wenn Sie eine Skriptdatei in Interactive SQL ausführen, indem Sie auf **Datei » Skript ausführen** klicken. Das Protokollieren muss aktiviert sein, damit diese Option eine Wirkung zeigt. Siehe „[START LOGGING-Anweisung \[Interactive SQL\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

**Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**input\_format-Option [Interactive SQL]**

Setzt das Standarddatenformat, das von der INPUT-Anweisung erwartet wird

**Zulässige Werte**

- **TEXT** Eingabezeilen werden als TEXT-Zeichen vorausgesetzt, eine Zeile pro Ausgabezeile, wobei die Werte durch Kommas voneinander getrennt werden. Alphabetische Zeichenfolgen können in Apostrophe oder Anführungszeichen eingeschlossen werden.

Das Standardtrennzeichen ist ein Komma (.). Zeichenfolgen, die Kommas enthalten, müssen in Apostrophe oder Anführungszeichen eingeschlossen werden. Wenn Apostrophe oder

Anführungszeichen verwendet werden, verdoppeln Sie die Anführungszeichen, um sie in einer Zeichenfolge zu verwenden. Optional können Sie die DELIMITED BY-Klausel verwenden, um ein anderes Trennzeichen anzugeben.

Drei weitere spezielle Sequenzen werden ebenfalls erkannt. Die zwei Zeichen \n repräsentieren eine Zeilenendmarke, \\ repräsentiert einen einzelnen Backslash und die Sequenz \xDD, wobei DD die hexadezimale Darstellung eines Zeichens ist, repräsentiert das Zeichen mit hexadezimalen Code DD.

- **FIXED** Eingabezeilen sind im Format mit fester Länge.

### Standardwert

TEXT

### Siehe auch

- „INPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## isql\_allow\_read\_client\_file-Option [Interactive SQL]

Steuert, ob das Lesen von Clientdateien durch die Verbindung zulässig ist.

### Zulässige Werte

On, Off, Prompt

### Standardwert

Prompt

### Bemerkungen

Diese Option steuert, ob der Datenbankserver Dateien auf dem Clientcomputer lesen darf. On heißt, dass das Lesen gestattet ist. Off heißt, dass das Lesen nicht gestattet ist. Prompt bedeutet, dass der Benutzer gefragt wird, welche Aktion durchgeführt werden soll.

Diese Option wird pro Verbindung gespeichert und bleibt nur für die Dauer der Verbindung aufrecht. Sie können diese Option mit der Anweisung SET TEMPORARY OPTION aktivieren. Wenn Sie das Schlüsselwort TEMPORARY weglassen, meldet Interactive SQL einen Fehler.

Mit dieser Option kann eine Datendatei ohne Benutzereingriff gelesen werden, wenn LOAD TABLE von einer gespeicherten Prozedur oder einem Trigger ausgeführt wird.

Sie müssen das READ CLIENT FILE-Systemprivileg haben, um eine Datei auf einem Clientcomputer lesen zu können.

**Siehe auch**

- „Zugriff auf Daten auf Clientcomputern“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „READ\_CLIENT\_FILE-Funktion“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „allow\_read\_client\_file-Option“ auf Seite 573
- „allow\_write\_client\_file-Option“ auf Seite 575
- „isql\_allow\_write\_client\_file-Option [Interactive SQL]“ auf Seite 859
- „Clientseitige Datensicherheit“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

**isql\_allow\_write\_client\_file-Option [Interactive SQL]**

Steuert, ob das Schreiben von Clientdateien durch die Verbindung zulässig ist.

**Zulässige Werte**

On, Off, Prompt

**Standardwert**

Prompt

**Bemerkungen**

Diese Option steuert, ob der Datenbankserver Dateien auf dem Clientcomputer schreiben darf. On heißt, dass das Schreiben gestattet ist. Off heißt, dass das Schreiben nicht gestattet ist. Prompt bedeutet, dass der Benutzer gefragt wird, welche Aktion durchgeführt werden soll.

Diese Option wird pro Verbindung gespeichert und bleibt nur für die Dauer der Verbindung aufrecht. Sie können diese Option mit der Anweisung SET TEMPORARY OPTION aktivieren. Wenn Sie das Schlüsselwort TEMPORARY weglassen, meldet Interactive SQL einen Fehler.

Sie müssen das WRITE CLIENT FILE-Systemprivileg haben, um in eine Datei auf einem Clientcomputer schreiben zu können.

**Siehe auch**

- „Zugriff auf Daten auf Clientcomputern“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „WRITE\_CLIENT\_FILE-Funktion [Zeichenfolge]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „UNLOAD-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „allow\_write\_client\_file-Option“ auf Seite 575
- „allow\_read\_client\_file-Option“ auf Seite 573
- „isql\_allow\_read\_client\_file-Option [Interactive SQL]“ auf Seite 858
- „Clientseitige Datensicherheit“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

**isql\_command\_timing-Option [Interactive SQL]**

Steuert, ob bei SQL-Anweisungen eine Zeitmessung durchgeführt wird

### Zulässige Werte

On, Off

### Standardwert

On

### Bemerkungen

Diese Boolesche Option bestimmt, ob bei SQL-Anweisungen eine Zeitmessung durchgeführt wird. Wenn Sie die Option auf On setzen, wird die Dauer der Ausführung im Fenster **Meldungen** angezeigt, nachdem Sie eine Anweisung ausgeführt haben. Wenn Sie diese Option auf "Off" setzen, wird keine Zeitangabe angezeigt.

Die Ausführungszeiten sind im Log enthalten, wenn die Funktionen für die Protokollierung und die Berichterstellung über die Ausführungszeit aktiviert sind. Siehe „[START LOGGING-Anweisung \[Interactive SQL\]](#)“ [\[SQL Anywhere Server - SQL-Referenzhandbuch\]](#).

Die isql\_command\_timing-Option wird als Option **Ausführungszeit für SQL-Anweisungen messen** auf der Registerkarte **Meldungen** angezeigt. Klicken Sie **Extras » Optionen » Meldungen** und aktivieren bzw. deaktivieren Sie die Option **Ausführungszeit für SQL-Anweisungen messen**.

### Siehe auch

- „[SET OPTION-Anweisung \[Interactive SQL\]](#)“ [\[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## isql\_escape\_character-Option [Interactive SQL]

Steuert die anstelle von nicht-druckbaren Zeichen verwendeten Escapezeichen in Daten, die in TEXT-Dateien exportiert werden.

### Zulässige Werte

Jedes einzelne Zeichen

### Standardwert

Ein Backslash (\)

### Bemerkungen

Wenn Interactive SQL Zeichenfolgen exportiert, die nicht-druckbare Zeichen enthalten (wie einen Zeilenvorschub), wird jedes nicht-druckbare Zeichen in ein hexadezimales Format konvertiert und mit einem vorangestellten Escapezeichen versehen. Das Zeichen, das Sie festlegen, wird in der Ausgabe verwendet, wenn Ihre OUTPUT-Anweisung keine ESCAPE CHARACTER-Klausel enthält. Diese Einstellung wird nur verwendet, wenn Sie Daten in eine Textdatei exportieren.

### Siehe auch

- „[isql\\_quote-Option \[Interactive SQL\]](#)“ auf Seite 863
- „[SET OPTION-Anweisung \[Interactive SQL\]](#)“ [\[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

**Beispiel**

Eine Tabelle erstellen, die einen Zeichenfolgenwert mit einem eingebetteten Zeilenvorschub enthält (als "\n" in der INSERT-Anweisung gekennzeichnet). Dann werden die Daten nach *c:\escape.txt* mit einem Rautenzeichen (#) als Escapezeichen exportiert.

```
CREATE TABLE escape_test( text varchar(10 ) );
INSERT INTO escape_test VALUES( 'one\ntwo' );
SET OPTION isql_escape_character='#';
SELECT * FROM escape_test;
OUTPUT TO c:\escape.txt FORMAT TEXT;
```

Dieser Code platziert die folgenden Daten in *escape.txt*:

```
'one#x0atwo'
```

Das Rautenzeichen (#) ist das Escapezeichen und **x0a** das hexadezimale Äquivalent des \n-Zeichens.

Die Start- und Endzeichen (in diesem Fall Apostrophe) hängen von der isql\_quote-Einstellung ab.

**isql\_field\_separator-Option [Interactive SQL]**

Steuert die Standardzeichenfolge, die zum Trennen der Werte in Daten verwendet wird, die in TEXT-Dateien exportiert werden.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Ein Komma (,)

**Bemerkungen**

Steuert die Standardzeichenfolge, die zum Trennen (oder Delimitieren) der Werte in Daten verwendet wird, die in TEXT-Dateien exportiert werden. Wenn eine OUTPUT-Anweisung keine DELIMITED BY-Klausel enthält, wird der Wert dieser Einstellung verwendet.

**Siehe auch**

- „isql\_quote-Option [Interactive SQL]“ auf Seite 863
- „isql\_escape\_character-Option [Interactive SQL]“ auf Seite 860
- „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Beispiel**

- Im ersten Beispiel wird das Feldtrennzeichen als Doppelpunkt in den Daten eingestellt, die in *c:\Employees.txt* exportiert werden.

```
SET OPTION isql_field_separator=': ';
SELECT Surname, GivenName FROM Employees WHERE EmployeeID < 150;
OUTPUT TO c:\Employees.txt FORMAT TEXT;
```

Dieser Code platziert die folgenden Daten in *Employees.txt*:

```
'Whitney': 'Fran'  
'Cobb': 'Matthew'  
'Chin': 'Philip'  
'Jordan': 'Julie'
```

Die Start- und Endzeichen (in diesem Fall Apostrophe) hängen von der `isql_quote`-Einstellung ab.

- Im nächsten Beispiel wird das Feldtrennzeichen als Tabulator in den Daten eingestellt, die in `c:\Employees.txt` exportiert werden.

```
SET OPTION isql_field_separator='\t';  
SELECT Surname, GivenName FROM Employees WHERE EmployeeID < 150;  
OUTPUT TO c:\Employees.txt FORMAT TEXT;
```

Dieser Code platziert die folgenden Daten in `Employees.txt`:

```
'Whitney' 'Fran'  
'Cobb' 'Matthew'  
'Chin' 'Philip'  
'Jordan' 'Julie'
```

Die Start- und Endzeichen (in diesem Fall Apostrophe) hängen von der `isql_quote`-Einstellung ab. Das Escapezeichen (in diesem Fall der Backslash) hängt von der `isql_escape_character`-Einstellung ab.

### **isql\_maximum\_displayed\_rows-Option [Interactive SQL]**

Gibt die maximale Anzahl an Zeilen an, die im Fensterausschnitt **Ergebnisse** in Interactive SQL angezeigt werden können.

#### **Zulässige Werte**

ALL oder eine nicht-negative Ganzzahl

#### **Standardwert**

500

#### **Bemerkungen**

Mit dieser Option können Sie die maximale Anzahl an Zeilen festlegen, die im Fensterausschnitt **Ergebnisse** angezeigt werden. Sie können den Wert für diese Option auch im Fenster **Optionen** in Interactive SQL setzen.

#### **Vorsicht**

Bei der Anzeige großer Ergebnismengen kann Interactive SQL zu viel Speicher beanspruchen. Wenn dieses Problem auftritt, meldet Interactive SQL das Problem, zeigt aber die Ergebnismenge nicht an.

#### **Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## isql\_print\_result\_set-Option [Interactive SQL]

Gibt an, welche Ergebnismengen gedruckt werden, wenn eine *.sql*-Datei ausgeführt wird.

### Zulässige Werte

- **LAST** Gibt die Ergebnismenge der letzten Anweisung in der Datei aus.
- **ALL** Gibt die Ergebnismengen jeder Anweisung in der Datei aus, die eine Ergebnismenge zurückgibt
- **NONE** Es werden keine Ergebnismengen ausgegeben.

### Standardwert

LAST

### Bemerkungen

Die Option `isql_print_result_set` hat nur dann Auswirkungen, wenn Sie das Interactive SQL-Dienstprogramm von der Befehlszeile ausführen (z.B. wenn eine *.sql*-Datei ausgeführt wird).

Mit dieser Option können Sie angeben, welche Ergebnismengen ausgedruckt werden sollen, wenn eine *.sql*-Datei ausgeführt wird.

### Siehe auch

- „[SET OPTION-Anweisung \[Interactive SQL\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## isql\_quote-Option [Interactive SQL]

Steuert die Standardzeichenfolge, die den Anfang und das Ende aller Zeichenfolgen von Daten markiert, die in TEXT-Dateien exportiert werden.

### Zulässige Werte

Zeichenfolge

### Standardwert

Ein Apostroph (')

### Bemerkungen

Steuert die Standardzeichenfolge, die den Anfang und das Ende aller Zeichenfolgen von Daten markiert, die in TEXT-Dateien exportiert werden. Wenn eine OUTPUT-Anweisung keine QUOTE-Klausel enthält, wird dieser Wert standardmäßig verwendet.

### Siehe auch

- „[isql\\_field\\_separator-Option \[Interactive SQL\]](#)“ auf Seite 861
- „[SET OPTION-Anweisung \[Interactive SQL\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Beispiel

Änderung der Standardzeichenfolge, sodass alle Zeichenfolgen mit einem Anführungszeichen eingeleitet und abgeschlossen werden.

```
SET OPTION isql_quote='';  
SELECT Surname, GivenName FROM Employees WHERE EmployeeID < 150;  
OUTPUT TO c:\Employees.txt FORMAT TEXT;
```

Dieser Code platziert die folgenden Daten in *Employees.txt*:

```
"Whitney", "Fran"  
"Cobb", "Matthew"  
"Chin", "Philip"  
"Jordan", "Julie"
```

Die Trennzeichen (in diesem Fall Kommas) hängen von der `isql_field_separator`-Einstellung ab.

## isql\_show\_multiple\_result\_sets-Option [Interactive SQL]

Gibt an, ob mehrere Ergebnismengen im Fenster **Ergebnisse** in Interactive SQL angezeigt werden können.

### Zulässige Werte

On, Off

### Standardwert

Off

### Bemerkungen

Setzen Sie diese Option auf On, damit Interactive SQL im Fensterausschnitt **Ergebnisse** mehrere Ergebnismengen anzeigt, wenn Sie eine Prozedur ausführen, die mehrere SELECT-Anweisungen zurückgibt.

Jede Ergebnismenge wird auf einer eigenen Registerkarte des Fensterausschnitts **Ergebnisse** angezeigt. Standardmäßig zeigt Interactive SQL nicht mehrere Ergebnismengen an. Die Einstellung dieser Option gilt für Interactive SQL auch, wenn es als Befehlszeilenprogramm ausgeführt wird.

Die `isql_show_multiple_result_sets`-Option erscheint auch als Option **Alle Ergebnismengen anzeigen**, wenn Interactive SQL als Fensteranwendung ausgeführt wird. Siehe [„Rückgabe von mehreren Ergebnismengen“ \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).

Beim Deployment von Interactive SQL können Sie verhindern, dass Benutzer die `isql_show_multiple_result_sets`-Option einstellen. Siehe [showMultipleResultSets \[SQL Anywhere Server - Programmierung\]](#).

### Siehe auch

- [„SET OPTION-Anweisung \[Interactive SQL\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

### Beispiele

Durch Ausführen der folgenden Anweisung wird `isql_show_multiple_result_sets` auf "On" gesetzt.

```
SET OPTION isql_show_multiple_result_sets=On
```

Um die ListPeople-Prozedur zu testen und mehrere Ergebnismengen in Interactive SQL anzuzeigen, führen Sie in Interactive SQL die folgende Anweisung aus:

```
SET OPTION isql_show_multiple_result_sets=On;  
CALL ListPeople ();
```

## nulls-Option [Interactive SQL]

Legt fest, wie NULL in der Datenbank angezeigt wird, wenn Ergebnisse in Interactive SQL angezeigt werden

### Zulässige Werte

Zeichenfolge

### Standardwert

(NULL)

### Bemerkungen

Setzen Sie diese Option nach Wunsch. Dieser Wert wird nicht verwendet, wenn Ergebnismengen in einer Datei gespeichert werden. Der beim Speichern in einer Datei verwendete Wert wird durch die Option output\_nulls angegeben.

### Siehe auch

- „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „output\_nulls-Option [Interactive SQL]“ auf Seite 867

## on\_error-Option [Interactive SQL]

Steuert, was geschieht, wenn beim Ausführen von Anweisungen in Interactive SQL ein Fehler auftritt

### Zulässige Werte

- **Stop** InteractiveSQL führt keine weiteren Anweisungen aus.
- **Prompt** Interactive SQL fordert den Benutzer zu einer Entscheidung auf, ob er fortfahren möchte.
- **Continue** Die Fehler werden an die Registerkarte "Meldungen" von Interactive SQL gesendet und Interactive SQL fährt mit dem Ausführen der Anweisungen fort.
- **Exit** Interactive SQL fährt herunter.
- **Notify\_Continue** Der Fehler wird gemeldet und der Benutzer wird aufgefordert, zum Fortfahren die Eingabetaste zu drücken oder auf **OK** zu klicken.
- **Notify\_Stop** Der Fehler wird gemeldet und der Benutzer wird aufgefordert, zum Stoppen der Anweisungsausführung die Eingabetaste zu drücken oder auf **OK** zu klicken.

- **Notify\_Exit** Der Fehler wird gemeldet und der Benutzer wird aufgefordert, zum Herunterfahren von Interactive SQL die Eingabetaste zu drücken oder auf **OK** zu klicken.

### Standardwert

Prompt

### Bemerkungen

Wenn Sie eine *.sql*-Datei ausführen, sind die Werte Stop und Exit äquivalent. Wenn Sie einen dieser Werte angeben, wird Interactive SQL heruntergefahren.

Diese Option wird ignoriert, wenn die onerror-Option des Interactive SQL-Dienstprogramms (dbisql) angegeben ist.

### Siehe auch

- „Interactive SQL-Dienstprogramm (dbisql)“ auf Seite 939
- „SET OPTION-Anweisung [Interactive SQL]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## output\_format-Option [Interactive SQL]

Legt das Standard-Ausgabeformat für Daten fest, die mit der SELECT-Anweisung abgerufen oder mit der OUTPUT-Anweisung in eine Datei oder Ausgabe umgeleitet wurden.

### Zulässige Werte

- **TEXT** Die Ausgabe ist eine Datei im TEXT-Format mit einer Tabellenzeile pro Ausgabezeile in der Datei. Alle Werte sind durch Kommas getrennt, und Zeichenfolgen werden in Apostrophe eingeschlossen. Die Trennzeichen und Apostrophe oder Anführungszeichen können mit den Klauseln DELIMITED BY und QUOTE geändert werden. Wenn All in der QUOTE-Klausel angegeben wird, werden alle Werte (nicht nur Zeichenfolgen) in Apostrophe oder Anführungszeichen gesetzt.

Drei weitere spezielle Sequenzen werden ebenfalls verwendet. Die zwei Zeichen \n repräsentieren eine Zeilenendmarke, \\ repräsentiert einen einzelnen Backslash und die Sequenz \xDD repräsentiert das Zeichen mit hexadezimalen Code DD.

- **FIXED** Die Ausgabe ist ein festes Format, bei dem jede Spalte eine feste Breite hat. Die Breite für jede Spalte kann mit der COLUMN WIDTH-Klausel angegeben werden. Wenn diese Klausel nicht vorhanden ist, wird die Breite für jede Spalte aus dem Datentyp der Spalte berechnet und ist breit genug, jeden Wert dieses Datentyps aufzunehmen. In diesem Format werden keine Spaltentitel ausgegeben.
- **HTML** Die Ausgabe ist im HTML-Format.
- **SQL** Die Ausgabe ist eine Interactive SQL INPUT-Anweisung, die erforderlich ist, um die Daten in der Tabelle neu zu erstellen.
- **XML** Die Ausgabe ist eine XML-Datei, kodiert in UTF-8 mit einer eingebetteten DTD. Binärwerte sind in CDATA-Blöcken kodiert, wobei die Binärdaten in Form von Zeichenfolgen mit jeweils zwei hexadezimalen Zeichen dargestellt werden.

**Bemerkungen**

Die output\_format-Option wird verwendet, wenn die OUTPUT-Anweisung nicht die FORMAT-Klausel angibt. Die output\_format-Option wird ignoriert, wenn der FORMAT-Klausel angegeben ist.

**Standardwert**

TEXT

**Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „OUTPUT-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**output\_length-Option [Interactive SQL]**

Steuert die Länge von Spaltenwerten, wenn Interactive SQL Informationen in eine externe Datei exportiert.

**Zulässige Werte**

Nicht-negative Ganzzahl

**Standardwert**

0 (keine Kürzung)

**Bemerkungen**

Diese Option steuert die maximale Länge von Spaltenwerten, wenn mit Interactive SQL Daten in eine externe Datei exportiert werden (unter Verwendung der Ausgabeumleitung mit der OUTPUT-Anweisung). Diese Option wirkt sich nur auf die Ausgabeformate TEXT, HTML und SQL aus.

**Siehe auch**

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**output\_nulls-Option [Interactive SQL]**

Legt fest, wie NULL exportiert wird.

**Zulässige Werte**

Zeichenfolge

**Standardwert**

Leere Zeichenfolge

**Bemerkungen**

Diese Option steuert, wie NULL von der OUTPUT-Anweisung geschrieben wird. Bei jedem NULL-Wert in der Ergebnismenge wird stattdessen die Zeichenfolge dieser Option zurückgegeben. Diese Option wirkt sich nur auf die Ausgabeformate TEXT, HTML, FIXED und SQL aus.

## Beispiel

Im folgenden Beispiel wird der Wert, der für NULL erscheint, zu **(unknown)** geändert:

```
SET OPTION output_nulls = '(unknown)';
```

## Siehe auch

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „IFNULL-Funktion [Verschiedene]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## truncation\_length-Option [Interactive SQL]

Steuert, wie breite Spalten gekürzt werden, damit die Anzeigen auf den Bildschirm passen

## Zulässige Werte

Ganzzahl

## Standardwert

256

## Bemerkungen

Die Option truncation\_length begrenzt die Länge der angezeigten Spaltenwerte. Die Einheit sind Zeichen. Ein Wert von "0" bedeutet, dass Spaltenwerte nicht gekürzt werden. Der Standardwert für die Kürzungslänge ist 256.

## Siehe auch

- „SET OPTION-Anweisung [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Versionsverwaltungsintegration in Interactive SQL

Interactive SQL integriert Versionsverwaltungssysteme von Drittherstellern, sodass Sie viele gebräuchliche Versionsverwaltungsvorgänge aus Interactive SQL ausführen können. Unter Windows integriert Interactive SQL die meisten Versionsverwaltungsprodukte, die die Microsoft Common Source Code Control API (SCC) unterstützen, wie z.B Microsoft Visual SourceSafe. Um Versionsverwaltungsprodukte zu verwenden, die die SCC API unter Windows und anderen Betriebssystemen nicht unterstützen, geben Sie eine Befehlszeile an, die für jeden Versionskontrollvorgang ausgeführt wird. Die Ausgabe dieser Befehle wird in einem Protokollfenster angezeigt.

Interactive SQL unterstützt die folgenden Aufgaben (sofern die Aufgabe vom Versionsverwaltungsprodukt unterstützt wird):

- Ein Versionsverwaltungsobjekt öffnen
- Abrufen
- Einchecken (Check-In)
- Auschecken (Check-Out)
- Auschecken rückgängig machen
- Versionen vergleichen
- Dateiverlauf anzeigen
- Dateieigenschaften anzeigen
- Den Versionsverwaltungsmanager ausführen

Wenn das darunterliegende Versionsverwaltungsprogramm eine Aktion nicht unterstützt, ist der entsprechende Menüeintrag deaktiviert. Microsoft Visual SourceSafe unterstützt z.B. alle diese Aktionen, aber die Verwendung eines benutzerdefinierten (Befehlszeilen-)Versionsverwaltungssystems unterstützt nicht das Öffnen eines Versionsverwaltungsprojekts oder das Ausführen eines Versionsverwaltungsmanagers.

Sie sollten mit den Vorgängen Ihres Versionsverwaltungsprogramms vertraut sein, bevor Sie es von Interactive SQL aus verwenden.

## Interactive SQL für die Verwendung der Versionsverwaltung konfigurieren

Bevor Sie Versionsverwaltungsaaktionen für Dateien durchführen können, z.B. das Ein- und Auschecken von Dateien, das Vergleichen von verschiedenen Versionen einer Datei oder das Anzeigen des Verlaufs für eine Datei, müssen Sie Interactive SQL für die Verwendung der Versionsverwaltung konfigurieren.

### Voraussetzungen

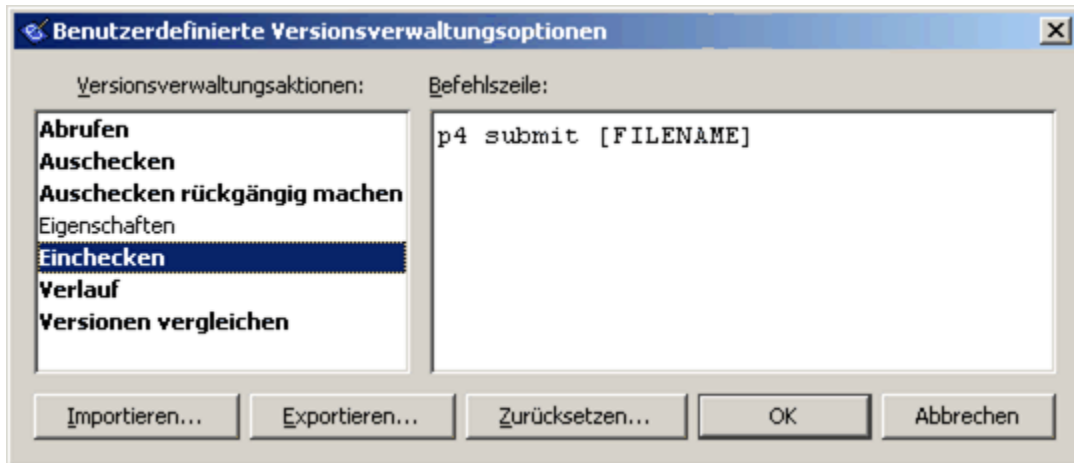
Ihr Versionsverwaltungssystem muss eingerichtet sein.

Wenn Sie Interactive SQL auf einem Windows-Computer mit einem Versionsverwaltungsprodukt ausführen, das die Microsoft SCC-API unterstützt, können Sie dieses Produkt oder ein benutzerdefiniertes System (über die Befehlszeile) verwenden.

### Aufgabe

1. Klicken Sie in Interactive SQL auf **Extras » Optionen**.
2. Klicken Sie im linken Fensterausschnitt auf **Versionsverwaltung**.
3. Klicken Sie auf **Integration der Versionsverwaltung aktivieren**.

Option	Aktion
SCC-Versionsverwaltungssysteme konfigurieren	Klicken Sie auf <b>OK</b> .
Andere Versionsverwaltungssysteme konfigurieren	<p>a. Klicken Sie auf <b>Konfigurieren</b>.</p> <p>b. Im Fenster <b>Benutzerdefinierte Versionsverwaltungsoptionen</b> klicken Sie auf <b>Zurücksetzen</b>.</p> <p>c. Wählen Sie Ihr Versionsverwaltungssystem aus der Liste und klicken Sie auf <b>OK</b>.</p> <p>d. Bearbeiten Sie ggf. die Liste, indem Sie eine Aktion in der Liste <b>Versionsverwaltungsaktionen</b> auswählen und den entsprechenden Befehl in den Fensterausschnitt <b>Befehlszeile</b> eingeben.</p> <p>Wenn Sie Befehle für Ihr System in der Liste <b>Versionsverwaltungsaktionen</b> festlegen, verwenden Sie den Platzhalter [FILENAME] für den Namen der Datei, die beim Ausführen des Befehls verwendet wird. Beispiel: Der Befehl zum Senden einer Datei in Perforce lautet <code>p4 submit [FILENAME]</code>. Befehle sind nur für die Aktionen definiert, die in der Liste fett erscheinen.</p> <p>Das Fenster <b>Benutzerdefinierte Versionsverwaltungsoptionen</b> mit den definierten Befehlen in Fettdruck.</p> <p>Wenn Sie keine Befehlszeile für eine Aktion festlegen, ist der Eintrag im Menü <b>Datei » Versionsverwaltung</b> deaktiviert.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Tipp</b>          Sie können Ihre Versionsverwaltungs-Befehlszeilen in eine externe Datei exportieren, indem Sie im Fenster <b>Benutzerdefinierte Versionsverwaltungsoptionen</b> auf <b>Exportieren</b> klicken (Zugriff über <b>Extras » Optionen</b> und Klicken auf <b>Konfigurieren</b> im Fensterausschnitt <b>Versionsverwaltung</b>). Sie können diese Befehlszeilen zu einem späteren Zeitpunkt wieder einlesen, indem Sie in diesem Fenster auf <b>Importieren</b> klicken. Dies ist nützlich, wenn Sie Interactive SQL-Versionsverwaltungs-Befehlszeilen auf mehreren Computern konfigurieren müssen.</p> </div> <p>e. Klicken Sie auf <b>OK</b> und dann nochmals auf <b>OK</b>.</p>



## Ergebnisse

Das Versionsverwaltungssystem wird integriert.

## Versionsverwaltungsprojekte und Interactive SQL

Einige Versionsverwaltungsprodukte erfordern, dass Sie ein Versionsverwaltungsprojekt öffnen, bevor Sie weitere Versionsverwaltungsaktionen durchführen können. Die genaue Definition, was ein Projekt ist, hängt vom Versionsverwaltungssystem ab, das Sie verwenden. Üblicherweise ist es ein Satz von Dateien, die unter die Versionsverwaltung fallen, zusammen mit einem Standort auf Ihrem lokalen Dateisystem, auf dem Arbeitskopien der Dateien abgelegt werden. Sie müssen dem Versionsverwaltungssystem üblicherweise Anmeldeinformationen angeben, z.B. Benutzer-ID und Kennwort, um ein Projekt zu öffnen.

Wenn Ihr Versionsverwaltungssystem das Öffnen eines Versionsverwaltungsprojekts unterstützt, ist der Menüeintrag **Datei » Versionsverwaltung » Versionsverwaltungsprojekt öffnen** aktiviert. Wenn Sie diese Option im Menü **Datei** verwenden, wird ein Versionsverwaltungs-spezifisches Fenster zum Öffnen eines Projekts angezeigt. Wenn Sie ein Projekt geöffnet haben, müssen Sie es nicht nochmals öffnen, auch nicht in nachfolgenden Interactive SQL-Sitzungen. Das Projekt wird automatisch geöffnet.

## Dateien mit Interactive SQL auschecken

Checken Sie eine Datei aus, indem Sie ihren Inhalt im Fensterausschnitt **SQL-Anweisungen** ändern oder den Befehl im Menü **Datei** verwenden.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

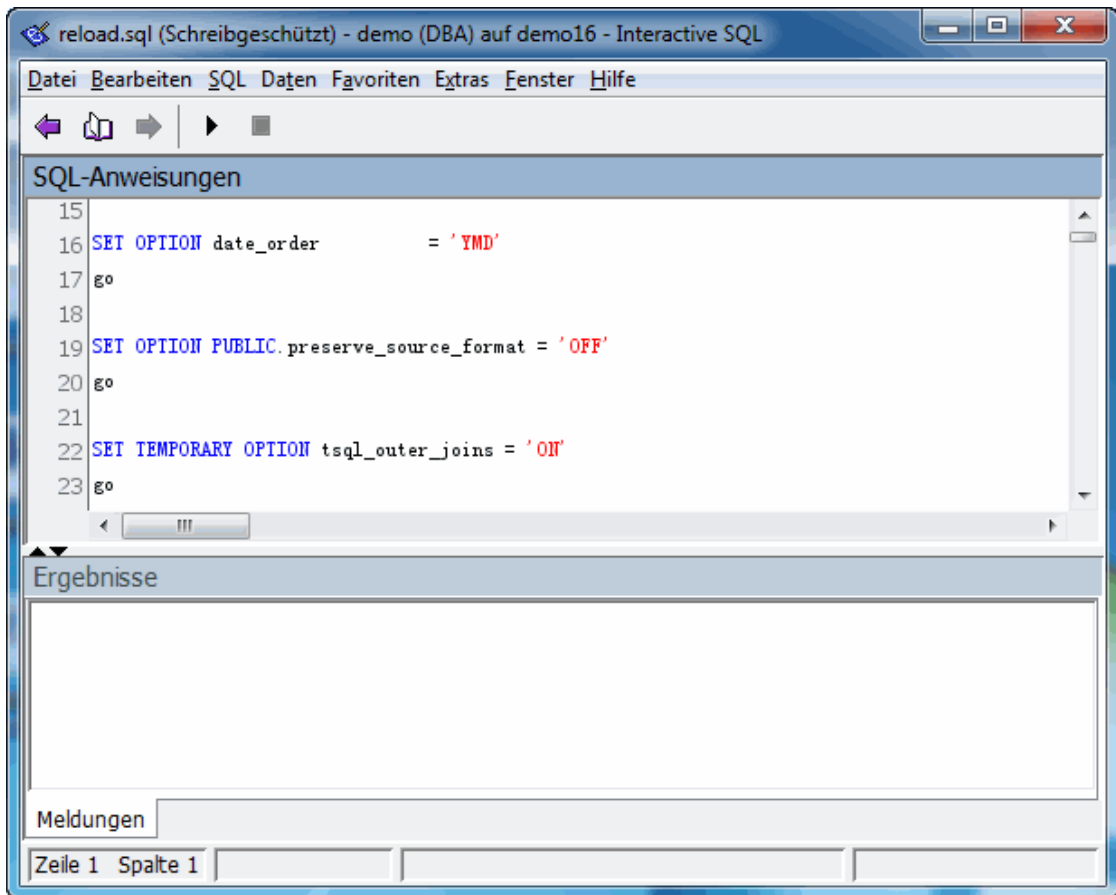
Wählen Sie beim Konfigurieren der Versionsverwaltungsoptionen für Interactive SQL die Option **Automatisches Auschecken von Dateien, wenn Editor-Inhalt geändert wird**, wenn Interactive SQL

versuchen soll, eine Datei auszuchecken, sobald Sie deren Inhalt im Fensterausschnitt **SQL-Anweisungen** ändern.

### Aufgabe

1. Klicken Sie in Interactive SQL auf **Datei » Öffnen** und navigieren Sie dann zu der Datei, die Sie öffnen möchten.

Der Dateistatus wird auf der Statusleiste am unteren Rand des Interactive SQL-Fensters angezeigt. Der Status kann **Eingecheckt**, **Ausgecheckt** und **Nicht erfasst** sein. Eingecheckte Dateien werden als schreibgeschützt angesehen, und **Schreibgeschützt** wird in der Interactive SQL-Titelleiste angezeigt. Die Datei im folgenden Beispiel ist eingecheckt:



#### Vorsicht

Wenn Sie ein SCC-API-kompatibles Versionsverwaltungssystem verwenden, ist der Status immer richtig. Wenn Sie das benutzerdefinierte Versionsverwaltungssystem verwenden, hängt der Status davon ab, ob die Datei schreibgeschützt ist oder nicht. Eine schreibgeschützte Datei wird als eingecheckt angesehen, aber bearbeitbare Dateien können entweder ausgecheckt sein oder nicht der Versionsverwaltung unterliegen.

2. Checken Sie die Datei aus, indem Sie auf **Datei » Versionsverwaltung » Auschecken** klicken.

### Ergebnisse

Abhängig vom verwendeten Versionsverwaltungsprodukt werden Sie möglicherweise zur Eingabe eines Kommentars oder anderer Optionen als Teil des Auscheck-Verfahrens aufgefordert.

### Nächste Schritte

Wenn Sie mit der Bearbeitung der Datei fertig sind, können Sie sie wieder über Interactive SQL einchecken. Klicken Sie auf **Datei » Versionsverwaltung » Einchecken**. Falls Sie dazu aufgefordert werden, geben Sie Kommentare zum Eincheckvorgang ein.

## Zusätzliche Versionsverwaltungsaktionen

Zusätzlich zum Öffnen von Versionsverwaltungsprojekten und dem Check-In bzw. Check-Out von Dateien unterstützt Interactive SQL mehrere weitere Versionsverwaltungsaktionen. Die Verfügbarkeit dieser Aktionen hängt vom verwendeten Versionsverwaltungssystem ab. Klicken Sie auf **Datei » Versionsverwaltung** und wählen Sie anschließend eine Aktion:

- **Abrufen** Diese Aktion ruft die letzte Kopie der Datei ab, die Sie derzeit im Fensterausschnitt **SQL-Anweisungen** geöffnet haben.
- **Auschecken rückgängig machen** Wenn Sie eine Datei ausgecheckt haben und Ihre Änderungen verwerfen möchten, klicken Sie auf **Datei » Versionsverwaltung » Auschecken rückgängig machen**. Dies verwirft die Arbeitskopie der Datei und lädt die Kopie der Datei herunter, die sich im Versionsverwaltungsarchiv befindet.
- **Versionen vergleichen** Diese Aktion vergleicht die Arbeitskopie der Datei, die Sie geöffnet haben, mit der Version im Versionsverwaltungsarchiv.
- **Verlauf** Diese Aktion zeigt eine Liste der Versionsverwaltungsaktionen (üblicherweise Check-Ins) an, die an der geöffneten Datei durchgeführt wurden.
- **Eigenschaften** Diese Aktion zeigt eine Liste von Versionsverwaltungseigenschaften an, die der geöffneten Datei zugeordnet sind.
- **Source Control-Manager ausführen** Diese Aktion lädt das Verwaltungsprogramm für Ihr Versionsverwaltungssystem. Wenn Sie z.B. Microsoft Visual SourceSafe verwenden, wird der Microsoft Visual SourceSafe Explorer geladen.

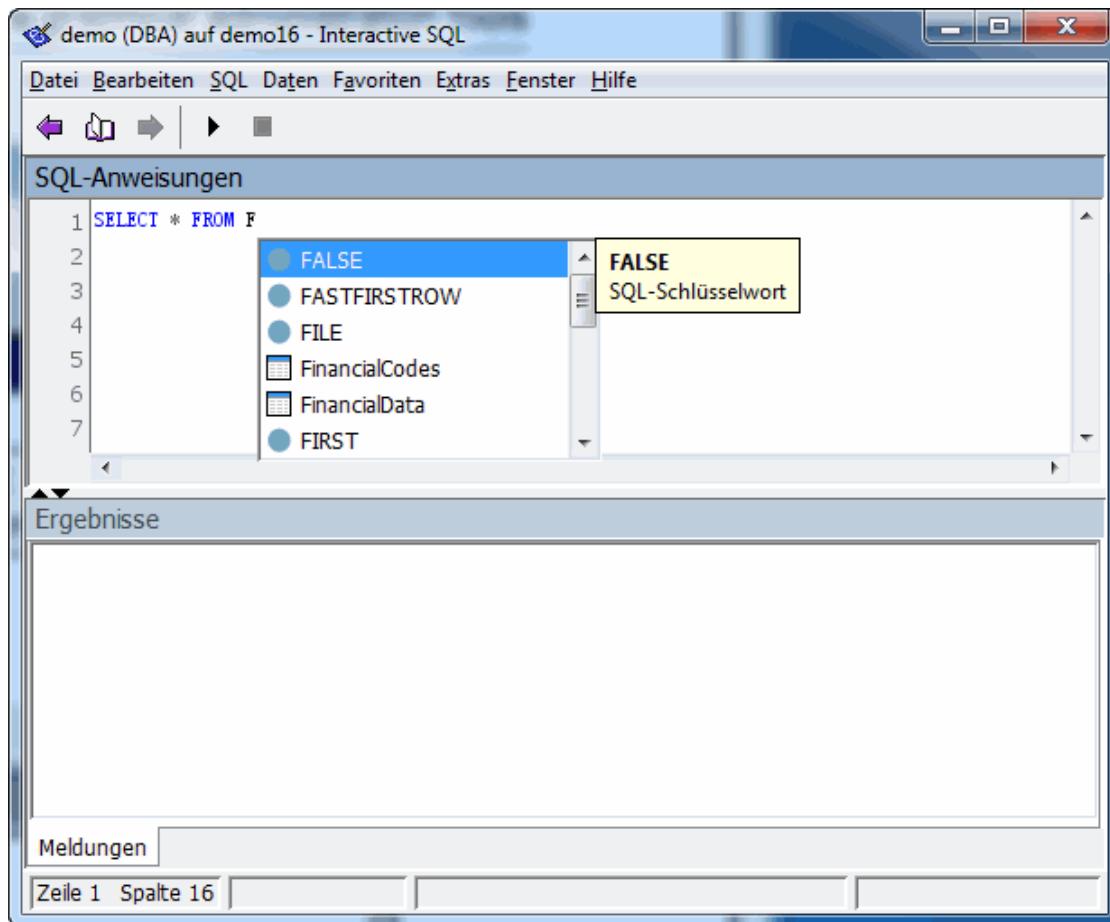
## Textvervollständigung

Interactive SQL und Sybase Central haben eine Textvervollständigungsoption, die komplette Schlüsselwörter und Objektnamen einfügt, während Sie die ersten Buchstaben eingeben. Beispiel: Wenn Sie den Buchstaben "S" eingeben, erscheint ein Textvervollständigungsfenster mit einer Liste der möglichen Schlüsselwörter oder Objektnamen, die mit dem Buchstaben "S" beginnen. Sie können die Einstellungen für die Textvervollständigung im Dialogfeld **Optionen** in Interactive SQL oder einem Texteditor-Fenster in Sybase Central festlegen.

## Beispiel

In Interactive SQL geben Sie den ersten Buchstaben eines Datenbank-Objektnamens in den Fensterausschnitt **SQL-Anweisungen** ein.

Standardmäßig wird das Textvervollständigungsfenster automatisch während des Tippens geöffnet. Alternativ dazu können Sie auch Strg+Leertaste oder Strg+Umschalt+Leertaste drücken, um das Fenster zu öffnen. Das Textvervollständigungsfenster enthält eine Liste der Datenbankobjekte, die mit den von Ihnen eingegebenen Buchstaben beginnen. Im folgenden Beispiel zeigt die Textvervollständigung alle Datenbankobjekte an, die mit dem Buchstaben F beginnen.



Wenn der gewünschte Objektname nicht erscheint, drücken Sie Strg+A, um eine vollständige Liste der Datenbankobjekte anzuzeigen (basierend auf von Ihnen gesetzten Filteroptionen, standardmäßig werden alle Datenbankobjekte aufgelistet).

Wählen Sie den Objektnamen in der Liste aus und drücken Sie die Eingabetaste.

Der Objektname wird im Fensterausschnitt **SQL-Anweisungen** angezeigt.

## Tastenkürzel bei der Textvervollständigung

Die folgenden Tastenkürzel stehen zur Verfügung, wenn die Textvervollständigungsliste geöffnet ist.

Taste	Beschreibung
Strg+A	Zeigt eine kontextunabhängige Liste der Übereinstimmungen an.
Strg+Anführungszeichen (") (oder Strg+Umschalt+')	Vervollständigt den Namen und setzt ihn in Anführungszeichen, unabhängig von der Einstellung der Option <code>quoted_identifier</code> . Siehe „ <a href="#">quoted_identifier-Option</a> “ auf Seite 660.
Strg+Stern (*) (oder Strg+Umschalt+8)	Fügt bei Tabellen eine durch Kommas getrennte Liste von Spalten ein, einschließlich Datentypen  Fügt bei gespeicherten Prozeduren den Prozedurnamen ein, gefolgt von einer durch Kommas getrennten Liste von Parameternamen und ihrer Datentypen
Strg+C	Ändert den Inhalt der Textvervollständigungsliste, indem Spalten angezeigt bzw. verborgen werden
Strg+F	Ändert den Inhalt der Textvervollständigungsliste, indem SQL-Funktionen angezeigt bzw. verborgen werden
Strg+P	Ändert den Inhalt der Textvervollständigungsliste, indem gespeicherte Prozeduren und Funktionen angezeigt bzw. verborgen werden
Strg+Pluszeichen (+) (oder Strg+Umschalt+=)	Fügt bei Tabellen eine durch Kommas getrennte Liste von Spalten ein  Fügt bei gespeicherten Prozeduren den Prozedurnamen ein, gefolgt von einer durch Kommas getrennten Liste von Parameternamen
Strg+S	Ändert den Inhalt der Textvervollständigungsliste, indem Systemobjekte angezeigt bzw. verborgen werden
Strg+Umschalt+Leertaste oder Strg+Leertaste	Öffnet das Textvervollständigungsfenster. Sie können auch Strg+Leertaste verwenden, um das Textvervollständigungsfenster zu öffnen.
Strg+T	Ändert den Inhalt der Textvervollständigungsliste, indem Tabellen angezeigt bzw. verborgen werden
Strg+V	Ändert den Inhalt der Textvervollständigungsliste, indem Ansichten angezeigt bzw. verborgen werden
Esc	Schließt das Textvervollständigungsfenster, ohne Text hinzuzufügen
Tabulatortaste	Akzeptiert die Auswahl und schließt das Textvervollständigungsfenster.

## Schnelllader-Option

Die Schnelllader-Option verkürzt die Startzeit für die grafischen Administrationstools von Sybase Central und Interactive SQL. Wenn der Schnelllader aktiviert ist, bleibt das betreffende Tool nach dem Schließen für eine konfigurierbare Zeitspanne im Speicher. Wenn Sie das Tool innerhalb dieser Zeitspanne neu starten, erfolgt der Start schnell. Wenn Sie das Tool nicht innerhalb dieser Zeitspanne neu starten, wird der Prozess beendet und gibt seine Ressourcen für das Betriebssystem frei. Standardmäßig ist der Zeitgeber für diese Inaktivität auf 30 Minuten eingestellt.

Wenn die Schnelllader-Option aktiviert ist, wird das Symbol des betreffenden Tools in der Taskleiste angezeigt. Sie können das Tool neu starten oder herunterfahren, indem Sie mit der rechten Maustaste auf das Taskleistensymbol klicken. Wenn Sie das Tool mithilfe des Taskleistensymbols herunterfahren, wird der Schnelllader-Prozess beendet und gibt seine Ressourcen für das Betriebssystem frei.

Standardmäßig ist die Schnelllader-Option aktiviert. Die Schnelllader-Option ist nur unter Windows verfügbar.

## Schnelllader-Option konfigurieren

Konfigurieren Sie die Schnelllader-Option von Sybase Central oder Interactive SQL, um die Startzeit für diese grafischen Administrationstools zu verkürzen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Die Schnelllader-Option nutzt einen TCP/IP-Port Ihres Computers. Falls dieser Port bereits von einem anderen Programm genutzt wird, können Sie die vom Schnelllader verwendete Portnummer ändern.

Wenn die Schnelllader-Option für die im Zeitgeber für Inaktivität angegebene Zeitspanne nicht verwendet wurde, wird sie beendet. Dadurch wird Speicherplatz für andere Anwendungen freigegeben. Standardmäßig ist der Zeitgeber für Inaktivität auf 30 Minuten eingestellt.

### Aufgabe

1. Klicken Sie in Interactive SQL oder Sybase Central auf **Extras » Optionen**.
2. Wählen Sie unter **Schnelllader** die Option **Schnelllader aktivieren** und klicken Sie dann auf **Konfigurieren**.
3. Füllen Sie die Felder **Portnummer** und **Schnelllader beenden** aus.
4. Klicken Sie zweimal auf **OK**.

### Ergebnisse

Die Schnelllader-Option wird konfiguriert.

## SQL Anywhere-Konsolendienstprogramm (dbconsole)

Das SQL Anywhere-Konsolendienstprogramm (dbconsole) stellt Verwaltungs- und Überwachungsfunktionen für Datenbankserver-Verbindungen zur Verfügung.

Das Dienstprogramm dbconsole wird auf mehreren Plattformen unterstützt. Weitere Hinweise zur Verfügbarkeit von Plattformen finden Sie unter <http://www.sybase.com/detail?id=1061806>.

Auf den Plattformen, die das Dienstprogramm dbconsole nicht unterstützen, können Sie die Eigenschaften der Verbindung, der Datenbank und des Servers verwenden, um Informationen zu erhalten. Sie können Ihren Datenbankserver aber auch von einem Computer überwachen, dessen Betriebssystem die SQL Anywhere-Konsole unterstützt (wie Windows, Mac OS X oder Linux).

Weitere Informationen über die Optionen, die das SQL Anywhere-Konsolendienstprogramm unterstützt, finden Sie unter „[SQL Anywhere-Konsolendienstprogramm \(dbconsole\)](#)“ auf Seite 981.

## Das SQL Anywhere-Konsolendienstprogramm starten (dbconsole)

Verwenden Sie das Dienstprogramm dbconsole, um Datenbankserververbindungen zu verwalten und zu überwachen.

### Voraussetzungen

Um mit Privilegien verbundene Vorgänge mithilfe des SQL Anywhere-Konsolendienstprogramms (dbconsole) ausführen zu können, müssen Sie die Privilegien für den betreffenden Vorgang haben.

**Linux** Sie müssen eine Version von Linux verwenden, die die Linux-Desktop-Symbole unterstützt. Die Desktop-Symbole müssen bei der Installation von SQL Anywhere installiert worden sein.

**Unix** Das Sourcen der SQL Anywhere-Dienstprogramme muss bereits abgeschlossen sein. Siehe „[Unix- und Mac OS X-Umgebungsvariablen](#)“ auf Seite 467.

### Aufgabe

- Starten Sie das SQL Anywhere-Konsolendienstprogramm und stellen Sie eine Verbindung mit einer Datenbank her.

Option	Aktion
Befehlszeile	<p>Führen Sie den folgenden Befehl aus:</p> <pre>dbconsole -c "connection-string"</pre> <p>Wenn Sie die Option -c weglassen, die Verbindungsparameter für die Datenbank angibt, oder wenn Sie nicht genügend Verbindungsparameter angeben, wird das Fenster <b>Verbinden</b> angezeigt, in dem Sie Verbindungsinformationen für die Datenbank eingeben können.</p>

Option	Aktion
Windows	Klicken Sie auf <b>Start » Programme » SQL Anywhere 16 » Administrations-tools » SQL Anywhere-Konsole</b> .
Linux	<ol style="list-style-type: none"> <li>Klicken Sie auf <b>Anwendungen » SQL Anywhere 16 » Administrations-tools » SQL Anywhere-Konsole</b>.</li> <li>Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</li> <li>Klicken Sie auf <b>Verbinden</b>.</li> </ol>
Mac OS X	<ol style="list-style-type: none"> <li>Doppelklicken Sie im Finder auf <b>DBConsole</b> in <i>/Applications/SQLAnywhere16</i>.</li> <li>Geben Sie die Verbindungsinformationen für Ihre Datenbank im Fenster <b>Verbinden</b> ein.</li> <li>Klicken Sie auf <b>Verbinden</b>.</li> </ol>

### Ergebnisse

Das SQL Anywhere-Konsolendienstprogramm wird gestartet und Sie werden mit einer Datenbank verbunden.

### Siehe auch

- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 981

## Das Hauptfenster des SQL Anywhere-Konsolendienstprogramms (dbconsole) konfigurieren

Sie können konfigurieren, welche Informationen in den Fensterausschnitten **Verbindungen**, **Eigenschaften** und **Meldungen** angezeigt werden.

### Voraussetzungen

Sie müssen das SERVER OPERATOR-Systemprivileg haben.

### Kontext und Bemerkungen

Das Dienstprogramm dbconsole besteht aus drei Fensterausschnitten:

- **Verbindungen** Zeigt Informationen über aktuelle Datenbankverbindungen an
- **Eigenschaften** Zeigt Informationen über Datenbanken und Datenbankserver an, die derzeit ausgeführt werden
- **Meldungen** Zeigt Datenbankserver-Meldungen an

## Aufgabe

1. Klicken Sie im Dienstprogramm dbconsole auf **Datei » Optionen**.

Option	Aktion
Fensterausschnitt <b>Verbindungen</b>	Im linken Fensterausschnitt klicken Sie auf <b>Verbindungsanzeige</b> .  Wählen Sie die Eigenschaften aus, die im Feld <b>Verbindungen</b> angezeigt werden sollen.
Fensterausschnitt <b>Eigenschaften</b>	Im linken Fensterausschnitt klicken Sie auf <b>Eigenschaftsanzeige</b> .  Wählen Sie die Datenbank und die Datenbankservereigenschaften, die im Feld <b>Eigenschaften</b> angezeigt werden sollen.
Fensterausschnitt <b>Meldungen</b>	Im linken Fensterausschnitt klicken Sie auf <b>Meldungsanzeige</b> .  Wählen Sie die Meldungsoptionen für die Meldungen aus, die im Feld <b>Meldungen</b> angezeigt werden sollen.

2. Klicken Sie auf **OK**.

## Ergebnisse

Die Informationen im Fensterausschnitt **Verbindungen**, **Eigenschaften** bzw. **Meldungen** werden angepasst.

## Siehe auch

- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 981

## Software-Updates

Sie können jederzeit nach SQL Anywhere-Software-Updates suchen, indem Sie eine der folgenden Methoden anwenden:

- **Startmenü** Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Updates suchen**.
- **Sybase Central** Klicken Sie auf **Hilfe » SQL Anywhere 16 » Updates suchen**.
- **Interactive SQL** Klicken Sie auf **Hilfe » Updates suchen**.
- **SQL Anywhere-Konsolendienstprogramm (dbconsole)** Klicken Sie auf **Hilfe » Updates suchen**.
- **SQL Anywhere-Dienstprogramm für Supportanfragen (dbsupport)** Führen Sie den folgenden Befehl aus:

```
dbsupport -iu
```

- **Sybase-Website** Gehen Sie zu <http://downloads.sybase.com>. Sie benötigen ein Login für Sybase.com, um diese Seite anzuzeigen.

**Siehe auch**

- „Fehlerbehandlung: Fehler in SQL Anywhere melden“ auf Seite 1108
- „Dienstprogramm für Supportanfragen (dbsupport)“ auf Seite 987
- Option -iu, dbsupport auf Seite 988

## Suchfunktion für Updates konfigurieren (Sybase Central)

Konfigurieren Sie SQL Anywhere so, dass Sie benachrichtigt werden, wenn Updates wie Supportpakete und Minor Releases verfügbar sind. Außerdem können Sie Performancedaten an das Entwicklungsteam senden, um zur Verbesserung des Produkts beizutragen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Standardmäßig sucht SQL Anywhere täglich nach Software-Updates.

**Aufgabe**

1. Klicken Sie auf **Hilfe » SQL Anywhere 16 » Suchfunktion für Updates konfigurieren**.
2. Bearbeiten Sie die Einstellungen unter **Software-Updates und Hinweise**.
3. Klicken Sie auf **OK**.

**Ergebnisse**

Die Suchfunktion für Updates wird konfiguriert.

**Siehe auch**

- „Dienstprogramm für Supportanfragen (dbsupport)“ auf Seite 987
- [Details zur Performancedatensammlung](#)

## Suchfunktion für Updates konfigurieren (Interactive SQL)

Konfigurieren Sie SQL Anywhere so, dass Sie benachrichtigt werden, wenn Updates wie Supportpakete und Minor Releases verfügbar sind. Außerdem können Sie Performancedaten an das Entwicklungsteam senden, um zur Verbesserung des Produkts beizutragen.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Standardmäßig sucht SQL Anywhere täglich nach Software-Updates.

### Aufgabe

1. Klicken Sie in Interactive SQL auf **Extras » Optionen » Support**.
2. Bearbeiten Sie die Einstellungen unter **Software-Updates und Hinweise**.
3. Klicken Sie auf **OK**.

### Ergebnisse

Die Suchfunktion für Updates wird konfiguriert.

### Siehe auch

- [„Dienstprogramm für Supportanfragen \(dbsupport\)“ auf Seite 987](#)
- [Details zur Performancedatensammlung](#)

## Updates konfigurieren (dbconsole)

Sie können SQL Anywhere so konfigurieren, dass Sie benachrichtigt werden, wenn Updates wie Supportpakete und Minor Releases verfügbar sind. Außerdem können Sie Performancedaten an das Entwicklungsteam senden, um zur Verbesserung des Produkts beizutragen.

### Voraussetzungen

Sie müssen das SERVER OPERATOR-Systemprivileg haben.

### Kontext und Bemerkungen

Standardmäßig sucht SQL Anywhere täglich nach Software-Updates.

### Aufgabe

1. Klicken Sie im SQL Anywhere-Konsolendienstprogramm auf **Datei » Optionen » Support**.
2. Bearbeiten Sie die Einstellungen unter **Software-Updates und Hinweise**.
3. Klicken Sie auf **OK**.

### Ergebnisse

Die Suchfunktion für Updates wird konfiguriert.

### Siehe auch

- [„SQL Anywhere-Konsolendienstprogramm \(dbconsole\)“ auf Seite 981](#)

## Dienstprogramme für die Datenbankadministration

SQL Anywhere verfügt über eine Reihe von Dienstprogrammen für die Datenbankadministration. Auf jedes der Dienstprogramme können Sie von Sybase Central oder Interactive SQL aus oder über eine Eingabeaufforderung zugreifen.

Weitere Hinweise zur Verfügbarkeit von Plattformen finden Sie unter <http://www.sybase.com/detail?id=1002288>.

Die Administrationsdienstprogramme verwenden eine Reihe von Registrierungseinträgen oder *.ini*-Dateien. Siehe „[Registrierung und INI-Dateien](#)“ auf Seite 487.

### Siehe auch

- „[Sybase Central](#)“ auf Seite 795
- „[Interactive SQL](#)“ auf Seite 814

## Konfigurationsdateien

Viele der von SQL Anywhere 16 zur Verfügung gestellten Dienstprogramme erlauben es Ihnen, Befehlszeilenoptionen in einer Konfigurationsdatei zu speichern. Wenn Sie eine große Menge dieser Optionen verwenden, kann es nützlich sein, sie in einer Konfigurationsdatei zu speichern.

Mit der *@data*-Option können Sie Umgebungsvariablen und Konfigurationsdateien in der Befehlszeile angeben. Um eine Konfigurationsdatei anzugeben, ersetzen Sie *data* durch Pfad und Name der Konfigurationsdatei. Wenn eine Umgebungsvariable und eine Konfigurationsdatei denselben Namen haben, wird die Umgebungsvariable verwendet.

Die Konfigurationsdateien können Zeilenumbrüche und eine beliebige Menge von Optionen enthalten, einschließlich die *@data*-Option. Sie können das Rautenzeichen (#) am Anfang einer Zeile verwenden, um die Zeile als Kommentar zu kennzeichnen. Wenn das kaufmännische Und (&) allein am Ende einer Zeile steht, bedeutet dies, dass die vorherige Einheit in der nächsten Zeile fortgesetzt wird. Die folgende Konfigurationsdatei könnte beispielsweise verwendet werden, um einen Server zu starten, der die starke Verschlüsselung gestattet:

```
-ec TLS(FIPS=Y;IDENTITY=rsaserver.id; &  
      IDENTITY_PASSWORD=test)  
-x TCPIP c:\mydemo.db
```

Der *@data*-Parameter kann überall in der Befehlszeile angegeben werden. In der Datei enthaltene Parameter werden an der betreffenden Stelle eingefügt. Sie können *@data* mehrfach in einer Befehlszeile verwenden, um mehrere Konfigurationsdateien anzugeben.

Dienstprogramme lesen die Befehlszeile, indem sie die angegebenen Konfigurationsdateien erweitern und die gesamte Befehlszeile von links nach rechts lesen. Wenn Sie Optionen angeben, die von anderen Optionen in der Befehlszeile aufgehoben werden, setzt sich die Option durch, die dem Zeilenende am nächsten ist. Konflikte zwischen Optionen können zu Fehlern führen.

**Hinweis**

Das Dienstprogramm für den Serverstart im Hintergrund (dbspawn) erweitert keine durch die @data-Option angegebenen Konfigurationsdateien.

Wenn Sie Kennwörter oder andere Informationen in einer Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922.

**Escapezeichen in der Konfigurationsdatei**

Wenn der Wert für eine Option in einer Konfigurationsdatei Werte mit Leerstellen enthält, muss der Wert in Anführungszeichen gesetzt werden. Wenn der Wert in Anführungszeichen zusätzliche Werte mit Leerstellen enthält, müssen die Anführungszeichen um die zusätzlichen Werte mit Escapezeichen versehen werden. SQL Anywhere unterstützt die Zeichenfolge \\ als Escapezeichen für einen Backslash \ und die Zeichenfolge \" als Escapezeichen für Anführungszeichen \".

In folgendem Abschnitt einer dbdsn-Konfigurationsdatei wurden zum Beispiel Anführungszeichen mit Escapezeichen versehen:

```
-l "subject=$remote_id;
  content=sync cardealer;
  action='run dbmlsync.exe -c \"filedsn=c:\my fdsns\CarDealer.dsn\"
  -ot dbmlsync.log -k -e sa=on';"
```

**Beispiel**

Die folgende Konfigurationsdatei enthält eine Reihe von Optionen für das Validierungsdienstprogramm (dbvalid):

```
#Connect to the sample database as the user DBA with password sql
-c "UID=DBA;PWD=sql;DBF=%SQLANYAMP16%\demo.db"
#Perform an express check on each table
-fx
#Log output messages to the specified file
-o "c:\validationlog.txt"
```

Wenn diese Konfigurationsdatei als c:\config.txt gespeichert wird, kann sie folgendermaßen in einem Befehl verwendet werden:

```
dbvalid @c:\config.txt
```

**Bedingte syntaktische Analyse in Konfigurationsdateien**

Sie können die bedingte syntaktische Analyse in Konfigurationsdateien verwenden, um die Dienstprogramme anzugeben, die die Dateien verwenden können. Bedingte Direktiven ermöglichen es, dass Befehlsparameter abhängig vom die Datei benutzenden Dienstprogramm aufgenommen oder ausgeschlossen werden. Das Dienstprogramm zum Verschleiern von Dateien (dbfhide) kann weiterhin zum Verbergen des Inhalts einer Konfigurationsdatei verwendet werden, wenn eine bedingte syntaktische Analyse in der Datei durchgeführt wird.

**Syntax**

```
configuration-file= text...
```

*text* : *comment* | *conditional* | *command-line-option*

*comment* : *line starting with # that is not a conditional*

*conditional* :

```
#if condition
text
[ #elif condition
text
] ...
[ #else
text
] ...
#endif
```

*condition* : { **tool**=*utility-name*[,*utility-name*]... | *utility-name* }

Die folgenden Werte werden für *utility-name* unterstützt:

dbbackup	dbinfo	dbmlsync	dbstop	dbxtract
dbdsn	dbinit	dbping	dbsupport	mlsrv
dbeng	dblic	dbremote	dbsvc	mluser
dberase	dblocate	dbspawn	dbunload	qaagent
dbfhide	dblog	dbsrv	dbupgrad	mlstop
dbhist	dblsn	dbstats	dbvalid	

## Bemerkungen

Um als Direktive behandelt zu werden, muss das erste nicht-leer Zeichen in einer Zeile die Raute (#) sein. Wenn ein Dienstprogramm in einer #if- oder #elif-Direktive angetroffen wird, werden die der Direktive nachfolgenden Zeilen aufgenommen, bis eine andere bedingte Direktive angetroffen wird. Die #else-Direktive behandelt die Bedingung, wenn das Dienstprogramm nicht in den vorangehenden Blöcken gefunden wurde. Die #endif-Direktive schließt die Struktur der bedingten Direktive ab.

Leerstellen sind in der Liste von Dienstprogrammnamen, die von **tool=** angegeben werden, nicht zulässig. Sie können bedingte Direktiven verschachteln. Wenn ein Fehler während der syntaktischen Analyse der Konfigurationsdatei auftritt, meldet das Dienstprogramm, dass die Konfigurationsdatei nicht geöffnet werden kann.

Das Dienstprogramm dbspawn ermöglicht die Angabe einer Referenz einer Konfigurationsdatei im zu erstellenden Befehl, aber es ist nicht möglich, eine Konfigurationsdatei mit Optionen für das dbspawn-Dienstprogramm anzugeben. Der erste Befehl unten wird beispielsweise unterstützt, aber der zweite Befehl wird *nicht* unterstützt:

```
dbspawn dbeng16 @myconfig.ini
dbspawn @spawnopts.ini dbeng16 demo.db
```

**Siehe auch**

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Datenquellen-Dienstprogramm (dbdsn)“ auf Seite 905
- „@data -Datenbankserveroption“ auf Seite 214
- „Löschen-Dienstprogramm (dberase)“ auf Seite 916
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Histogramm-Dienstprogramm (dbhist)“ auf Seite 923
- „Informations-Dienstprogramm (dbinfo)“ auf Seite 925
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Dienstprogramm für die Serverlizenzierung (dblic)“ auf Seite 964
- „Dienstprogramm für die Serverauflistung (dblocate)“ auf Seite 960
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998
- „MobiLink Listener-Dienstprogramm für Windows-Geräte (dblsn)“ [*MobiLink - Serverinitiierte Synchronisation*]
- „dbmlsync-Syntax“ [*MobiLink - Clientadministration*]
- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „SQL Remote-Nachrichtenagent-Dienstprogramm (dbremote)“ [*SQL Remote*]
- „Dienstprogramm für den Serverstart im Hintergrund (dbspawn)“ auf Seite 983
- „Serverstopp-Dienstprogramm (dbstop)“ auf Seite 984
- „Dienstprogramm für Dienste (dbsvc) für Linux“ auf Seite 968
- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974
- „Dienstprogramm zum Entladen (dbunload)“ auf Seite 1000
- „Dienstprogramm zum Upgrade (dbupgrad)“ auf Seite 1017
- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „Extraktionsdienstprogramm (dbxtract)“ [*SQL Remote*]
- „mlsrv16-Syntax“ [*MobiLink - Serveradministration*]
- „Dienstprogramm für die MobiLink-Benutzerauthentifizierung (mluser)“ [*MobiLink - Serveradministration*]

**Beispiel**

Die folgende Konfigurationsdatei kann mit 'dbping', 'dbstop' und 'dbvalid' verwendet werden.

```
#if tool=dbping,dbstop,dbvalid
#always make tools quiet
-q
-c "UID=DBA;PWD=sql;Host=myhost;DBN=mydb"
#if dbping
#make a database connection
-d
#elif tool=dbstop
#don't ask
-y
#else
#must be dbvalid
#use WITH EXPRESS CHECK
-fx
#endif
#endif
```

## Sicherungsdienstprogramm (dbbackup)

Erstellt eine clientseitige oder serverseitige Sicherung von Datenbankdateien und Transaktionslogs für laufende Datenbanken.

### Syntax

**dbbackup** [ *options* ] *target-directory*

Option	Beschreibung
<i>@data</i>	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „ <a href="#">Konfigurationsdateien</a> “ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „ <a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a> “ auf Seite 922.
<b>-aw</b> [ - ]	Aktiviert die automatische Optimierung der Writer-Threads, sodass die Performance der Sicherung durch eine erhöhte Anzahl von Writer-Threads insgesamt verbessert werden kann. Das Angeben von -aw- deaktiviert die automatische Optimierung der Writer-Threads und verhindert, dass der Datenbankserver zusätzliche Writer-Threads erstellt. Die Optionen -aw und -aw- müssen mit der Option -s verwendet werden.
<b>-b</b> <i>block-size</i>	Gibt die maximale Blockgröße (in Anzahl von Seiten) an, die zur Übertragung von Seiten vom Datenbankserver an dbbackup verwendet wird. Das dbbackup-Dienstprogramm versucht, diese Anzahl von Seiten zuzuweisen. Wenn das fehlschlägt, vermindert es wiederholt diesen Wert um die Hälfte, bis die Zuweisung erfolgreich ist. Standardwert ist 128 Seiten.
<b>-bc</b> <i>Kommentar</i>	Erfasst einen Kommentar in der Sicherungsverlaufsdatei. Bei Archivsicherungen wird der Kommentar auch in der Archivdatei erfasst. Die Option -bc muss mit der Option -s verwendet werden.
<b>-c</b> " <i>key-word=value; ...</i> "	Legt Verbindungsparameter fest.
<b>-d</b>	Sichert nur die Hauptdatenbankdateien, ohne die Transaktionslogdatei (sofern vorhanden) zu sichern.
<b>-h</b> [ - ]	Aktiviert den Sicherungsverlauf, wodurch eine Zeile an die Datei <i>backup.syb</i> angehängt wird. Das Angeben von -h- deaktiviert den Sicherungsverlauf und verhindert Aktualisierungen der Datei <i>backup.syb</i> . Die Optionen -h und -h- müssen mit der Option -s verwendet werden.

Option	Beschreibung
<b>-k</b> <i>checkpoint-log-copy-option</i>	<p>Gibt an, wie dbbackup die Datenbankdateien verarbeitet, bevor sie in das Zielverzeichnis geschrieben werden. Die Entscheidung, entweder Pre-Images während einer Sicherung anzuwenden oder das Checkpoint-Log als Teil der Sicherung zu kopieren, wirkt sich auf die Performance aus. Wenn die Option -s angegeben ist, um eine auf dem Server durchgeführte Sicherung durchzuführen, ist die Standardeinstellung für -k "auto". Anderenfalls ist die Standardeinstellung "copy".</p> <p><b>auto</b> Der Datenbankserver überprüft die Menge des verfügbaren Speicherplatzes auf dem Datenträger, der das Sicherungsverzeichnis enthält. Wenn zumindest doppelt so viel Speicherplatz wie die Größe der Datenbank zum Start der Sicherung verfügbar ist, wird die Sicherung durchgeführt, als ob "copy" angegeben wurde. Anderenfalls wird sie durchgeführt, als ob "nocopy" angegeben wurde. Diese Einstellung kann nur verwendet werden, wenn ebenfalls die Option -s angegeben ist.</p> <p><b>copy</b> Die Sicherung liest die Datenbankdateien, ohne Pre-Images bei geänderten Seiten anzuwenden. Das gesamte Checkpoint-Log und der System-DBSpace werden in das Sicherungsverzeichnis kopiert. Beim nächsten Start der Datenbank stellt der Datenbankserver die Datenbank in dem Status wieder her, in dem sie beim Checkpoint zum Start der Sicherung war.</p> <p>Da keine Seiten-Pre-Images in die temporäre Datei geschrieben werden müssen, kann die Verwendung dieser Option zu einer besseren Sicherungsperformance führen und interne Server-Konfliktsituationen mit anderen Verbindungen vermindern, die während einer Sicherung betrieben werden. Da die Sicherungskopie der Datenbankdatei jedoch das Checkpoint-Log enthält, das Pre-Images von Seiten enthält, die seit dem Start der Sicherung geändert wurden, kann die Sicherungskopie der Datenbankdateien größer als die Datenbankdateien zum Zeitpunkt des Sicherungsstarts sein. Die Option copy sollte nur verwendet werden, wenn der Speicherplatz im Zielverzeichnis kein Problem darstellt.</p> <p><b>nocopy</b> Das Checkpoint-Log wird nicht als Teil der Sicherung kopiert. Diese Option bewirkt, dass Pre-Images von geänderten Dateien in der temporären Datei gespeichert werden, damit sie während des Sicherungsvorgangs angewendet werden können. Die Sicherungskopien der Datenbankdateien haben dieselbe Größe wie die Datenbank zum Zeitpunkt des Sicherungsstarts. Die Sicherungskopien können tatsächlich etwas kleiner sein, weil das Checkpoint-Log in der Kopie nicht enthalten ist. Diese Option führt zu kleineren gesicherten Datenbankdateien, aber die Sicherung braucht möglicherweise länger und kann die Performance von anderen Vorgängen im Datenbankserver beeinträchtigen. Sie ist in Situationen nützlich, bei denen der Speicherplatz auf dem Ziellaufwerk beschränkt ist.</p> <p><b>recover</b> Der Datenbankserver kopiert das Checkpoint-Log (wie bei der Option copy), wendet aber das Checkpoint-Log an der Datenbank an, wenn die Sicherung abgeschlossen ist. Dies stellt die gesicherten Datenbankdateien im selben Status (und derselben Größe) wieder her, in der sie beim Start des Sicherungsvorgangs waren. Diese Option kann nützlich sein, wenn der Speicherplatz auf dem</p>

Option	Beschreibung
	Sicherungslaufwerk beschränkt ist (sie benötigt dieselbe Menge an Speicherplatz wie die copy-Option zum Sichern des Checkpoint-Logs, aber die resultierende Dateigröße ist kleiner). Diese Einstellung kann nur verwendet werden, wenn ebenfalls die Option -s angegeben ist.
<b>-l filename</b>	<p>Damit kann ein Sekundärsystem rasch aktiviert werden, wenn ein Server ausfällt. Eine Live-Sicherung stoppt nicht. Sie läuft, solange der Server läuft. Sie läuft, bis der Primärserver nicht mehr verfügbar ist. Zu diesem Zeitpunkt wird sie beendet, die gesicherte Logdatei ist aber funktionsfähig und kann dazu verwendet werden, ein zweites System schnell zu starten. Siehe <a href="#">„Unterschiede zwischen Live-Sicherungen und Transaktionslogspiegeldateien“ auf Seite 1033</a> und <a href="#">„Live-Sicherungen erstellen“ auf Seite 1044</a>.</p> <p>Wenn Sie die Option -l angeben, dürfen Sie nicht die Option -s verwenden, um auf dem Server eine Sicherungskopie durchzuführen.</p>
<b>-n</b>	<p>Ändert die Namenskonvention für die Sicherungs-Transaktionslogdatei in <i>jmmmtxx.log</i>, wobei <i>xx</i> aufeinanderfolgende Buchstaben von <b>AA</b> bis <b>ZZ</b> sind und <i>jmmmtt</i> den aktuellen Wert für Jahr, Monat und Tag darstellt. Diese Option wird mit -r verwendet.</p> <p>Die Sicherungskopie der Transaktionslogdatei wird im Verzeichnis gespeichert, das in der Befehlszeile unter Verwendung der <i>jmmmtxx.log</i>-Namenskonvention festgelegt wurde. Dadurch können Sicherungen von mehreren Versionen der Transaktionslogdatei im gleichen Sicherungsverzeichnis aufbewahrt werden.</p> <p>Sie können auch die Optionen -x und -n verwenden, um die Logkopie umzubenennen. Zum Beispiel:</p> <pre>dbbackup -c "UID=DBA;PWD=sql" -x -n mybackupdir</pre>
<b>-o filename</b>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-p</b>	<p>Sendet formatierte Meldungen zum Verarbeitungsfortschritt vom Datenbankserver an den Client.</p> <p>Die Option -p wird ignoriert, es sei denn die Option -s wird für eine serverseitige Sicherung verwendet.</p> <p>Weitere Hinweise zu formatierten Meldungen zum Verarbeitungsfortschritt finden Sie unter <a href="#">„progress_messages-Option“ auf Seite 657</a>.</p>
<b>-q</b>	Unterdrückt die Ausgabe von Meldungen. Diese Option ist nur verfügbar, wenn Sie dieses Dienstprogramm über eine Eingabeaufforderung ausführen.

Option	Beschreibung
<b>-r</b>	<p>Benennt das Transaktionslog um und startet ein neues Transaktionslog. Erzwingt einen Checkpoint und bewirkt die folgenden drei Schritte:</p> <ol style="list-style-type: none"> <li>1. Die aktuell arbeitende Transaktionslogdatei wird kopiert und in dem in der Befehlszeile festgelegten Verzeichnis gespeichert.</li> <li>2. Das aktuelle Transaktionslog bleibt in seinem aktuellen Verzeichnis, wird jedoch unter Verwendung des Formats <i>jmmmtt.xx.log</i> umbenannt, wobei <i>xx</i> aufeinanderfolgende Buchstaben von AA bis ZZ sind und <i>jmmmtt</i> den aktuellen Wert für Jahr, Monat und Tag darstellt. Diese Datei ist dann nicht mehr das aktuelle Transaktionslog.</li> <li>3. Eine neue Transaktionslogdatei wird erstellt, die keine Transaktionen enthält. Sie wird nach der Datei benannt, die zuvor das aktuelle Transaktionslog war und dann vom Datenbankserver als aktuelles Transaktionslog verwendet wird.</li> </ol>
<b>-s</b>	<p>Erstellt eine Sicherungskopie auf dem Server mit der BACKUP DATABASE-Anweisung. Wenn Sie die Option -s angeben, darf die Option -l (zum Erstellen einer Live-Sicherung des Transaktionslogs) nicht benutzt werden. Die Verzeichnisangabe erfolgt ausgehend vom aktuellen Serververzeichnis, deshalb wird empfohlen, einen vollständigen Pfadnamen anzugeben. Außerdem muss der Server über Schreibberechtigung für das angegebene Verzeichnis verfügen. Wenn die Option -s angegeben wird, zeigt das Sicherungsdienstprogramm keine Fortschrittsanzeige an und fordert nicht zur Bestätigung auf, bevor vorhandene Dateien überschrieben werden. Wenn Sie vor dem Überschreiben vorhandener Dateien zur Bestätigung aufgefordert werden möchten, dürfen Sie weder -s noch -y angeben. Sie müssen -s angeben, wenn Sie die Wiederherstellungsoption -k angeben.</p>
<b>-t</b>	<p>Erstellt eine Sicherung, die als inkrementelle Sicherung verwendet werden kann, da das Transaktionslog auf die letzte gesicherte Kopie der Datenbankdatei(en) angewendet werden kann.</p>
<b>-wa</b>	<p>Wartet, bis die Transaktionen abgeschlossen sind, um das Transaktionslog umzubenennen oder zu kürzen. Die Option -wa muss mit der Option -s verwendet werden.</p>
<b>-wb</b>	<p>Verzögert die Sicherung der Datenbank, bis keine aktiven Transaktionen mehr vorhanden sind. Die Option -wb muss mit der Option -s verwendet werden.</p>
<b>-x</b>	<p>Sichert das vorhandene Transaktionslog, das ursprüngliche Transaktionslog wird gelöscht und ein neues wird gestartet. Verwenden Sie diese Option nicht, wenn Sie mit einer Datenbankspiegelung arbeiten. Siehe „<a href="#">Verwaltung von Transaktionslogdateien in einem Datenbankspiegelungssystem</a>“ auf Seite 1484.</p>

Option	Beschreibung
<b>-xo</b>	<p>Löscht das aktuelle Transaktionslog und startet ein neues. Dieser Vorgang führt keine Sicherung durch, da er ausschließlich bezweckt, in Nicht-Replikationsumgebungen Speicherplatz freizugeben. Verwenden Sie diese Option nicht, wenn Sie mit einer Datenbankspiegelung arbeiten. Siehe „<a href="#">Verwaltung von Transaktionslogdateien in einem Datenbankspiegelungssystem</a>“ auf Seite 1484.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>Vorsicht</b>  Wenn Sie diese Option verwenden, kann dies zu einer Datenbank führen, die nach einem Datenträgerfehler nicht wiederhergestellt werden kann. Verwenden Sie diese Option nur, wenn Datenverluste akzeptabel sind.</p> <p>Verwenden Sie die Option -xo nicht bei Datenbanken, die repliziert oder synchronisiert werden. SQL Remote und MobiLink stützen sich auf die Informationen aus dem Transaktionslog.</p> </div>
<b>-y</b>	Erstellt das Sicherungsverzeichnis ohne Ihre Bestätigung oder ersetzt eine frühere Sicherungsdatei im Verzeichnis ohne Ihre Bestätigung. Wenn Sie vor dem Überschreiben vorhandener Dateien zur Bestätigung aufgefordert werden möchten, dürfen Sie weder -s noch -y angeben.
<i>target-directory</i>	Gibt das Verzeichnis an, in das die Sicherungsdateien kopiert werden. Wenn das Verzeichnis nicht existiert, wird es erstellt. Das übergeordnete Verzeichnis muss allerdings bereits bestehen. Standardmäßig erstellt das Sicherungsdienstprogramm eine clientseitige Sicherung der Datenbankdateien. Um eine Sicherung auf dem Server zu erstellen, verwenden Sie die Anweisung BACKUP DATABASE mit der Option -s.

## Privilegien

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

## Bemerkungen

Das Sicherungsdienstprogramm stellt eine Sicherungskopie von allen Dateien einer einzelnen Datenbank her. Eine einfache Datenbank besteht aus zwei Dateien: der Haupt-Datenbankdatei und dem Transaktionslog. Kompliziertere Datenbanken können Tabellen in mehreren Dateien speichern, wobei jede Datei ein eigener DBSpace ist. Alle Sicherungsdateien heißen genauso wie die Datenbankdateien. Die vom Sicherungsdienstprogramm erstellte Sicherungskopie umfasst für jede gesicherte Datei eine separate Datei.

Weitere Hinweise zum Erstellen von Archivsicherungen (eine einzige Datei, die sowohl Datenbankdatei als auch Transaktionslog enthält) finden Sie unter „[Archivsicherungen](#)“ auf Seite 1034.

Das Verwenden des Sicherungsdienstprogramms auf einer laufenden Datenbank entspricht dem Kopieren der Datenbankdateien, wenn die Datenbank nicht läuft. Sie können das Sicherungsdienstprogramm zum Sichern der Datenbank ausführen, während andere Anwendungen oder Benutzer sie verwenden.

Wenn keine der Optionen -d oder -t verwendet wird, werden alle Datenbankdateien gesichert.

Standardmäßig erstellt das Sicherungsdienstprogramm eine clientseitige Sicherung der Datenbankdateien. Um eine Sicherung auf dem Server zu erstellen, verwenden Sie die Anweisung BACKUP DATABASE mit der Option -s.

Weitere Hinweise zur Durchführung von serverseitigen Sicherungen finden Sie unter „[BACKUP-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

**Vorsicht**

Sicherungskopien der Datenbank und des Transaktionslogs dürfen auf keinen Fall geändert werden. Wenn während der Sicherung keine Transaktionen aktiv waren oder Sie BACKUP DATABASE WITH CHECKPOINT LOG RECOVER oder WITH CHECKPOINT LOG NO COPY angegeben haben, können Sie die Validität der Sicherungsdatenbank im Schreibschutzmodus prüfen, oder indem Sie eine Kopie der Sicherungsdatenbank validieren.

Wenn jedoch Transaktionen aktiv waren oder Sie BACKUP DATABASE WITH CHECKPOINT LOG COPY angegeben haben, muss der Datenbankserver eine Wiederherstellung der Datenbank bei ihrem Start durchführen. Die Wiederherstellung ändert die Sicherungskopie, und das sollte vermieden werden.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag).

Weitere Informationen zu Beendigungscode finden Sie unter „[Exit-Codes der Softwarekomponenten](#)“ [*SQL Anywhere Server - Programmierung*].

**Beispiel**

Der folgende Befehl sichert zum Beispiel die Beispieldatenbank, die auf dem Computer "sample\_host" läuft, im Verzeichnis *SQLAnybackup*. Hierzu wird eine Verbindung als DBA-Benutzer hergestellt:

```
dbbackup -c "Host=sample_host;DBN=demo;UID=DBA;PWD=sql" SQLAnybackup
```

**Siehe auch**

- „Sicherung und Datenwiederherstellung“ auf Seite 1027
- „Sicherungskopien“ auf Seite 1035
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Broadcast Repeater-Dienstprogramm (dbns16)

Ermöglicht es Clients, SQL Anywhere-Datenbankserver zu finden, die in anderen Subnetzen und hinter Firewalls laufen, wo sie von UDP-Broadcasts normalerweise nicht erreicht werden.

**Syntax**

```
dbns16 [ options ] [ address ... ]
```

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
-ap port	Gibt die vom Datenbankserver verwendete Portnummer an. Die Standard-Portnummer ist 2638.
-m ip	Gibt die IP-Adresse des Computers an, auf dem der DBNS-Prozess läuft. Dieser Parameter ist bei Computern mit mehr als einer IP-Adresse erforderlich. Diese Adresse muss eine IPv4-Adresse sein.
-o filename	Schreibt die Ausgabe, die im Broadcast Repeater-Meldungsfenster angezeigt wird, in die benannte Datei.
-p port	Gibt die Portnummer an, die vom DBNS Broadcast Repeater verwendet wird. Der Standardwert ist 3968. Wenn es Firewalls zwischen den Subnetzen gibt, müssen Sie die vom Broadcast Repeater-Dienstprogramm verwendete Portnummer für TCP-Verbindungen zwischen DBNS-Prozessen ebenso wie den Port 2638 für Standard-Client/Server-Kommunikation öffnen.
-q	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
-s	Veranlasst den neuen DBNS-Prozess, zu prüfen, ob ein anderer DBNS-Prozess auf diesem Teilnetz bereits läuft, und gibt, bevor er herunterfährt, einen Fehler zurück, wenn ein anderer DBNS-Prozess gefunden wird.
-ud	<p>(Nur Unix) Führt den DBNS Broadcast Repeater unter Unix-Betriebssystemen als Daemon aus. Wenn Sie den DBNS Broadcast Repeater als Daemon ausführen, ist es empfehlenswert, die Option -o zur Protokollierung der Ausgaben zu verwenden.</p> <p>Wenn Sie den Datenbankserver als Dämon starten, werden seine Berechtigungen durch die umask-Einstellung des aktuellen Benutzers gesteuert. Es wird empfohlen, den umask-Wert vor dem Start des DBNS Broadcast Repeaters festzulegen, um sicherzustellen, dass der Datenbankserver die entsprechenden Berechtigungen hat.</p>
-ui	(Nur Unix) Startet den DBNS Broadcast Repeater unter Linux mit X Window-Serverunterstützung im Shell-Modus, wenn keine verwendbare Anzeige verfügbar ist.
-ux	(Nur Unix) Öffnet das Fenster <b>SQL Anywhere Broadcast Repeater</b> unter Linux. (Verwenden Sie den X Window-Server.)

Option	Beschreibung
<b>-x host</b>	Führt den DBNS-Prozess herunter, der auf dem angegebenen Host läuft. Sie können eine IP-Adresse oder einen Hostnamen angeben.
<b>-z</b>	Startet den DBNS Broadcast Repeater im Debug-Modus. Im Fehlersuchmodus wird im Fenster " Broadcast Repeater-Meldungen" eine Zeile für jedes SQL Anywhere Broadcast-Paket angezeigt, das empfangen und weitergeleitet wird. Der Fehlersuchmodus sollte aufgrund der Ausführlichkeit seiner Ausgabe nur verwendet werden, wenn es Systemanbindungsprobleme gibt.
<i>address</i>	Gibt die IP-Adresse oder den Hostnamen von anderen Computern an, die DBNS-Prozesse ausführen oder ausführen werden. Dies ermöglicht es DBNS-Prozessen, einander zu erkennen und Informationen über bekannte Datenbankserver und andere DBNS-Prozesse auszutauschen.

### Privilegien

Keine.

### Bemerkungen

Mit dem Broadcast Repeater können SQL Anywhere-Clients auch SQL Anywhere-Datenbankserver finden, die in anderen Subnetzen und hinter Firewalls laufen, wo sie von UDP-Broadcasts ohne Host-Verbindungsparameter oder LDAP normalerweise nicht erreicht werden.

*address* kann entweder eine IP-Adresse oder ein Computernamen sein. Verwenden Sie Leerstellen, um mehrere Adressen voneinander zu trennen.

Dieses Dienstprogramm ist auf unterstützten Unix- und allen 32-Bit- und 64-Bit-Windows-Plattformen verfügbar.

Die Clients und Datenbankserver müssen 9.0.2 oder später ausführen, um den SQL Anywhere Broadcast Repeater zu verwenden.

#### Vorsicht

Es wird empfohlen, das dbns16-Dienstprogramm nicht auf einem Computer auszuführen, auf dem ein SQL Anywhere-Datenbankserver läuft, weil es möglich ist, dass dbns oder der Datenbankserver keine UDP-Broadcasts empfängt.

### Siehe auch

- „Fehlerbehandlung: Datenbankserver mithilfe des Broadcast Repeater-Dienstprogramms suchen“ auf Seite 85

### Beispiel

Nehmen wir an, Sie wollen es Computern auf den Subnetzen 10.50.83.255 und 10.50.125.255 ermöglichen, eine Verbindung mithilfe von Broadcasts herzustellen. Sie benötigen einen Computer auf dem Subnetz 10.50.83.255 (Computer A auf 10.50.83.114) und einen auf dem Subnetz 10.50.125.255 (Computer B auf 10.50.125.103).

Führen Sie auf beiden Computern dbns16 aus, um die IP-Adresse des anderen Computers zu übergeben.  
Führen Sie den folgenden Befehl auf Computer A aus:

```
dbns16 10.50.125.103
```

Führen Sie auf Computer B den folgenden Befehl aus:

```
dbns16 10.50.83.114
```

Wenn einer der beiden Computer mehr als eine IP-Adresse hat, müssen Sie die lokale IP-Adresse mithilfe der Option -m angeben.

Führen Sie auf Computer A den folgenden Befehl aus:

```
dbns16 -m 10.50.83.114 10.50.125.103
```

# Dienstprogramm zum Erstellen von Zertifikaten [createcert)

Erstellt X.509-Zertifikate.

## Syntax

**createcert** [ -r | -s ]

Option	Name der Eingabeaufforderung	Beschreibung
@data	k.A.	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „Konfigurationsdateien“ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, wenden Sie das Dienstprogramm zum Verschleiern von Dateien (dbfhide) auf die Konfigurationsdatei an. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922.
-b value	Länge des RSA-Schlüssels eingeben (512-16384)	Gibt die Länge des RSA-Schlüssels an. Die Länge kann zwischen 512 und 16384 Bit liegen.  Diese Option wird ignoriert, wenn die Option -s angegeben ist.

Option	Name der Eingabeaufforderung	Beschreibung
<b>-c</b> <i>filename</i>	<b>Dateipfad des Zertifikats des Signierenden eingeben</b>	<p>Gibt einen Speicherort und einen Dateinamen für das Zertifikat des Signierenden an.</p> <p>Wenn Sie diese Informationen angeben, ist das generierte Zertifikat ein signiertes Zertifikat. Wenn Sie diese Informationen nicht angeben, ist das generierte Zertifikat ein selbstsigniertes Stammzertifikat.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>
<b>-ca</b> {0 / 1}	<b>Zertifizierungsstelle FALSE (0) oder TRUE (1)</b>	<p>Erstellt ein Zertifizierungsstellen-Zertifikat, das zum Signieren anderer Zertifikate verwendet werden kann. Standardmäßig sind Zertifikate keine Zertifizierungsstellen (0).</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>
<b>-ck</b> <i>filename</i>	<b>Dateipfad des privaten Schlüssels des Signierenden eingeben</b>	<p>Ein Speicherort und ein Dateiname zum Speichern des privaten Schlüssels, der der Zertifikatanforderung zugeordnet ist. Diese Eingabeaufforderung wird nur angezeigt, wenn Sie für die Option -c einen Dateinamen angeben.</p>
<b>-co</b> <i>filename</i>	<b>Dateipfad zum Speichern des Zertifikats eingeben</b>	<p>Schreibt das öffentliche Zertifikat in die angegebene Datei.</p> <p>Geben Sie einen Speicherort und einen Dateinamen zum Speichern des Zertifikats an. Andernfalls wird das Zertifikat nicht gespeichert.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>

Option	Name der Eingabeaufforderung	Beschreibung
<b>-cp</b> <i>password</i>	<b>Kennwort für den privaten Schlüssel des Signierenden eingeben</b>	<p>Gibt das Kennwort ein, das verwendet wurde, um den privaten Schlüssel des Signierenden zu verschlüsseln.</p> <p>Dieses Kennwort muss nur angegeben werden, wenn der private Schlüssel verschlüsselt wurde.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>
<b>-io</b> <i>filename</i>	<b>Dateipfad zum Speichern der Identität eingeben</b>	<p>Gibt einen Speicherort und einen Dateinamen zum Speichern der generierten Identität an.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>
<b>-ko</b> <i>filename</i>	<b>Dateipfad zum Speichern des privaten Schlüssels eingeben</b>	<p>Gibt einen Speicherort und einen Dateinamen zum Speichern des privaten Schlüssels an.</p>
<b>-kp</b> <i>password</i>	<b>Kennwort zum Schutz des privaten Schlüssels eingeben</b>	<p>Gibt ein Kennwort zum Verschlüsseln des privaten Schlüssels an.</p> <p>Wenn Sie kein Kennwort angeben, wird der private Schlüssel nicht verschlüsselt. Diese Option gilt nur, wenn Sie mit der Option -ko einen Dateinamen angeben.</p>
<b>-m</b> <i>value</i>	<b>Seriennummer</b>	<p>Gibt eine Seriennummer an. Die Seriennummer muss eine hexadezimale Zeichenfolge aus 40 Ziffern oder weniger sein. Diese Nummer muss unter allen vom aktuellen Signierenden signierten Zertifikaten eindeutig sein. Wenn Sie keine Seriennummer angeben, generiert createcert eine GUID als Seriennummer.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>

Option	Name der Eingabeaufforderung	Beschreibung
<b>-p1</b>	k.A.	Verwendet PKCS #1 statt des Standardwerts PKCS #8, um unverschlüsselte private RSA-Schlüssel zu kodieren.
<b>-r</b>	k.A.	Generiert eine PKCS #10-Zertifikatanforderung.  Wenn diese Option angegeben ist, gelten die folgenden Optionen nicht: <ul style="list-style-type: none"> <li>• -c</li> <li>• -ca</li> <li>• -ck</li> <li>• -co</li> <li>• -cp</li> <li>• -m</li> <li>• -io</li> <li>• -u</li> <li>• -x</li> <li>• -v</li> </ul>
<b>-ro</b> <i>filename</i>	<b>Dateipfad zum Speichern der Anforderung</b>	Gibt einen Speicherort und einen Dateinamen zum Speichern der PCKS #10-Zertifikatanforderung an.  Diese Option gilt nur, wenn Sie die Option -r angeben.

Option	Name der Eingabeaufforderung	Beschreibung
<b>-s</b> <i>filename</i>	k.A.	<p>Gibt den Speicherort und den Dateinamen der zu signierenden PKCS10-Zertifikatanforderung an. Die Zertifikatanforderung kann DER- oder PEM-kodiert sein. Wenn diese Option angegeben ist, gelten die folgenden Optionen nicht:</p> <ul style="list-style-type: none"> <li>● -b</li> <li>● -ec</li> <li>● -sc</li> <li>● -scn</li> <li>● -sl</li> <li>● -so</li> <li>● -sou</li> <li>● -sst</li> <li>● -t</li> <li>● -x</li> </ul>
<b>-sa</b> <i>value</i>	k.A.	<p>Legt fest, welcher der folgenden Signaturalgorithmen verwendet werden soll: sha1, sha256, sha384 oder sha512.</p> <p>Der Standardalgorithmus ist sha256.</p>
<b>-sc</b> <i>value</i>	<b>Betreffinformationen</b>	<p>Gibt den Landescode für den Betreff an.</p> <p>Diese Option wird ignoriert, wenn die Option -s angegeben ist.</p>
<b>-scn</b> <i>value</i>	<b>Betreffinformationen</b>	<p>Gibt den Namen für den Betreff an.</p> <p>Diese Option wird ignoriert, wenn die Option -s angegeben ist.</p>
<b>-sl</b> <i>value</i>	<b>Betreffinformationen</b>	<p>Gibt den Ort für den Betreff an.</p> <p>Diese Option wird ignoriert, wenn die Option -s angegeben ist.</p>

Option	Name der Eingabeaufforderung	Beschreibung
<b>-so</b> <i>value</i>	<b>Betreffinformationen</b>	Gibt die Organisation für den Betreff an.  Diese Option wird ignoriert, wenn die Option -s angegeben ist.
<b>-sou</b> <i>value</i>	<b>Betreffinformationen</b>	Gibt die Organisationseinheit für den Betreff an.  Diese Option wird ignoriert, wenn die Option -s angegeben ist.
<b>-sst</b> <i>value</i>	<b>Betreffinformationen</b>	Gibt das Bundesland bzw. den Kanton für den Betreff an.  Diese Option wird ignoriert, wenn die Option -s angegeben ist.
<b>-t</b> <i>type</i>	<b>Verschlüsselungstyp wählen ((R)SA oder (E)CC)</b>	Gibt den Verschlüsselungstyp an. Geben Sie RSA an.  Diese Option wird ignoriert, wenn die Option -s angegeben ist.

Option	Name der Eingabeaufforderung	Beschreibung
<b>-u</b> <i>value,...</i>	<b>Schlüsselsyntax</b>	<p>Gibt an, wie das Zertifikat verwendet werden soll.</p> <p>Geben Sie eine kommasetrennte Liste von Zahlen an, die festlegen, wie der private Schlüssel des Zertifikats verwendet werden kann. Dies ist eine erweiterte Option. Der Standardwert sollte in den meisten Fällen akzeptabel sein. Der Standardwert hängt davon ab, ob das Zertifikat eine Zertifizierungsstelle ist. Der Standardwert für ein Zertifikat mit Zertifizierungsstelle ist <b>6,7</b>. Der Standardwert für ein Zertifikat ohne Zertifizierungsstelle ist <b>3,4,5</b>.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p> <p>Werte sind:</p> <ul style="list-style-type: none"> <li>• 1. Digitale Signatur</li> <li>• 2. Unleugbarkeit</li> <li>• 3. Schlüsselchiffrierung</li> <li>• 4. Datenverschlüsselung</li> <li>• 5. Schlüsselübereinstimmung</li> <li>• 6. Zertifikatsignierung</li> <li>• 7. CRL-Signierung</li> <li>• 8. Nur verschlüsseln</li> <li>• 9. Nur entschlüsseln</li> </ul>
<b>-v</b> <i>years</i>	<b>Zertifikat gültig für wie viele Jahre (1-100)</b>	<p>Gibt die Anzahl der Jahre (zwischen 1 und 100) an, die das Zertifikat gültig ist. Nach diesem Zeitraum läuft das Zertifikat, zusammen mit allen von ihm signierten Zertifikaten, ab.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>
<b>-x</b>	k.A.	<p>Generiert ein selbstsigniertes Zertifikat.</p> <p>Diese Option wird ignoriert, wenn die Option -r angegeben ist.</p>

## Privilegien

Keine.

## Bemerkungen

Benutzer wenden sich normalerweise an Drittanbieter, um Zertifikate zu erwerben. Diese Zertifizierungsstellen stellen ihre eigenen Tools zur Erstellung von Zertifikaten zur Verfügung. Die folgenden Tools sind möglicherweise bei der Erstellung von Zertifikaten für Entwicklungs- und Testzwecke besonders nützlich und können auch für Produktionszertifikate verwendet werden.

Um ein signiertes Zertifikat zu erstellen, können Sie keine Optionen angeben und sich von createcert zur Eingabe der erforderlichen Werte auffordern lassen. Sie können auch die erforderlichen Optionen für Ihr Zertifikat angeben.

Wenn Sie den Prozess in zwei Schritte aufteilen möchten, damit z.B. eine Person eine Anforderung erstellt und eine zweite sie signiert, kann die erste Person createcert mit der Option -r ausführen, um die Anforderung zu erstellen, und die zweite Person kann createcert mit der Option -s ausführen, um die Anforderung zu signieren.

Wenn Sie ein Unternehmensstammzertifikat (ein Zertifikat, das andere Zertifikate signiert) erstellen möchten, ist es empfehlenswert, das selbstsignierte Stammzertifikat mit Zertifizierungsstelle zu erstellen und die Standardsignierung zu verwenden. Geben Sie beispielsweise **y** für die Option **-ca** an und **6,7** für die Option **-u**.

Wenn Sie ein Unternehmensstammzertifikat (ein Zertifikat, das andere Zertifikate signiert) generieren möchten, ist es empfehlenswert, das selbstsignierte Stammzertifikat mit Zertifizierungsstelle zu erstellen und die Standardsignierung zu verwenden.

## Beispiel

Im folgenden Beispiel wird ein selbstsigniertes Zertifikat mit den folgenden Merkmalen erstellt:

- 1024-Bit-RSA-Schlüssel
- Generierte Seriennummer
- Gültig für 5 Jahre
- Keine Zertifizierungsstelle
- Verwendet für Schlüsselchiffrierung, Datenchiffrierung und Schlüsselübereinstimmung
- Privater Schlüssel mit dem Kennwort "sql"

```
createcert.exe -t rsa -b 1024 -sc CA -sst ON -sl Waterloo -so  
MyOrganizationalUnit -sou MyCompany -scn test -x -m 0 -v 5 -ca 0 -u 3,4,5 -  
co root-cert.pem -ko root-key.pem -io root-id.pem -kp sql
```

Im folgenden Beispiel wird ein durch Zertifizierungsstellenschlüssel signiertes Zertifikat mit den folgenden Merkmalen erstellt:

- 1024-Bit-RSA-Schlüssel

- Generierte Seriennummer
- Gültig für 5 Jahre
- Keine Zertifizierungsstelle
- Verwendet für Schlüsselchiffrierung, Datenchiffrierung und Schlüsselübereinstimmung
- Privater Schlüssel mit dem Kennwort "sql":

```
createcert.exe -t rsa -b 1024 -sc CA -sst ON -sl Waterloo -so  
MyOrganizationalUnit -sou MyCompany -scn test -c ca-cert.pem -ck ca-key.pem -  
cp cakeypass -m 0 -v 5 -ca 0 -u 3,4,5 -co root-cert.pem -ko root-key.pem -io  
root-id.pem -kp sql
```

Das folgende Beispiel erstellt ein signiertes Zertifikat. Da in diesem Beispiel kein Dateiname für das Zertifikat des Signierenden angegeben wird, handelt es sich um ein selbstsigniertes Stammzertifikat.

```
createcert  
SQL Anywhere-Dienstprogramm zum Generieren von X.509-Zertifikaten Version  
16.0.3330  
Verschlüsselungstyp wählen ((R)SA oder (E)CC): r  
Länge des RSA-Schlüssels eingeben (512-16384): 1024  
Schlüsselpaar wird generiert...  
Landescode: CA  
Bundesland/Kanton: Ontario  
Ort: Waterloo  
Organisation: Sybase iAnywhere  
Organisationseinheit: Engineering  
Name: Test Certificate  
Dateipfad des Zertifikats des Signierenden eingeben:  
Zertifikat ist ein selbstsignierter Stamm  
Seriennummer [GUID generieren]:  
Generierte Seriennummer: bfb89a26fb854955954cabcd056e177  
Zertifikat gültig für wie viele Jahre (1-100): 10  
Zertifizierungsstelle (J/N) [N]: n  
1. Digitale Signatur  
2. Unleugbarkeit  
3. Schlüsselchiffrierung  
4. Datenverschlüsselung  
5. Schlüsselübereinstimmung  
6. Zertifikatsignierung  
7. CRL-Signierung  
8. Nur verschlüsseln  
9. Nur entschlüsseln  
Schlüsselsyntax [3,4,5]: 3,4,5  
Dateipfad zum Speichern des Zertifikats eingeben: cert.pem  
Dateipfad zum Speichern des privaten Schlüssels eingeben: key.pem  
Kennwort zum Schutz des privaten Schlüssels eingeben: pwd  
Dateipfad zum Speichern der Identität eingeben: id.pem
```

Im folgenden Beispiel wird ein Unternehmensstammzertifikat (ein Zertifikat, das andere Zertifikate signiert) erstellt, bei dem es sich um ein selbstsigniertes Stammzertifikat mit Zertifizierungsstelle handelt und für das die Standardsignierung verwendet wird. Die Antwort auf die Eingabeaufforderung **Zertifizierungsstelle** bzw. die Option -ca sollte **y** sein und die Antwort auf die Eingabeaufforderung **Schlüsselsyntax** bzw. die Option -u **6,7** (Standardeinstellung).

```
Zertifizierungsstelle (J/N) [N]: y  
1. Digitale Signatur
```

2. Unleugbarkeit
  3. Schlüsselchiffrierung
  4. Datenchiffrierung
  5. Schlüsselübereinstimmung
  6. Zertifikatsignierung
  7. CRL-Signierung
  8. Nur verschlüsseln
  9. Nur entschlüsseln
- Schlüsselsyntax [6,7]: 6,7

### Siehe auch

- [Zertifikate auf Seite 1444](#)
- [„Dienstprogramm zum Anzeigen von Zertifikaten \(viewcert\)“ auf Seite 903](#)
- [„Datenbankserveroption -ec “ auf Seite 230](#)
- [„Verbindungsparameter Encryption \(ENC\)“ auf Seite 359](#)
- [„FIPS-zertifizierte Verschlüsselungstechnologie“ auf Seite 1445](#)

## Dienstprogramm zum Anzeigen von Zertifikaten (viewcert)

Zeigt Werte innerhalb eines Public Key Infrastructure-Objekts (PKI) an, konvertiert die Kodierung von PKI-Objekten oder ver- und entschlüsselt private Schlüssel.

### Syntax

**viewcert** [ *options* ] *input-file*

Option	Beschreibung
<b>@data</b>	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe <a href="#">„Konfigurationsdateien“ auf Seite 882</a> .  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, wenden Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei an. Siehe <a href="#">„Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922</a> .
<b>-d</b>	DER verschlüsselt die Ausgabe. Diese Option ist nur zusammen mit der Option -o sinnvoll. Sie kann nicht mit -p verwendet werden. Standardmäßig gibt viewcert das PKI-Objekt in einem lesbaren Textformat aus.
<b>-ip input-password</b>	Gibt das Kennwort an, das erforderlich ist, um den privaten Schlüssel zu entschlüsseln, wenn die <i>Eingabedatei</i> einen verschlüsselten privaten Schlüssel enthält.
<b>-o filename</b>	Gibt die Datei an, in die viewcert die Ausgabedaten schreiben soll. Standardmäßig schreibt viewcert Ausgabedaten in das Fenster der Eingabeaufforderung, in der das Programm läuft.
<b>-op output-password</b>	Gibt das Kennwort an, das viewcert verwenden muss, um einen privaten Schlüssel zu verschlüsseln. Diese Option ist nur mit -d oder -p sinnvoll. Standardmäßig werden private Schlüssel nicht verschlüsselt.

Option	Beschreibung
<b>-p</b>	PEM verschlüsselt die Ausgabe. Diese Option ist nur zusammen mit der Option -o sinnvoll. Sie kann nicht mit -d verwendet werden. Standardmäßig gibt viewcert das PKI-Objekt in einem lesbaren Textformat aus.
<b>-p1</b>	Verwendet PKCS #1 statt des Standardwerts PKCS #8, um unverschlüsselte private RSA-Schlüssel zu kodieren.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<i>input-file</i>	Gibt eine Datei an, die ein DER- oder PEM-kodiertes PKI-Objekt sein muss.

### Privilegien

Keine.

### Bemerkungen

Mit dem viewcert-Dienstprogramm können Sie die folgenden Typen von PKI-Objekten anzeigen:

- X.509-Zertifikate
- Zertifikatanforderungen
- Private Schlüssel
- Zertifikatsperrlisten (CRLs)

Mit viewcert können Sie auch zwischen DER- und PEM-Kodierungstypen konvertieren und private Schlüssel ver- bzw. entschlüsseln.

Das Dienstprogramm viewcert unterstützt RSA-Objekte.

### Siehe auch

- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894
- „Getrennt lizenzierbare Komponenten“ [SQL Anywhere 16 - Einführung]

### Beispiel

Das folgende Beispiel ermöglicht es Ihnen, das in SQL Anywhere enthaltene RSA-Beispielzertifikat anzuzeigen. Führen Sie im Verzeichnis `%SQLANYSAM16%\Certificates` den folgenden Befehl aus:

```
viewcert rsaroot.crt
```

Dieses Beispiel bewirkt die folgende Ausgabe:

```
SQL Anywhere-Dienstprogramm zum Anzeigen von X.509-Zertifikaten Version
16.0.0.1403

X.509-Zertifikat
-----
Name:                RSA Root
Landescode:          test
Bundesland/Kanton:   test
Ort:                 test
```

```

Organisation:          test
Organisationseinheit:  test
Aussteller:            RSA Root
Seriennummer:          89e3f123dcb74624a9ae78a845ccd183
Ausgestellt:           Jan 29, 2012  11:45:00
Ablauf:                Jan 30, 2032  11:45:00
Signaturalgorithmus:   RSA, SHA1
Schlüsseltyp:          RSA
Schlüsselgröße:        2048 Bit
Grundlegende Integritätsregeln: Ist eine Zertifizierungsstelle,
Beschränkung der Pfadlänge: 10
Schlüsselsyntax:       Zertifikat-Signierung, CRL-Signierung

```

## Datenquellen-Dienstprogramm (dbdsn)

Erstellt, löscht und beschreibt SQL Anywhere ODBC-Datenquellen und listet sie auf

### Syntax

```

dbdsn [ modifier-options ]
{ -l[ s | u ]
| -d[ s | u ] dsn
| -g[ s | u ] dsn
| -w[ s | u ] dsn [details-options;...]
| -cl }

```

Hauptoption	Beschreibung
@ <i>data</i>	<p>Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.</p>
-l[ <b>s</b>   <b>u</b> ]	<p>Listet die verfügbaren ODBC-Datenquellen auf. Sie können das Listenformat ändern, indem Sie die Optionen -b oder -v verwenden. Unter Windows können Sie die Option mit den Systembezeichnern <b>u</b> (Benutzer) oder <b>s</b> (System) ändern. Standardwert ist <b>u</b>.</p>
-d[ <b>s</b>   <b>u</b> ] <i>dsn</i>	<p>Löscht die benannte Datenquelle. Wenn Sie die Option -y angeben, werden bestehende Datenquellen ohne Bestätigungsaufforderung gelöscht. Unter Windows können Sie die Option mit den Systembezeichnern <b>u</b> (Benutzer) oder <b>s</b> (System) ändern. Standardwert ist <b>u</b>.</p>

Hauptoption	Beschreibung
<b>-g</b> <i>[ s   u ] dsn</i>	Listet die Definition der benannten Datenquelle auf. Sie können das Format der Ausgabe ändern, indem Sie die Optionen <b>-b</b> oder <b>-v</b> verwenden. Unter Windows können Sie die Option mit den Systembezeichnern <b>u</b> (Benutzer) oder <b>s</b> (System) ändern. Standardwert ist <b>u</b> .
<b>-w</b> <i>[ s   u ] dsn [ details-options ]</i>	Erstellt eine neue Datenquelle oder überschreibt eine Datenquelle, wenn eine Datenquelle mit demselben Namen vorhanden ist. Sie müssen die Option <b>-c</b> mit der Option <b>-w</b> angeben. Wenn Sie <b>-y</b> angeben, werden bestehende Datenquellen ohne Bestätigungsaufforderung überschrieben. Unter Windows können Sie die Option mit den Systembezeichnern <b>u</b> (Benutzer) oder <b>s</b> (System) ändern. Standardwert ist <b>u</b> .
<b>-cl</b>	Listet die Verbindungsparameter auf, die vom Dienstprogramm dbdsn unterstützt werden.

Änderungsoptionen	Beschreibung
<b>-b</b>	Formatiert die Ausgabe der Liste in eine einzeilige Verbindungszeichenfolge.
<b>-cm</b>	<p>Zeigt den Befehl an, der zum Erstellen der Datenquelle verwendet wurde. Mit dieser Option kann der Erstellungsbehl in eine Datei ausgegeben werden, die verwendet werden kann, um die Datenquelle auf einem anderen Computer zu installieren oder den ursprünglichen Zustand einer Datenquelle wiederherzustellen, wenn sie geändert wurde. Sie müssen die Optionen <b>-g</b> oder <b>-l</b> zusammen mit der Option <b>-cm</b> verwenden, andernfalls schlägt der Befehl fehl. Die Angabe von <b>"-g"</b> zeigt den Erstellungsbehl für die angegebene Datenquelle an, während die Angabe von <b>"-l"</b> den Erstellungsbehl für alle Datenquellen anzeigt.</p> <p>Wenn die angegebene Datenquelle nicht existiert, wird der Befehl zum Löschen der Datenquelle generiert. Beispiel: Wenn die mydsn-Datenquelle auf dem Computer nicht existiert, würde dbdsn <b>-cm -g mydsn</b> den folgenden Befehl zum Löschen der mydsn-Datenquelle zurückgeben:</p> <pre>dbdsn -y -du "mydsn"</pre>

Änderungsoptionen	Beschreibung
<b>-dr</b>	<p>Nimmt den Driver-Parameter auf, wenn Datenquellen angezeigt werden. Wenn Sie die Option <code>-cm</code> zur Neuerstellung von Datenquellen verwenden, kann die aktuelle Version von dbdsn Datenquellen erstellen, die eine andere Version des ODBC-Treibers referenzieren.</p> <p>Führen Sie beispielsweise den folgenden Befehl aus, um eine Datenquelle der Version 11 zu erstellen:</p> <pre>dbdsn -y -wu "11.0 Student Sample" -c "UID=DBA;PWD=sql;...;Driver= SQL Anywhere 11"</pre> <p>Wenn Sie <code>dbdsn -cm -l</code> ausführen, listet dbdsn denselben Befehl ohne den Parameter "Driver=" auf, wodurch die ODBC-Datenquelle unter Verwendung des SQL Anywhere ODBC-Treibers der Version 16 neu erstellt wird.</p> <p>Wenn Sie allerdings <code>dbdsn -dr -cm -l</code> ausführen, wird der Parameter "Driver=" einbezogen und die Datenbank genauso neu erstellt, wie sie ursprünglich erstellt wurde: unter Verwendung des ODBC-Treibers der Version 11.</p>
<b>-f</b>	Zeigt den Namen der Systemdatei, die benutzt wird. Diese Option ist nur unter Unix verfügbar.
<b>-ns</b>	<p>Gibt an, dass die Einstellungen der Umgebungsvariablen benutzt werden, um den Speicherort der Systeminformationsdatei (standardmäßig <code>.odbc.ini</code>) zu ermitteln. Diese Option ist auch nützlich um zu bestimmen, welche Datei von dbdsn verwendet wird, wenn es in der Umgebung mehrere Kandidaten für die Systeminformationsdatei gibt. Diese Option ist nur unter Unix verfügbar.</p> <p>Wenn Sie bei der Erstellung einer Datenquelle nicht die Option <code>-ns</code> angeben, sucht dbdsn im Stammverzeichnis und Pfad des Benutzers nach der Systeminformationsdatei.</p>
<b>-o filename</b>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-or</b>	<p>Erstellt bei Angabe mit der Option <code>-c</code> eine Datenquelle für den SQL Anywhere 16 - Oracle-Treiber. Zum Beispiel:</p> <pre>dbdsn -w MyOracleDSN -or -c Userid=DBA;Password=sql; ServiceName=abcd;ArraySize=500;ProcResults=y</pre> <p>Sie können die Option <code>-cl</code> mit der Option <code>-or</code> angeben, um eine Liste der Verbindungsparameter für den SQL Anywhere 16 - Oracle-Treiber abzurufen.</p>
<b>-pe</b>	Verschlüsselt das Kennwort, das im Verbindungsparameter angegeben wurde, und speichert das verschlüsselte Kennwort in der Datenquelle mit dem ENP-Verbindungsparameter.

Änderungsoptionen	Beschreibung
<b>-q</b>	Unterdrückt die Ausgabe in das Meldungsfenster des Datenbankservers. Wenn Sie beim Löschen oder Ändern einer Datenquelle die Option -q angeben, müssen Sie auch -y angeben.
<b>-v</b>	Formatiert die Ausgabe der Liste über mehrere Zeilen, wie bei einer Tabelle.
<b>-y</b>	Löscht oder überschreibt alle Datenquellen automatisch, ohne eine Bestätigung anzufordern. Wenn Sie beim Löschen oder Ändern einer Datenquelle die Option -q angeben, müssen Sie auch -y angeben.

Detailoptionen	Beschreibung
<b>-c</b> "keyword=value;..."	Gibt Verbindungsparameter als Verbindungszeichenfolge an.
<b>-cw</b>	Stellt sicher, dass der DBF-Parameter (Angabe mit -c) ein absoluter Dateiname ist. Wenn der Wert von DBF kein absoluter Dateiname ist, zieht das Datenquellen-Dienstprogramm das aktuelle Arbeitsverzeichnis heran (CWD). Diese Option ist sinnvoll, da einige Betriebssysteme keine CWD-Informationen in Batchdateien verfügbar halten.

## Privilegien

Keine.

## Bemerkungen

Die Änderungsoptionen können vor oder nach der Angabe der Hauptoptionen definiert werden.

Das Datenquellen-Dienstprogramm ist eine plattformübergreifende Alternative zum ODBC-Datenquellen-Administrator für das Erstellen, Löschen, Beschreiben und Auflisten von ODBC-Datenquellen. Das Dienstprogramm ist für Batch-Vorgänge nützlich.

### Vorsicht

Das Speichern von Benutzer-IDs, Kennwörtern (verschlüsselt oder nicht-verschlüsselt) und/oder Datenbankschlüsseln in einer Datenquelle ist nicht sicher. Es wird empfohlen, dass Sie diese Informationen nicht in einer Datenquelle speichern, wenn die Datenbank sensible Daten enthält.

Unter Windows werden die Datenquellen in der Registrierung eingetragen.

Hinweise zur Erstellung einer Datenquelle mit dem ODBC-Datenquellen-Administrator unter Windows finden Sie unter „[ODBC-Datenquellen](#)“ auf Seite 38.

Unter Unix-Betriebssystemen werden Datenquellen in der Systeminformationsdatei (standardmäßig *.odbc.ini* genannt) gespeichert. Wenn Sie unter Unix mit dem Datenquellen-

Dienstprogramm ODBC-Datenquellen erstellen oder löschen, aktualisiert das Dienstprogramm automatisch den Abschnitt [ODBC Data Sources] in der Systeminformationsdatei. Wenn Sie unter Unix den Treiberverbindungsparameter nicht mit der Option -c angeben, fügt das Datenquellendienstprogramm automatisch einen Treibereintrag mit dem vollen Pfad des SQL Anywhere ODBC-Treibers basierend auf der Einstellung der SQLANY16-Umgebungsvariablen hinzu.

**Vorsicht**

Unter Unix dürfen Sie die Systeminformationsdatei (*.odbc.ini*) nicht mit dem Dienstprogramm zum Verschleiern von Dateien (dbfhide) verschleiern, es sei denn, Sie verwenden ausschließlich SQL Anywhere-Datenquellen. Wenn Sie vorhaben, andere Datenquellen (wie z.B. für die MobiLink-Synchronisation) zu verwenden, kann das Verbergen des Inhalts der Systeminformationsdatei möglicherweise dazu führen, dass andere Treiber nicht richtig funktionieren.

Beendigungscodes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag).

**Siehe auch**

- „Konfigurationsdateien“ auf Seite 882
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Verbindungsparameter“ auf Seite 337
- „ODBC-Verbindungsparameter“ auf Seite 911
- „SQL Anywhere 16 - Oracle-ODBC-Treiber“ [*MobiLink - Serveradministration*]
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]
- „ODBC-Datenquellen“ auf Seite 38
- „ODBC-Datenquellen unter Unix“ auf Seite 49

**Beispiel**

Eine Version der Datenquelle "newdsn" schreiben. Keine Bestätigung anfordern, wenn die Datenquelle bereits vorhanden ist:

```
dbdsn -y -w newdsn -c "UID=DBA;PWD=sql;Host=myhost"
```

Oder, mit einer anderen Reihenfolge der Optionen:

```
dbdsn -w newdsn -c "UID=DBA;PWD=sql;Host=myhost" -y
```

Alle bekannten benutzerdefinierten Datenquellen mit einem Datenquellennamen pro Ausgabezeile auflisten.:

```
dbdsn -l
```

Alle bekannten Systemdatenquellen mit einem Datenquellennamen pro Ausgabezeile auflisten:

```
dbdsn -ls
```

Alle Datenquellen mit der ihnen zugeordneten Verbindungszeichenfolge auflisten:

```
dbdsn -l -b
```

Die Verbindungszeichenfolge für die benutzerdefinierte Datenquelle MyDSN anzeigen:

```
dbdsn -g MyDSN
```

Die Verbindungszeichenfolge für die System-Datenquelle MyDSN anzeigen:

```
dbdsn -gs MyDSN
```

Die Datenquelle BadDSN löschen, aber zuerst die Verbindungsparameter für BadDSN auflisten und eine Bestätigung anfordern:

```
dbdsn -d BadDSN -v
```

Die Datenquelle BadDSN löschen, ohne zur Bestätigung aufzufordern:

```
dbdsn -d BadDSN -y
```

Eine Datenquelle namens NewDSN für den Datenbankserver MyServer erstellen:

```
dbdsn -w NewDSN -c "UID=DBA;PWD=sql;Server=MyServer"
```

Wenn NewDSN bereits besteht, werden Sie aufgefordert, das Überschreiben der Datenquelle zu bestätigen.

Alle Verbindungsparameter-Namen und ihre Aliase auflisten:

```
dbdsn -cl
```

Listet alle Benutzerdatenquellen auf:

```
dbdsn -l -o dsninfo.txt
```

Listet alle Verbindungsparameter auf:

```
dbdsn -cl -o dsninfo.txt
```

Absoluten Dateinamen angeben. Wenn die ODBC-Datenquelle erstellt wird, enthält sie *DBF=c:\SQLAnywhere16\my.db*.

```
c:\SQLAnywhere16> dbdsn -w testdsn -cw -c  
UID=DBA;PWD=sql;Server=SQLAny;DBF=my.db
```

Führen Sie den folgenden Befehl aus, um die Datenquelle **SQL Anywhere 16 Demo** zu erstellen und sie in eine Datei namens *restoredsn.bat* auszugeben:

```
dbdsn -cm -gs "SQL Anywhere 16 Demo" > restoredsn.bat
```

Die Datei *restoredsn.bat* enthält z. B. Folgendes:

```
dbdsn -y -ws "SQL Anywhere 16 Demo" -c "UID=DBA;PWD=sql;  
DBF='C:\Documents and Settings\All Users\Documents\SQL Anywhere 16\Samples  
\demo.db';  
Server=demo16;START='C:\Program Files\SQL Anywhere 16\Bin32\dbeng16.exe';  
ASTOP=yes;Description='SQL Anywhere 16 Sample Database'"
```

Führen Sie den folgenden Befehl aus, um den Speicherort der Systeminformationsdatei unter Unix zurückzugeben:

```
dbdsn -f
```

Der Befehl gibt diese Ausgabe zurück:

```
dbdsn using /home/user/.odbc.ini
```

Den Standort der Systeminformationsdatei ändern:

```
export ODBCINI=./myodbc.ini
```

Den neuen Standort der Systeminformationsdatei mithilfe von dbdsn -f überprüfen:

```
dbdsn using ./myodbc.ini
```

Die Option -ns bei der Erstellung der Datenquelle verwenden:

```
dbdsn -w NewDSN -c "UID=DBA" -ns
```

Dies ergibt die folgende Ausgabe:

```
Configuration "newdsn" written to file ./myodbc.ini
```

## ODBC-Verbindungsparameter

Das Datenquellendienstprogramm (dbdsn) unterstützt die folgenden ODBC-Verbindungsparameter. Boolesche Argumente (TRUE oder FALSE) sind entweder YES bzw. 1 bei TRUE oder NO bzw. 0 bei FALSE.

Name	Beschreibung
Delphi	Delphi kann mehrere Lesezeichenwerte für eine Zeile nicht verarbeiten. Wenn Sie diesen Wert auf NO setzen, wird jeder Zeile ein Lesezeichenwert zugeordnet, und nicht zwei wie im Normalfall. Wenn Sie diese Option auf YES setzen, verbessern Sie damit möglicherweise die Performance scrollfähiger Cursor.
Describe-Cursor	<p>Mit diesem Parameter können Sie angeben, wie oft ein Cursor neu beschrieben werden soll, wenn eine Prozedur aufgerufen wird. Die Standardeinstellung ist "Wenn nötig".</p> <ul style="list-style-type: none"> <li>• <b>Nie</b> Geben Sie 0, N oder NO an, wenn Sie sich sicher sind, dass Ihre Cursor nicht neu beschrieben werden müssen. Cursor neu zu beschreiben ist kostenträchtig und kann die Performance beeinträchtigen.</li> <li>• <b>Wenn nötig:</b> Geben Sie 1, Y oder YES an, wenn der ODBC-Treiber ermitteln soll, ob ein Cursor neu beschrieben werden muss. Das Vorhandensein einer RESULT-Klausel in Ihrer Prozedur verhindert, dass ODBC-Anwendungen die Ergebnismenge neu beschreiben, nachdem ein Cursor geöffnet wurde. Dies ist die Standardeinstellung.</li> <li>• <b>Immer</b> Wenn Sie 2, A oder ALWAYS angeben, wird der Cursor jedes Mal neu beschrieben, wenn er geöffnet wird. Wenn Sie Transact-SQL-Prozeduren verwenden oder Prozeduren, die mehrere Ergebnismengen zurückgeben, müssen Sie den Cursor jedes Mal neu beschreiben, wenn er geöffnet wird.</li> </ul>
Description	Mit diesem Parameter können Sie eine Beschreibung der ODBC-Datenquelle eingeben.

Name	Beschreibung
Driver	<p>Mit diesem Parameter können Sie wie folgt einen ODBC-Treiber für die Verbindung angeben: <code>Driver=driver-name</code>. Standardmäßig ist der verwendete Treiber <b>SQL Anywhere 16</b>. Der <i>Treibername</i> muss <b>SQL Anywhere X</b> sein, wobei <i>X</i> die Hauptversionsnummer der Software ist. Wenn der <i>Treibername</i> nicht mit <b>SQL Anywhere</b> beginnt, kann er vom Datenquellen-Dienstprogramm (dbdsn) nicht gelesen werden.</p> <p>Unter Unix gibt dieser Parameter den voll qualifizierten Pfad zum Shared Object an. Wenn Sie unter Unix den Treiberverbindungsparameter nicht angeben, fügt das Datenquellendienstprogramm automatisch einen Treibereintrag mit dem vollen Pfad des SQL Anywhere ODBC-Treibers basierend auf der Einstellung der SQLANY16-Umgebungsvariablen hinzu.</p>
Escape	<p>Dieser Parameter gibt das Escapezeichen an, das in der LIKE-Klausel von SQL-Anweisungen verwendet wird, die vom ODBC-Treiber generiert werden, wenn eine Liste von Tabellen oder Spalten zurückgegeben wird.</p> <p>Der ODBC-Treiber verwendet standardmäßig die Tilde (~). In einigen Anwendungen wird als Escapezeichen jedoch der Backslash (\) erwartet.</p> <p>Das folgende Fragment einer Verbindungszeichenfolge legt den Backslash als Escapezeichen fest:</p> <pre>"DSN=SQL Anywhere 16 Demo;UID=DBA;PWD=sql;ESCAPE=\\;Host=myhost"</pre>
GetTypeInfoChar	<p>Wenn diese Option auf YES gesetzt ist, werden CHAR-Spalten als SQL_CHAR und nicht als SQL_VARCHAR zurückgegeben. Standardmäßig werden CHAR-Spalten als SQL_VARCHAR zurückgegeben.</p>
InitString	<p>Mit InitString können Sie einen Befehl angeben, der unmittelbar nach Verbindungsherstellung ausgeführt wird. So können Sie beispielsweise eine Datenbankoption setzen oder eine gespeicherte Prozedur aufrufen.</p>

Name	Beschreibung
IsolationLevel	<p>Sie können einen der folgenden Werte angeben, um die Ausgangs-Isolationsstufe für diese Datenquelle einzustellen:</p> <ul style="list-style-type: none"> <li> <b>0</b> Diese Isolationsstufe wird auch die read uncommitted-Stufe (nicht festgeschriebene Anweisungen lesen) genannt. Es handelt sich dabei um die Standard-isolationsstufe. Sie ermöglicht einen maximalen Parallelitätsgrad, allerdings können noch nicht festgeschriebene Daten (Dirty Reads), nicht wiederholbare Lesevorgänge und Phantomzeilen in den Ergebnismengen vorkommen. </li> <li> <b>1</b> Diese Isolationsstufe wird auch die read committed-Stufe (festgeschriebene Anweisungen lesen) genannt. Auf dieser Stufe ist weniger Parallelität möglich als auf Stufe 0, aber einige der Inkonsistenzen in den Ergebnismengen, die auf Isolationsstufe 0 vorkommen, werden eliminiert. Nicht wiederholbare Zeilen und Phantomzeilen können vorkommen, aber Dirty Reads werden verhindert. </li> <li> <b>2</b> Diese Isolationsstufe wird auch die repeatable read-Stufe (wiederholbare Lesevorgänge) genannt. Phantomzeilen können auftreten. Dirty Reads und nicht wiederholbare Zeilen werden verhindert. </li> <li> <b>3</b> Diese Isolationsstufe wird auch die serializable-Stufe (serialisierbar) genannt. Auf dieser Stufe wird der geringste Parallelitätsgrad verfügbar gemacht. Diese Isolationsstufe bietet die strengsten Auflagen. Dirty Reads, nicht wiederholbare Lesevorgänge und Phantomzeilen werden verhindert. </li> <li> <b>Snapshot</b> Sie müssen die Snapshot-Isolation für die Datenbank aktivieren, um diese Isolationsstufe zu verwenden. Die Snapshot-Isolationsstufen verhindern alle Interferenzen zwischen Lese- und Schreibvorgängen. Schreibvorgänge können sich weiterhin überlagern. Für die Konfliktlösung sind einige Inkonsistenzen möglich und die Performance entspricht der von Isolationsstufe 0. </li> <li> <b>Statement-snapshot</b> Sie müssen die Snapshot-Isolation für die Datenbank aktivieren, um diese Isolationsstufe zu verwenden. Die Snapshot-Isolationsstufen verhindern alle Interferenzen zwischen Lese- und Schreibvorgängen. Schreibvorgänge können sich weiterhin überlagern. Für die Konfliktlösung sind einige Inkonsistenzen möglich und die Performance entspricht der von Isolationsstufe 0. </li> <li> <b>Readonly-statement-snapshot</b> Sie müssen die Snapshot-Isolation für die Datenbank aktivieren, um diese Isolationsstufe zu verwenden. Die Snapshot-Isolationsstufen verhindern alle Interferenzen zwischen Lese- und Schreibvorgängen. Schreibvorgänge können sich weiterhin überlagern. Für die Konfliktlösung sind einige Inkonsistenzen möglich und die Performance entspricht der von Isolationsstufe 0. </li> </ul>

Name	Beschreibung
Key-InSQLStatistics	Setzen Sie diesen Parameter auf YES, wenn die SQLStatistics-Funktion Fremdschlüssel zurückgeben soll. Die ODBC-Spezifikation legt fest, dass SQLStatistics keine Primär- oder Fremdschlüssel zurückgeben soll. Einige Microsoft-Anwendungen (wie Microsoft Visual Basic und Microsoft Access) setzen allerdings voraus, dass Primär- und Fremdschlüssel von SQLStatistics zurückgegeben werden.
LazyAuto-commit	Setzen Sie diesen Parameter auf YES, um den Festschreibevorgang bis zum Ende einer Anweisung zu verzögern.
PrefetchOnOpen	Wenn PrefetchOnOpen auf YES eingestellt ist, wird eine Prefetch-Anforderung mit der Anforderung, den Cursor zu öffnen, gesendet. Der Prefetch hindert eine Netzwerkanforderung daran, jedesmal Zeilen abzurufen, wenn ein Cursor geöffnet wird. Spalten müssen bereits gebunden sein, damit der Prefetch beim geöffneten Cursor stattfindet. Dieser Verbindungsparameter vermindert möglicherweise die Anzahl von Client/Server-Anforderungen, was die Performance über ein LAN oder WAN verbessern kann.
PreventNot-Capable	Der SQL Anywhere ODBC-Treiber gibt einen Fehler zurück, weil er keine Qualifizierer unterstützt. Einige ODBC-Anwendungen verarbeiten diesen Fehler nicht einwandfrei. Setzen Sie diesen Parameter auf YES, um die Rückgabe dieser Fehlermeldung zu verhindern und diesen Anwendungen die fehlerfreie Funktion zu ermöglichen.
Suppress-Warnings	Setzen Sie diesen Parameter auf YES, wenn Sie Warnmeldungen unterdrücken möchten, die vom Datenbankserver bei einem Fetch-Vorgang zurückgegeben werden. Die Versionen 8.0.0 und höher des Datenbankservers geben mehr Fetch-Warnungen ab als frühere Versionen der Software. Bei Anwendungen, die mit einer älteren Version der Software implementiert werden, können Sie mit dieser Option sicherstellen, dass korrekt mit den Fetch-Warnungen umgegangen wird.
SuppressInfoForDataTypes	<p>Setzen Sie diesen Parameter auf eine kommasetrennte Liste von Datentypnamen, um zu verhindern, dass der ODBC-Treiber Informationen zu den angegebenen Datentypen zurückgibt. Die angegebenen Datentypen werden weder von der SQLGetTypeInfo-Funktion noch von der DatabaseMetaData.getTypeInfo-Funktion zurückgegeben. Die Anwendung kann jedoch den Datentyp in Spaltendeklarationen und in Ergebnismengenabfragen verwenden. Beispiel: In der folgenden Verbindungszeichenfolge wird verhindert, dass der ODBC-Treiber Informationen zu den Datentypen NVARCHAR, LONG VARCHAR und VARBIT zurückgibt.</p> <p><code>SuppressInfoForDataTypes=nvarchar,long nvarchar,varbit</code></p>
TranslationDLL	Diese Option dient der Abwärtskompatibilität. Die Verwendung von Übersetzern wird nicht empfohlen.
Translation-Name	Diese Option dient der Abwärtskompatibilität. Die Verwendung von Übersetzern wird nicht empfohlen.

Name	Beschreibung
Translation-Option	Diese Option dient der Abwärtskompatibilität. Die Verwendung von Übersetzern wird nicht empfohlen.

**Siehe auch**

- „Richtlinien zum Auswählen der Isolationsstufen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

**dbisqlc-Dienstprogramm (nicht mehr empfohlen)**

Das dbisqlc-Dienstprogramm führt SQL-Anweisungen in einer Datenbank aus.

**Hinweis**

Das dbisqlc-Dienstprogramm unterstützt nicht alle SQL-Anweisungen und -Funktionen, die von Interactive SQL unterstützt werden, und möglicherweise nicht alle Funktionen, die in der aktuellen Version des Datenbankservers verfügbar sind. Es wird empfohlen, das Interactive SQL-Dienstprogramm zu verwenden.

**Syntax**

**dbisqlc** [ *options* ] [ *dbisqlc-statement* | *dbisql-script-file* ]

Option	Beschreibung
<b>-c</b> <i>"key-word=value; ..."</i>	Legt Verbindungsparameter fest. Wenn Interactive SQL keine Verbindung herstellen kann, erscheint ein Fenster, in das Sie die Verbindungsparameter eingeben können.
<b>-d</b> <i>delimiter</i>	Gibt ein Befehlstrennzeichen an. Anführungszeichen um das Trennzeichen sind optional und nur dann erforderlich, wenn die Befehlsebene selbst das Trennzeichen auf spezielle Art interpretiert.  Das angegebene Befehlstrennzeichen wird bei allen Verbindungen in der aktuellen dbisqlc-Sitzung verwendet.
<b>-q</b>	Unterdrückt die Ausgabe von Meldungen. Dies ist nur dann nützlich, wenn Sie Interactive SQL mit einer Anweisung oder einer Skriptdatei starten. Das Angeben dieser Option unterdrückt keine Fehlermeldungen, sondern Folgendes: <ul style="list-style-type: none"> <li>• Warnungen und andere nicht-schwerwiegende Meldungen</li> <li>• Die Ausgabe von Ergebnismengen</li> </ul>
<b>-x</b>	Durchsucht Anweisungen, führt sie aber nicht aus. Dies ist nützlich, um lange Skriptdateien auf Syntaxfehler zu überprüfen.

## Privilegien

Keine.

## Bemerkungen

Mit dem Dienstprogramm dbisqlc können Sie SQL-Anweisungen eingeben oder SQL-Skriptdateien ausführen.

Wenn eine *dbisqlc*-Anweisung angegeben wird, führt dbisqlc die Anweisung aus. Sie können auch einen Skriptdateinamen angeben. Wenn weder eine *dbisqlc*-Anweisung noch ein Argument für die *dbisqlc*-Skriptdatei angegeben wird, wechselt dbisqlc in den interaktiven Modus. Dort können Sie eine Anweisung in ein Befehlsfenster eingeben.

Das Dienstprogramm dbisqlc ist unter Microsoft Windows, Mac OS X und Unix verfügbar.

## Siehe auch

- „Verbindungsparameter“ auf Seite 337
- „Interactive SQL-Dienstprogramm (dbisql)“ auf Seite 939
- „SQL-Sprachelemente“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Beispiel

Mit dem folgenden Befehl wird die Skriptdatei *mycom.sql* auf dem aktuellen Standardserver ausgeführt und dabei werden die Benutzer-ID "DBA" und das Kennwort "sql" verwendet. Wenn in der Skriptdatei ein Fehler auftritt, wird der Prozess heruntergefahren.

```
dbisqlc -c "UID=DBA;PWD=sql" mycom.sql
```

Führen Sie den folgenden Befehl aus, um einen Benutzer zur aktuellen Standarddatenbank hinzuzufügen:

```
dbisqlc -c "UID=DBA;PWD=sql" CREATE USER joe IDENTIFIED BY passwd
```

# Löschen-Dienstprogramm (dberase)

Löscht Datenbankdateien und diesen zugeordnete Transaktionslogs oder einzelne Transaktionslogdateien.

## Syntax

**dberase** [ *options* ] *database-file*

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.

Option	Beschreibung
<b>-ek</b> <i>key</i>	Gibt den Chiffrierschlüssel für stark verschlüsselte Datenbanken im Befehl an. Wenn Sie mit einer stark verschlüsselten Datenbank arbeiten, müssen Sie den Chiffrierschlüssel angeben, bevor Sie die Datenbank oder das Transaktionslog verwenden können. Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie bei einer stark verschlüsselten Datenbank nicht den richtigen Schlüssel angeben.
<b>-ep</b>	Gibt an, dass Sie zur Eingabe des Chiffrierschlüssel aufgefordert werden wollen. Diese Option öffnet ein Fenster, in das Sie den Chiffrierschlüssel eingeben. Diese zusätzliche Sicherheitsmaßnahme verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird. Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie bei einer stark verschlüsselten Datenbank nicht den richtigen Schlüssel angeben.
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt. Wenn Sie diese Option angeben, müssen Sie auch die Option -y angeben, sonst schlägt der Vorgang fehl.
<b>-y</b>	Löscht jede Datei, ohne Aufforderung zur Bestätigung. Wenn Sie -q angeben, müssen Sie auch die Option -y angeben, sonst schlägt der Vorgang fehl.

### Privilegien

Keine.

### Bemerkungen

Mit dem Löschen-Dienstprogramm können Sie eine Datenbankdatei und ihr zugeordnetes Transaktionslog oder eine Transaktionslogdatei bzw. eine Transaktionslog-Spiegeldatei löschen. Alle Datenbankdateien und Transaktionslogdateien sind als schreibgeschützt markiert. Damit soll verhindert werden, dass die Datenbank ungewollt beschädigt und die Datenbankdateien aus Versehen gelöscht werden.

*database-file* kann eine Datenbankdatei oder eine Transaktionslogdatei sein. Der vollständige Dateiname einschließlich Erweiterung muss angegeben werden. Wenn eine Datenbankdatei angegeben ist, wird die zugeordnete Transaktionslogdatei (und der Spiegel, wenn vorhanden) ebenfalls gelöscht.

#### Hinweis

Mit dem Löschen-Dienstprogramm werden DBSpaces nicht gelöscht. Wenn Sie einen DBSpace löschen möchten, verwenden Sie die DROP DBSPACE-Anweisung.

Das Löschen einer Datenbankdatei, die andere DBSpaces referenziert, löscht nicht automatisch die DBSpace-Dateien. Um die DBSpace-Dateien selbst zu löschen, müssen Sie den schreibgeschützten Modus aufheben und anschließend die Dateien einzeln löschen. Alternativ können Sie mit der DROP

DATABASE-Anweisung oder dem **Assistenten zum Löschen einer Datenbank** eine Datenbank und deren zugeordnete DBSpace-Dateien löschen.

Wenn Sie eine Datenbankdatei löschen, werden die zugeordneten Transaktionslogs und Transaktionslogspiegel ebenfalls gelöscht. Wenn Sie ein Transaktionslog für eine Datenbank löschen, die ebenfalls einen Transaktionslogspiegel unterhält, wird der Spiegel nicht gelöscht.

Die zu löschende Datenbank darf nicht laufen, wenn dieses Dienstprogramm verwendet wird.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlslag).

#### Siehe auch

- „Konfigurationsdateien“ auf Seite 882
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „DROP DBSPACE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbanken löschen (Dienstprogramm dberase)“ auf Seite 149
- „Datenbanken löschen (Sybase Central)“ auf Seite 149
- „DROP DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]

## Dienstprogramm für die Verwaltung von ETD-Dateien (dbmanageetd)

Generiert ein Diagnoselog, das es dem Benutzer ermöglicht, Informationen zu benutzerdefinierten und Systemereignissen zu überprüfen.

#### Syntax

**dbmanageetd** [ *options* ] [ *filtering-options* ] [ *information-options* ] [ *output-format-options* ] [ *output-redirection-options* ] *filename*

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.
-m	Führt mehrere Diagnosedateien zusammen.
-s	Zeigt eine Diagnosezusammenfassung an. Die Option -s darf nicht zusammen mit der Ausgabeformatoption -etd verwendet werden.
-h	Zeigt die Syntaxhilfe an.

Filteroption	Beschreibung
<b>-fe</b> <i>event-name, ...</i>	Filtert nach Ereignisname.
<b>-fh</b> <i>host, ...</i>	Filtert nach Hostname.
<b>-fl</b> <i>severity-level</i>	Filtert nach Schweregrad. Gültige Schweregrade sind CRITICAL, ERROR, WARNING, INFORMATION oder DEBUG.
<b>-fr</b> <i>offset,count</i>	Filtert nach Datensatzbereich. Offset ist ein Offset gegenüber 0. Anzahl ist die Anzahl der zurückgegebenen Datensätze.
<b>-ft</b> <i>from,to</i>	Filtert nach Zeitstempelbereich.  Das Zeitstempelformat sollte <i>JJJJ - MM - TThh:mm:ss.sssTZD</i> sein. Dabei gilt: <i>TZD</i> ist die Zeitzoneangabe (Z oder <i>+hh:mm</i> oder <i>-hh:mm</i> ).  Verwenden Sie Z für UTC-Offset oder <i>+hh:mm</i> oder <i>-hh:mm</i> zur Angabe einer Zeitzoneanpassung.
<b>-fregex</b> <i>regex</i>	Filtert nach dem regulären Ausdruck in Ereignisdaten (nur Windows und Linux)

Informationsoption	Beschreibung
<b>-all</b>	Zeigt alle Informationen an (Prozesskennung, Thread-ID, Hostname, Hostinformationen und Dateiname).
<b>-epoch</b>	Zeigt die Uhrzeit im Epochenformat in Millisekunden an.
<b>-filename</b>	Zeigt den Dateinamen an.
<b>-hostinfo</b>	Zeigt die Hostinformationen an. Zu diesen Informationen gehören Betriebssystemversion und Prozessortyp.
<b>-hostname</b>	Zeigt das Hostnamenfeld an.
<b>-pid</b>	Zeigt das Prozesskennungsfeld an.
<b>-tid</b>	Zeigt das Thread-ID-Feld an.
<b>-tzadjminutes</b>	Gibt den Wert für die Zeitzoneanpassung in Minuten an. Standardwert ist die Ortszeit des Computers, auf dem das Dienstprogramm ausgeführt wird.
<b>-utc</b>	Zeigt die Uhrzeit im UTC-Format an.

Ausgabeformatoption	Beschreibung
<b>-text</b>	Zeigt die Ausgabe im Zeichensatz des Betriebssystems an. Dieser Wert ist die Standardeinstellung. Der Zeichensatz des Betriebssystems wird verwendet, es sei denn, eine Kodierung wird mit der Option <i>-te</i> angegeben.
<b>-etd</b>	Zeigt die Ausgabe im ETD-Dateiformat an. Geben Sie die Option <i>-o</i> mit dieser Option an. Die Option <i>-etd</i> kann nicht mit der Option <i>-s</i> verwendet werden.
<b>-xml</b>	Zeigt die Ausgabe im XML-Format mit UTF-8 an.
<b>-le</b>	Listet die verfügbaren Zeichensatzkodierungen auf. Geben Sie <i>+</i> an, um die erweiterte Liste anzuzeigen.
<b>-te <i>encoding</i></b>	Gibt die Zeichensatzkodierung für das Ausgabeformat <i>-text</i> an. Standardmäßig wird der Zeichensatz des Betriebssystems verwendet.

Ausgabeumleitungsoption	Beschreibung
<b>-o <i>filename</i></b>	Der Name der Datei, in der die Ausgabe gespeichert wird.

### Voraussetzungen

Sie müssen bereits eine Ereignisprotokollierungssitzung eingerichtet haben, mit der Informationen in einer ETD-Datei protokolliert wurden.

### Privilegien

Keine

### Bemerkungen

Die Filteroptionen *-fe* und *-fh* akzeptieren durch Kommata getrennte Listen von Werten.

Die Ausgabe wird auf dem Bildschirm angezeigt, es sei denn, die Option *-o* ist angegeben.

## Siehe auch

- „Ereignisprotokollierung“ auf Seite 1101
- „CREATE TEMPORARY TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE TEMPORARY TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP TRACE EVENT SESSION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „NOTIFY TRACE EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_events-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_fields-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_sessions-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_events-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_targets-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_trace\_event\_session\_target\_options-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Beispiel

1. **Anzeigen einer Zusammenfassung der Diagnosedaten** Führen Sie den folgenden Befehl aus, um eine Zusammenfassung der Diagnosedaten anzuzeigen:

```
dbmanageetd -s diagnostic-log.etd
```

2. **Anzeigen einer Liste von Ereignissen mit einem Schweregrad von ERROR und höher** Verwenden Sie c

```
dbmanageetd -fl error diagnostic-log
```

3. **Konvertieren einer .etd-Datei in eine .xml-Datei** Verwenden Sie die Optionen -xml und -o. Beispiel:

```
dbmanageetd -xml -o merged.xml diagnostic-log.etd
```

4. **Anzeigen von Ereignissen nur für einen bestimmten Host** Verwenden Sie die Option -fh, um nur Ereignisse vom Host "MyHost" anzuzeigen. Beispiel:

```
dbmanageetd -fh MyHost diagnostic-log.etd
```

5. **Zusammenführen mehrerer .etd-Dateien von verschiedenen Hosts** Verwenden Sie die Option -bg. Beispiel:

```
dbmanageetd -m -etd -o merged.etd machine1.etd machine2.etd machine3.etd machine4.etd
```

6. **Anzeigen von nach Zeitstempelbereich gefilterten Ereignissen** Verwenden Sie die Option -ft, um Ereignisse anzuzeigen, die am 26. März 2012 zwischen 01:30 Uhr und 02:00 Uhr EST aufgetreten sind. Beispiel:

```
dbmanageetd -ft
2012-03-26T01:30:00.000-04:00,2012-03-26T02:00:00.000-04:00 diagnostic-log.etd
```

## Dienstprogramm zum Verschleiern von Dateien (dbfhide)

Verwendet die einfache Verschlüsselung, um den Inhalt von Konfigurations- und Initialisierungsdateien zu verbergen

### Syntax

**dbfhide** [ *options* ] *original-configuration-file encrypted-configuration-file*

Option	Beschreibung
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-w</b>	Verschlüsselt die Datei mit einer von Microsoft zur Verfügung gestellten Verschlüsselungs-API. Die Datei kann nur von Datenbankservern oder Tools auf demselben Computer verwendet werden, auf dem die Datei verschlüsselt wurde. Nur der Benutzer, der die Datei verschlüsselt hat, kann die Datei verwenden. Diese Option wird nur unter Windows unterstützt.
<b>-wm</b>	Verschlüsselt die Datei mit einer von Microsoft zur Verfügung gestellten Verschlüsselungs-API. Die Datei kann nur von Datenbankservern oder Tools auf demselben Computer verwendet werden, auf dem die Datei verschlüsselt wurde. Jeder Benutzer auf dem Computer, auf dem der Datei verschlüsselt wurde, kann die Datei lesen. Diese Option wird nur unter Windows unterstützt.
<i>original-configuration-file</i>	Gibt den Namen der Originaldatei an.
<i>encrypted-configuration-file</i>	Gibt einen Namen für die neue verschleierte Datei an.

### Privilegien

Keine.

### Bemerkungen

Dieses Dienstprogramm akzeptiert den **@data**-Parameter zum Einlesen von Optionen aus einer Konfigurationsdatei nicht.

Konfigurationsdateien werden von manchen Dienstprogrammen verwendet, um Befehlszeilenoptionen aufzubewahren. Diese Optionen könnten ein Kennwort enthalten. Standardmäßig verwendet dbfhide einfache Verschlüsselung in der angegebenen Datei.

Sie können weder den Inhalt einer verschlüsselten Datei ändern noch die Verschlüsselung von einer Datei entfernen. Um Änderungen an einer verschlüsselten Datei vorzunehmen, müssen Sie die Datei ersetzen. Deshalb wird empfohlen, dass Sie Kopien der Konfigurationsdateien erstellen und die Kopien verschlüsseln. Die ursprünglichen Dateien müssen sich an einem anderen Speicherort befinden, damit sie erneut zum Erstellen von Kopien verwendet werden können. Gehen Sie folgendermaßen vor, um verschlüsselte Konfigurationsdateien zu ersetzen: Erstellen Sie Kopien der ursprünglichen Dateien,

nehmen Sie die gewünschten Änderungen an den Kopien vor, verschlüsseln Sie die Kopien und ersetzen Sie dann die alten verschlüsselten Dateien durch diese neuen Dateien.

Wenn Sie die Option `-w` oder die Option `-wm` angeben, wird die Datei mithilfe einer von Microsoft bereitgestellten API verschlüsselt. Die API protokolliert den zum Verschlüsseln der Datei verwendeten Chiffrierschlüssel. Der Chiffrierschlüssel wird mit dem angemeldeten Benutzer oder Computer verknüpft.

### Siehe auch

- „Konfigurationsdateien und Datenbankserver-Startoptionen“ auf Seite 162
- „Datensicherheit“ auf Seite 1402
- „Konfigurationsdateien“ auf Seite 882
- „Bedingte syntaktische Analyse in Konfigurationsdateien“ auf Seite 883
- „Inhalte von .ini-Dateien verbergen“ auf Seite 489

### Beispiel

Erstellen Sie eine Konfigurationsdatei, die den Personal Datenbankserver und die Beispieldatenbank startet. Damit sollte der Cache auf 10 MB eingestellt werden und diese Instanz des Personal Servers den Namen *Elora* erhalten. Die Konfigurationsdatei würde wie folgt geschrieben werden:

```
# Configuration file for server Elora
-n Elora
-c 10M
"%SQLANY16%\demo.db"
```

(Zeilen, die mit # beginnen, werden als Kommentare behandelt.)

Nennen Sie die Datei *sample.txt*. Wenn Sie die Datenbank mit dieser Konfigurationsdatei starten wollen, würde Ihre Befehlszeile wie folgt aussehen:

```
dbsrv16 @sample.txt
```

Jetzt fügen Sie der Konfiguration eine einfache Verschlüsselung hinzu.

```
dbfhide sample.txt encrypted_sample.txt
```

Benutzen Sie die Datei *encrypted\_sample.txt*, um eine Datenbank zu starten.

```
dbsrv16 @encrypted_sample.txt
```

## Histogramm-Dienstprogramm (dbhist)

Konvertiert ein Histogramm in ein Microsoft Excel-Diagramm mit Informationen über die Selektivität von Prädikaten

### Syntax

```
dbhist [ options ] -t table-name [ excel-output-filename ]
```

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „ <a href="#">Konfigurationsdateien</a> “ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „ <a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a> “ auf Seite 922.
-c options	Legt Verbindungsparameter fest. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
-n colname	Gibt den Namen der Spalte an, mit der das Histogramm verknüpft werden soll. Wenn Sie keine Spalte angeben, werden alle Spalten in der Tabelle, die Histogramme haben, zurückgegeben.
-t table-name	Gibt den Namen der Tabelle oder materialisierten Ansicht an, für die das Diagramm generiert werden soll.
-u owner	Gibt den Eigentümer der Tabelle oder materialisierten Ansicht an.
excel-output-name	Gibt den Namen der generierten Microsoft Excel-Datei an. Wenn kein Name angegeben wird, werden Sie von Microsoft Excel mit dem Fenster <b>Speichern unter</b> zur Eingabe eines Namens aufgefordert.

## Privilegien

Sie müssen das MANAGE STATISTICS-Systemprivileg haben.

## Bemerkungen

Histogramme werden in der Systemtabelle ISYSCOLSTAT gespeichert und können auch mit der Prozedur sa\_get\_histogram abgerufen werden. Das Histogramm-Dienstprogramm konvertiert ein Histogramm in ein Microsoft Excel-Diagramm mit Informationen über die Selektivität von Prädikaten. Das Histogramm-Dienstprogramm (dbhist) funktioniert nur unter Windows. Außerdem muss Microsoft Excel 97 oder später installiert sein.

Statistiken (einschließlich Histogramme) sind möglicherweise für eine Tabelle oder materialisierte Ansicht nicht vorhanden, beispielsweise wenn Statistiken kürzlich gelöscht wurden. In diesem Fall gibt das Histogramm-Dienstprogramm die Meldung `Histogramm enthält keine Daten,` Vorgang wird abgebrochen zurück. In diesem Fall müssen Sie die Statistiken erstellen und dann das Histogramm-Dienstprogramm neuerlich ausführen. Um Statistiken für eine Tabelle oder eine materialisierte Ansicht zu erstellen, führen Sie eine CREATE STATISTICS-Anweisung aus.

Wenn Sie die Selektivität eines Prädikats gegenüber einer Zeichenfolgenspalte ermitteln möchten, verwenden Sie die Funktion ESTIMATE oder ESTIMATE\_SOURCE. Wenn Sie versuchen, ein Histogramm aus Zeichenfolgenspalten abzurufen, geben sa\_get\_histogram und das Histogramm-Dienstprogramm einen Fehler aus.

Die Tabellen werden mit dem Spaltennamen benannt. Spaltennamen werden ab 24 Zeichen gekürzt. Jedes Auftreten von "\", "/", "?", "\*", "[", "]" und ":" (die in Microsoft Excel nicht zulässig sind) wird durch Unterstriche ( \_ ) ersetzt. Diagrammnamen wird das Wort "chart" vorangestellt, gefolgt von denselben Namenskonventionen wie oben. Doppelt vorkommende Namen (aufgrund von Zeichenersetzungen, Kürzungen oder mit "chart" beginnenden Spaltennamen) ergeben einen Microsoft Excel-Fehler, der besagt, dass keine Duplikatnamen verwendet werden dürfen. Die Tabelle wird dennoch mit jenen Namen erstellt, die mit ihrer früheren Version erstellt wurden (Sheet1, Chart1 usw.).

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlenschlag).

Sie können Histogramme auch mit der gespeicherten Prozedur `sa_get_histogram` abrufen.

### Siehe auch

- „CREATE STATISTICS-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]
- „sa\_get\_histogram-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Quellen der Selektivitätsschätzung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Optimiererschätzungen und -statistiken“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „ESTIMATE-Funktion [Verschiedene]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ESTIMATE\_SOURCE-Funktion [Verschiedene]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

### Beispiel

Der folgende Befehl (auf einer Zeile eingegeben) erstellt ein Microsoft Excel-Diagramm für die Spalte ProductID in der Tabelle SalesOrderItems für die Datenbank *demo.db* und speichert es als *histogram.xls*.

```
dbhist -c "UID=DBA;PWD=sql;DBF=%SQLANYAMP16%\demo.db" -n ProductID -t  
SalesOrderItems histogram.xls
```

Die folgende Anweisung generiert für jede Spalte mit einem Histogramm in der Tabelle SalesOrders Diagramme. Dies geschieht unter der Annahme, dass die Beispieldatenbank bereits gestartet ist. Diese Anweisung versucht außerdem, eine Verbindung mittels UID=DBA und PWD=sql herzustellen. Für die Ausgabedatei ist kein Name angegeben, daher werden Sie von Microsoft Excel aufgefordert, einen Namen einzugeben.

```
dbhist -t SalesOrders -c "UID=DBA;PWD=sql"
```

## Informations-Dienstprogramm (dbinfo)

Zeigt Informationen über die angegebene Datenbank an

### Syntax

```
dbinfo [ options ]
```

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „ <a href="#">Konfigurationsdateien</a> “ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „ <a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a> “ auf Seite 922.
-c "keyword=value; ..."	Legt Verbindungsparameter fest. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
-o filename	Schreibt Ausgabemeldungen in die benannte Datei.
-q	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
-u	Zeigt Informationen über die Nutzung und Größe aller Tabellen, einschließlich System- und benutzerdefinierter Tabellen, und materialisierter Ansichten an.  Sie können Seitennutzungsstatistiken nur anfordern, wenn keine anderen Benutzer mit der Datenbank verbunden sind. Die Seitennutzungsinformationen werden mit der sa_table_page_usage-Systemprozedur abgerufen, die das MANAGE ANY STATISTICS-Systemprivileg erfordert.

## Privilegien

Jeder beliebige Benutzer kann dbinfo ausführen. Um Seitennutzungsstatistiken zu erhalten, müssen Sie jedoch das MANAGE ANY DBSPACE-Systemprivileg haben.

## Bemerkungen

Das Dienstprogramm dbinfo zeigt Informationen über eine Datenbankdatei an. Es gibt Auskunft über Folgendes: Name der Datenbank, Namen aller Transaktionslogdateien oder Logspiegel, Seitengröße, Kollationsname und -label, ob Tabellenverschlüsselung aktiviert ist sowie andere Informationen. Optional kann es auch Statistiken über die Tabellenverwendung und Details anzeigen.

Sie können das Dienstprogramm dbinfo verwenden, um die Größe einer Tabelle auf der Festplatte zu ermitteln. Dazu führen Sie einen Befehl des folgenden Typs aus:

```
dbinfo -u -c "UID=DBA;PWD=sql;DBF=%SQLANYAMP16%\demo.db"
```

Das Ergebnis zeigt, wie viele Seiten verwendet werden, um die Daten der Tabellen Ihrer Datenbank zu speichern, und den von diesen Seiten belegten Prozentsatz ("% Seiten verw."). Für jede Tabelle können

Sie dann die Anzahl der Seiten mit der Datenbankseitengröße multiplizieren und das Ergebnis danach mit "% Seiten verw." multiplizieren, um zu ermitteln, wie viel Speicherplatz von Ihrer Tabelle belegt wird.

Sie können wie folgt noch weitere Informationen über eine Datenbankdatei erhalten:

- Abfragen von einzelnen Datenbankeigenschaften unter Verwendung der DB\_PROPERTY-Systemfunktion.
- Abfragen aller Datenbankeigenschaften mit der sa\_db\_properties-Systemprozedur.
- Verwendung der Option -pd mit dem Ping-Dienstprogramm (dbping). Bei der Verwendung von -pd gibt dbping den Wert für jede angegebene Datenbankeigenschaft zurück.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

#### Siehe auch

- „DB\_PROPERTY-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_db\_properties-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]

## Dienstprogramm Initialisierung (dbinit)

Erstellt eine neue Datenbank.

#### Syntax

**dbinit** [ *options* ] *new-database-file*

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „Konfigurationsdateien“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922.</p>

Option	Beschreibung
<b>-a</b>	<p>Bewirkt, dass Zeichenfolgenvergleiche Akzentunterschiede zwischen Buchstaben erkennen. Z.B. ist e kleiner als é, wenn der Unicode-Kollationsalgorithmus (Unicode Collation Algorithm, UCA) für CHAR- oder NCHAR-Datentypen verwendet wird (siehe -z und -zn). Mit Ausnahme japanischer Datenbanken, die mit UCA-Kollation erstellt wurden, werden Akzente standardmäßig ignoriert (daher ist e gleich é). Wenn die Basisbuchstaben (Buchstaben ohne Akzente und entfernte Groß-/Kleinschreibung) ansonsten gleich sind, werden Akzente von links nach rechts verglichen.</p> <p>Die Standardeinstellung für Berücksichtigung von Akzenten einer UCA-Kollation beim Erstellen einer japanischen Datenbank ist <i>Berücksichtigung von Akzenten</i>. Damit werden Akzentbuchstaben erkannt. Siehe „<a href="#">Unicode-Kollationsalgorithmus (UCA)</a>“ auf Seite 516.</p>
<b>-af</b>	<p>Bewirkt, dass Zeichenfolgenvergleiche Akzentunterschiede zwischen Buchstaben erkennen (z.B. ist e kleiner als é), wenn der UCA für CHAR- oder NCHAR-Datentypen verwendet wird (siehe -z und -zn). Standardmäßig werden Akzente ignoriert (d.h. e ist gleich é). Wenn die Basisbuchstaben (Buchstaben mit entfernten Akzenten) ansonsten gleich sind, werden Akzente von rechts nach links verglichen, entsprechend den Regeln der französischen Sprache.</p> <p>Siehe „<a href="#">Unicode-Kollationsalgorithmus (UCA)</a>“ auf Seite 516.</p>
<b>-b</b>	<p>Auffüllen mit Leerzeichen in der Datenbank aktivieren.</p> <p>SQL Anywhere vergleicht alle Zeichenfolgen, als ob sie eine variable Länge hätten und unter Verwendung der VARCHAR-Domäne gespeichert würden. Dies schließt Zeichenfolgenvergleiche ein, die CHAR- oder NCHAR-Spalten mit fester Länge betreffen. Überdies kürzt SQL Anywhere niemals Werte oder füllt sie mit nachgestellten Leerzeichen auf, wenn die Werte in der Datenbank gespeichert werden.</p> <p>Standardmäßig behandelt SQL Anywhere Leerzeichen als signifikante Zeichen. Daher ist der Wert "a " (das Zeichen "a", gefolgt von einem Leerzeichen) nicht mit der Ein-Zeichen-Zeichenfolge "a" äquivalent. Ungleichheits-Vergleiche behandeln ebenfalls ein Leerzeichen wie jedes andere Zeichen in der Kollation.</p> <p>Wenn das Auffüllen mit Leerzeichen aktiviert ist (dbinit-Option -b), entspricht die Semantik von Zeichenfolgenvergleichen besser dem ANSI/ISO SQL-Standard. Bei aktiviertem Auffüllen mit Leerzeichen ignoriert SQL Anywhere in einem Vergleich nachgestellte Leerzeichen.</p> <p>Im obestehenden Beispiel gibt ein Gleichheitsvergleich von "a" mit "a" in einer mit Leerzeichen aufgefüllten Datenbank TRUE zurück. In einer mit Leerzeichen aufgefüllten Datenbank werden Zeichenfolgen fester Länge mit Leerzeichen aufgefüllt, wenn sie von einer Anwendung abgerufen werden. Die Verbindungsoption ansi_blanks steuert, ob die Anwendung eine Warnung über die Kürzung einer Zeichenfolge bei einer solchen Zuordnung erhält. Siehe „<a href="#">ansi_blanks-Option</a>“ auf Seite 575.</p>

Option	Beschreibung
<b>-c</b>	<p>Berücksichtigt bei allen Werten die Groß- /Kleinschreibung bei Vergleichen und Zeichenfolgenverarbeitung. Bezeichner in der Datenbank beachten die Groß-/Kleinschreibung nicht, selbst in Datenbanken, die die Groß-/Kleinschreibung beachten.</p> <p>Mit Ausnahme von japanischen Datenbanken, die mit der UCA-Kollation erstellt wurden, ist das Standardverhalten, dass alle Vergleiche <i>die Groß-/Kleinschreibung nicht beachten</i>. Die Standardeinstellung für Berücksichtigung von Groß-/Kleinschreibung einer UCA-Kollation beim Erstellen einer japanischen Datenbank ist <i>Berücksichtigung der Groß-/Kleinschreibung</i>.</p> <p>Diese Option wird aus Gründen der Kompatibilität mit dem ISO/ANSI SQL-Standard bereitgestellt.</p>
<b>-dba</b> [ <i>DBA-user</i> ] [ <i>,pwd</i> ]	<p>Gibt eine Benutzer-ID und ein Kennwort an, die verwendet werden können, um sich nach der Erstellung bei der Datenbank anzumelden. Dieser Benutzer hat volle Administrationsrechte für die Datenbank, sodass er alle mit Privilegien verbundenen Vorgänge ausführen und ein Sicherheitsmodell einrichten kann. Wenn keine Angabe gemacht wurde, wird der Benutzer "DBA" mit dem Kennwort "sql" erstellt (empfohlen).</p> <p>Wenn Sie ein anderes Kennwort angeben, muss es aus 7-Bit-ASCII-Zeichen bestehen. Andere Zeichen funktionieren möglicherweise nicht korrekt, wenn der Server die Konvertierung aus dem Clientzeichensatz in UTF-8 nicht durchführen kann.</p> <p>Einer der folgenden Befehle erstellt eine Datenbank mit einem Benutzer namens "DBA" und dem Standardkennwort "sql":</p> <pre>dbinit -dba DBA mydb.db dbinit -dba testuser, mydb.db</pre> <p>Der folgende Befehl verwendet die Standardbenutzer-ID "DBA" mit dem Kennwort "mypwd":</p> <pre>dbinit -dba ,mypwd mydb.db</pre> <p>Der folgende Befehl ändert den DBA-Benutzer in Benutzer1 mit dem Kennwort "mypwd":</p> <pre>dbinit -dba user1,mypwd mydb.db</pre>
<b>-dbs</b> <i>size</i> [ <b>k</b>   <b>m</b>   <b>g</b>   <b>p</b> ]	<p>Weist vorab Speicher für die Datenbank zu. Vorabzuweisungen von Speicherplatz für die Datenbank tragen dazu bei, das Risiko der Speicherplatzknappheit auf dem Laufwerk zu verringern, auf dem die Datenbank läuft. Überdies kann die Performance verbessert werden, indem die Menge der Daten erhöht wird, die in der Datenbank gespeichert werden können, bevor der Datenbankserver die Datenbank vergrößern muss, was ein zeitaufwändiger Vorgang sein kann.</p> <p>Standardmäßig wird die <i>Größe</i> in Byte angegeben. Sie können <b>k</b>, <b>m</b>, <b>g</b> oder <b>p</b> verwenden, um die Einheit in kB, MB, GB bzw. Seiten anzugeben.</p>

Option	Beschreibung
<b>-ea</b> <i>algorithm</i>	<p>Gibt den Verschlüsselungsalgorithmus für die Datenbank- oder Tabellenverschlüsselung an (-et). Geben Sie <code>-ea simple</code> für die einfache Verschlüsselung an (nicht -ek oder -ep). Eine einfache Verschlüsselung ist gleichbedeutend mit der Verschleierung und dient nur dazu, die Daten bei einem zufälligen Direktzugriff auf die Datenbankdatei zu verbergen, wobei das Entschlüsseln der Daten in Ihrer Datenbank mithilfe eines Festplatten-Dienstprogramms erschwert wird.</p> <p>Um die Sicherheit zu erhöhen, geben Sie AES oder AES256 für starke 128-Bit- bzw. 256-Bit-Verschlüsselung an. Geben Sie AES_FIPS oder AES256_FIPS für FIPS-zertifizierte 128-Bit- bzw. 256-Bit-Verschlüsselung an. Bei starker Verschlüsselung müssen Sie auch die Option -ek oder -ep angeben. Siehe „<a href="#">Einfache Verschlüsselung und starke Verschlüsselung</a>“ auf Seite 1425.</p> <p>Um eine nicht verschlüsselte Datenbank zu erstellen, geben Sie <code>-ea none</code> an oder Sie beziehen die Option -ea nicht ein (und geben keine der Optionen -et, -ep und -ek an).</p> <p>Wenn Sie die Option -ea nicht angeben, ist das Standardverhalten wie folgt:</p> <ul style="list-style-type: none"> <li>• -ea none, wenn -ek, -ep oder -et nicht angegeben ist</li> <li>• -ea AES, wenn -ek oder -ep angegeben ist (mit oder ohne -et)</li> <li>• -ea simple, wenn -et ohne -ek oder -ep verwendet wird</li> </ul> <p>Algorithmusnamen berücksichtigen die Groß- und Kleinschreibung nicht.</p> <p>Unter Windows Mobile werden die AES_FIPS- und AES256_FIPS-Algorithmen nur mit ARM-Prozessoren unterstützt.</p> <p>Der folgende Befehl erstellt eine stark verschlüsselte Datenbank mit Angabe des Chiffrierschlüssels und des Algorithmus.</p> <pre>dbinit -ek "0kZ2o56AK#" -ea AES_FIPS "myencrypteddb.db"</pre> <p>Datenkomprimierungsprogramme können verschlüsselte Datenbankdateien nicht so stark komprimieren wie unverschlüsselte.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b> Erforderliche getrennt lizenzierbare Komponenten.</p> <p>FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.</p> <p>Siehe „<a href="#">Getrennt lizenzierbare Komponenten</a>“ [<i>SQL Anywhere 16 - Einführung</i>].</p> </div>

Option	Beschreibung
<b>-ek</b> <i>key</i>	<p>Gibt an, dass eine stark verschlüsselte Datenbank erstellt werden soll, wobei der Chiffrierschlüssel direkt in die Befehlszeile eingegeben wird. Die -ek-Option wird mit einem AES-Algorithmus benutzt, der optional mit der -ea-Option angegeben wird. Wenn Sie die -ek-Option ohne die -ea-Option angeben, wird standardmäßig AES verwendet.</p> <p>Bei der Angabe der Option -et wird die Datenbank nicht verschlüsselt. Stattdessen wird die Tabellenverschlüsselung aktiviert. Siehe „<a href="#">Tabellenverschlüsselung</a>“ auf Seite 1437.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Vorsicht</b></p> <p>Achten Sie bei stark verschlüsselten Datenbanken darauf, eine Kopie des Schlüssels an einem sicheren Ort zu verwahren. Wenn Sie den Chiffrierschlüssel verlieren, gibt es keine Möglichkeit, auf die Daten zuzugreifen, auch nicht mit Unterstützung durch den technischen Support. Die Datenbank muss verworfen und eine neue Datenbank muss erstellt werden.</p> </div>
<b>-ep</b>	<p>Gibt an, dass Sie eine stark verschlüsselte Datenbank anlegen wollen, wobei der Chiffrierschlüssel in einem Dialogfeld eingegeben wird. Diese zusätzliche Sicherheitsmaßnahme verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird.</p> <p>Sie müssen den Chiffrierschlüssel ein zweites Mal eingeben, um zu bestätigen, dass die erste Eingabe korrekt war. Wenn die Eingaben nicht übereinstimmen, schlägt die Initialisierung fehl.</p> <p>Bei der Angabe der Option -et wird die Datenbank nicht verschlüsselt. Stattdessen wird die Tabellenverschlüsselung aktiviert.</p> <p>Weitere Hinweise finden Sie unter „<a href="#">Einfache Verschlüsselung und starke Verschlüsselung</a>“ auf Seite 1425.</p>

Option	Beschreibung
<b>-et</b>	<p>Aktiviert die Tabellenverschlüsselung mit dem Verschlüsselungsalgorithmus (und Schlüssel), wie für die -ea-Option angegeben. Verwenden Sie diese Option, wenn Sie verschlüsselte Tabellen anstelle einer Verschlüsselung der Datenbank erstellen möchten. Wenn Sie -et mit -ek oder -ep, aber nicht -ea eingeben, wird der AES-Algorithmus standardmäßig benutzt. Wenn Sie nur die Option -et angeben, wird die einfache Verschlüsselung verwendet.</p> <p>Ein Aktivieren der Tabellenverschlüsselung bedeutet nicht, dass Ihre Tabellen verschlüsselt sind. Sie müssen die Tabellen einzeln nach der Datenbankerstellung verschlüsseln. Siehe <a href="#">„Tabellen verschlüsseln“ auf Seite 1440</a>.</p> <p>Wenn die Tabellenverschlüsselung aktiviert ist, werden Tabellenseiten für die verschlüsselte Tabelle, zugeordnete Indexseiten und Seiten der temporären Tabelle ebenso verschlüsselt wie Transaktionslogseiten, die Transaktionen von verschlüsselten Tabellen enthalten.</p> <p>Im folgenden Beispiel wird die Datenbank <i>new.db</i> erstellt, in der die starke Verschlüsselung für Tabellen aktiviert ist, wobei der Schlüssel "abc" und der AES_FIPS-Verschlüsselungsalgorithmus verwendet werden:</p> <pre>dbinit -et -ek abc -ea AES_FIPS new.db</pre>
<b>-i</b>	<p>Schließt jConnect-Systemobjekte aus der Datenbank aus. Wenn Sie den jConnect-JDBC-Treiber verwenden möchten, um auf Systemkataloginformationen zuzugreifen, müssen Sie die jConnect-Katalogunterstützung installieren (die standardmäßig installiert wird). Wenn Sie diese Option angeben, können Sie weiterhin JDBC verwenden, solange Sie nicht auf Systeminformationen zugreifen. Auf Wunsch können Sie die jConnect-Unterstützung zu einem späteren Zeitpunkt mit Sybase Central oder der ALTER DATABASE-Anweisung hinzufügen.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„jConnect-Systemobjekte in einer Datenbank installieren“ [SQL Anywhere Server - Programmierung]</a>.</p> <p>Wenn Sie eine Datenbank für die Verwendung in Windows Mobile erstellen, finden Sie weitere Hinweise unter <a href="#">„jConnect unter Windows Mobile“ auf Seite 440</a>.</p>
<b>-k</b>	<p>Erstellt die SYSCOLUMNS- und SYSINDEXES-Ansichten nicht. Standardmäßig werden bei der Datenbankerstellung die Ansichten "SYS.SYSCOLUMNS" und "SYS.SYSINDEXES" zur Kompatibilität mit Systemtabellen generiert, die in Watcom SQL (Versionen 4 und älter) verfügbar waren. Diese Anzeigen kollidieren mit den Sybase Adaptive Server Enterprise-Kompatibilitätsansichten dbo.syscolumns und dbo.sysindexes.</p>
<b>-l</b>	<p>Listet die empfohlenen Kollationssequenzen auf und stoppt dann. Es wird keine Datenbank erstellt. Verwenden Sie zum Angeben einer Kollationssequenz die Option -z.</p> <p>Um eine Liste älterer Kollationen anzuzeigen, einschließlich alternativer Kollationen, die aus Gründen der Kompatibilität mit älteren Versionen von SQL Anywhere bereitgestellt werden, und Kollationen für spezielle Zwecke, geben Sie die Option -l+ an.</p>

Option	Beschreibung
<b>-le</b>	<p>Listet die verfügbaren Zeichensatzkodierungen auf und stoppt dann. Es wird keine Datenbank erstellt. Jede Zeichensatzkodierung wird durch eine oder mehrere Bezeichnungen (Labels) gekennzeichnet. Es gibt Zeichenfolgen, mit denen die Kodierung gekennzeichnet werden kann. Jede Zeile im angezeigten Text listet das Kodierungslabel und alternative Bezeichnungen auf, anhand derer die Kodierung identifiziert werden kann. Diese Bezeichnungen gehören zu einer von mehreren allgemeinen Kategorien: SA (das SQL Anywhere-Label), IANA (Internet Assigned Numbers Authority), MIME (Multipurpose Internet Mail Extensions), ICU (International Components for Unicode), JAVA oder ASE (Adaptive Server Enterprise).</p> <p>Um eine Liste von Zeichensatzkodierungen mit den alternativen Labels anzuzeigen, geben Sie die Option <code>-le+</code> an.</p> <p>Wenn das Dienstprogramm <code>dbinit</code> die Zeichensatzkodierung ausgibt, handelt es sich immer um die SQL Anywhere-Version des Labels. Beispiel: Der folgende Befehl gibt die CHAR-Zeichensatzkodierung <code>windows-1250</code> zurück:</p> <pre>dbinit -ze cp1250 -z uca test.db</pre>
<b>-m file-name</b>	Erstellt einen Transaktionslogspiegel. Ein Transaktionslogspiegel ist eine identische Kopie eines Transaktionslogs, die normalerweise auf einem getrennten Medium gehalten wird, um die Daten besser zu schützen. Standardmäßig verwendet SQL Anywhere keinen Transaktionslogspiegel.
<b>-n</b>	Erstellt eine Datenbank ohne Transaktionslog. Wenn Sie eine Datenbank ohne Transaktionslog erstellen, sparen Sie Festplattenspeicher, müssen aber mit geringerer Performance rechnen, weil bei jedem Festschreiben ein Checkpoint gesetzt wird. Wenn Ihre Datenbank beschädigt wird und Sie kein Transaktionslog haben können die Daten nicht wiederhergestellt werden. Das Transaktionslog ist zur Daten-Replikation erforderlich und bietet beim Ausfall eines Datenträgers oder Systems zusätzliche Sicherheit für Datenbankinformationen.
<b>-o file-name</b>	Schreibt Ausgabemeldungen in die benannte Datei.

Option	Beschreibung
<b>-p</b> <i>page-size</i> [ <b>k</b> ]	<p>Gibt die Seitengröße für die Datenbank an. Die Seitengröße (in Byte) kann für eine Datenbank 2048, 4096, 8192, 16384 oder 32768 betragen, wobei 4096 der Standardwert ist. Verwenden Sie <b>k</b>, um die Einheit KByte festzulegen (zum Beispiel -p 4k).</p> <p>Größere Seiten bringen im Allgemeinen bei großen Datenbanken Vorteile. So ist zum Beispiel die Anzahl der zum Durchsuchen einer Tabelle erforderlichen I/O-Vorgänge geringer, weil jeweils eine ganze Seite eingelesen wird. Es gibt bei großen Seiten allerdings zusätzliche Speicheranforderungen. Es wird dringend empfohlen, dass Sie die Performance testen (und sonstige Tests durchführen), wenn Sie eine Seitengröße wählen. Danach wählen Sie die kleinste Seitengröße, die zufriedenstellende Ergebnisse liefert. Für die meisten Anwendungen sind Seitengrößen von 16 kB oder 32 kB nicht zu empfehlen. Verwenden Sie in Produktionssystemen keine Seitengrößen von 16 kB oder 32 kB, außer wenn Sie sicher sind, dass immer ein großer Datenbankserver-Cache verfügbar ist, und Sie die Kompromisse bei Speicher- und Festplattenplatz gegen die Performance-Eigenschaften abgewägt haben. Wenn eine große Anzahl von Datenbanken auf einem Server gestartet wird, sollten Sie eine angemessene Seitengröße wählen.</p> <p>Siehe:</p> <ul style="list-style-type: none"> <li>• „Tipp: Angemessene Seitengröße verwenden“ [<a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a>]</li> </ul>
<b>-pd</b>	<p>Legt fest, dass Systemprozeduren vor Version 16.0, die mit Privilegien verbundene Vorgänge durchführen, mit den Privilegien des Definierers (Eigentümers) ausgeführt werden, nicht mit denjenigen des Aufrufers. Wenn -pd angegeben wird, benötigt ein Benutzer zum Ausführen dieser Systemprozeduren keine zusätzlichen Privilegien außer dem EXECUTE-Privileg für die Prozeduren. Diese Einstellung wirkt sich nicht auf Systemprozeduren aus, die in Version 16.0 oder später hinzugefügt wurden und mit Privilegien verbundene Vorgänge durchführen, und auch nicht auf das Standardverhalten für benutzerdefinierte Prozeduren, die sich weiterhin nach dem Definierer richten. Eine Liste dieser Prozeduren finden Sie unter „<a href="#">Systemprozeduren vor Version 16.0 als Aufrufer oder Definierer ausführen</a>“ [<a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a>].</p>
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.

Option	Beschreibung
<b>-s</b> [ - ]	<p>Fügt globale Prüfsummen hinzu (eine Prüfsumme wird jeder Datenbankseite hinzugefügt). Standardmäßig ist diese Option aktiviert. Mit Prüfsummen kann festgestellt werden, ob eine Datenbankseite auf der Festplatte geändert wurde. Wenn Sie eine Datenbank mit aktivierten globalen Prüfsummen erstellen, berechnet das System eine Prüfsumme, direkt bevor eine Datenbankseite auf die Festplatte geschrieben wird. Wenn die Seite von der Festplatte gelesen wird, ermittelt das System die Prüfsumme erneut und vergleicht sie mit dem auf der Seite gespeicherten Wert. Wenn die Prüfsummen unterschiedlich sind, wurde die Seite auf der Festplatte geändert oder beschädigt und ein Fehler tritt auf. Bei kritischen Datenbankseiten werden immer Prüfsummen durch den Datenbankserver berechnet, unabhängig vom Wert der Option -s.</p> <p>Prüfsummen sind für Datenbanken automatisch aktiviert, die auf Windows Mobile und bestimmten Speichermedien wie z.B. Wechseldatenträgern laufen, damit eine Früherkennung von möglichen Datenbankbeschädigungen möglich ist.</p> <p>Wenn eine Datenbank mit deaktivierten globalen Prüfsummen erstellt wird, können Sie Seiten, während sie geschrieben werden, weiterhin mit der Option -wc oder der START DATABASE-Anweisung Prüfsummen hinzufügen. Siehe <a href="#">„Erkennung von Beschädigungen mithilfe von Prüfsummen“</a> auf Seite 1084.</p>
<b>-t</b> <i>transaction-log-name</i>	<p>Gibt den Namen der Transaktionslogdatei an. Das Transaktionslog ist eine Datei, in der der Datenbankserver alle von allen Benutzern durchgeführten Änderungen protokolliert. Hierbei ist es gleichgültig, welche Anwendung verwendet wird. Das Transaktionslog spielt eine entscheidende Rolle beim Sichern und Wiederherstellen sowie bei der Datenreplikation. Wenn der Dateiname keinen Pfad hat, wird es in dasselbe Verzeichnis wie die Datenbankdatei platziert. Wenn Sie dbinit ausführen, ohne die Option -t oder -n anzugeben, wird ein Transaktionslog mit demselben Dateinamen wie die Datenbankdatei erstellt, jedoch mit der Erweiterung .log.</p> <p>Weitere Hinweise finden Sie unter <a href="#">„Das Transaktionslog“</a> auf Seite 135.</p>

Option	Beschreibung
<b>-z coll</b> [ <i>collation-tailoring-string</i> ]	<p>Gibt die Kollationssequenz für die Datenbank an. Die Kollationssequenz wird zum Sortieren und Vergleichen von Zeichendatentypen (CHAR, VARCHAR und LONG VARCHAR) verwendet. Die Kollation liefert Zeichenvergleichs- und Sortierinformationen für die verwendete Kodierung (Zeichensatz). Es ist wichtig, dass Sie Ihre Kollation mit Umsicht auswählen. Sie kann nach der Erstellung der Datenbank nicht mehr geändert werden, außer durch Entladen und Neuladen der Datenbank. Wenn keine Kollation angegeben ist, verwendet SQL Anywhere eine auf Sprache und Zeichensatz des Betriebssystems basierende Kollation. Hinweise zum Anzeigen der verfügbaren Kollationssequenzen finden Sie unter der Option -l.</p> <p>Siehe:</p> <ul style="list-style-type: none"> <li>• „Hinweise zur Kollation“ auf Seite 522</li> <li>• „Empfohlene Zeichensätze und Kollationen“ auf Seite 529</li> <li>• „Alternative Kollationen“ auf Seite 518</li> </ul> <p>Optional können Sie Optionen der Kollationsanpassung (<i>collation-tailoring-string</i>) für eine zusätzliche Steuerung bei Zeichensortierungen und -vergleichen angeben. Diese Optionen werden in der Form von Schlüsselwort=Wert-Paaren, die in Klammern gesetzt werden, hinter dem Kollationsnamen angegeben. Zum Beispiel:</p> <pre>dbinit -c -z uca(locale=es;case=LowerFirst) spanish2.db</pre> <p>Siehe „Optionen der Kollationsanpassung“ auf Seite 523.</p> <p>In <i>collation-tailoring-string</i> angegebene Einstellungen für Groß- und Kleinschreibung sowie Akzente heben die entsprechenden Optionen für dbinit (-c, -a und -af) auf, sofern Sie beides angeben.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b></p> <p>Datenbanken, die mit Optionen der Kollationsanpassung initialisiert wurden, können nicht von einem Datenbankserver einer früheren Version als 10.0.1 gestartet werden.</p> </div>
<b>-ze encoding</b>	<p>Gibt die Kodierung für die Kollation an. Die meisten mit -z angegebenen Kollationen legen sowohl die Kodierung (Zeichensatz) als auch die Reihenfolge fest. Bei diesen Kollationen sollte Option -ze nicht angegeben werden.</p> <p>Wenn die durch die Option -z angegebene Kollation UCA (Unicode Collation Algorithm) ist, kann die Option -ze UTF-8 oder eine beliebige Einbyte-Kodierung für CHAR-Datentypen angeben. Standardmäßig verwendet SQL Anywhere UTF-8. Verwenden Sie die Option -ze, damit eine sprachumgebungsspezifische Kodierung festgelegt und die Vorteile des UCAs bei Vergleichen und Sortierungen erhalten bleiben.</p>

Option	Beschreibung
<b>-zn coll</b> [ <i>collation-tailoring-string</i> ]	<p>Gibt die Kollationssequenz an, die zum Sortieren und Vergleichen von nationalen Zeichendatentypen (NCHAR, NVARCHAR und LONG NVARCHAR) verwendet wird. Die Kollation liefert Zeichen-Sortierinformationen für die verwendete UTF-8-Kodierung (Zeichensatz). Werte sind UCA (Standardwert) oder UTF8BIN. Mit UTF8BIN wird eine binäre Sortierung aller Zeichen erstellt, deren Kodierung größer als 0x7E ist. Wenn die DLLs dbicu16 und dbicudt16 nicht installiert sind, ist die NCHAR-Standardkollation UTF8BIN. Siehe <a href="#">„Hinweise zur Kollation“ auf Seite 522</a>.</p> <p>Optional können Sie Optionen der Kollationsanpassung (<i>Zeichenfolge_zur_Kollationsanpassung</i>) für eine zusätzliche Steuerung bei Zeichensortierungen und -vergleichen angeben. Diese Optionen werden in der Form von Schlüsselwort=Wert-Paaren, die in Klammern gesetzt werden, hinter dem Kollationsnamen angegeben. Zum Beispiel:</p> <pre>dbinit -c -zn UCA(case=LowerFirst) sens.db</pre> <p>Siehe <a href="#">„Optionen der Kollationsanpassung“ auf Seite 523</a>.</p> <p>In <i>collation-tailoring-string</i> angegebene Einstellungen für Groß- und Kleinschreibung sowie Akzente heben die entsprechenden Optionen für dbinit (-c, -a und -af) auf, sofern Sie beides angeben.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b> Datenbanken, die mit Optionen der Kollationsanpassung initialisiert wurden, können nicht von einem Datenbankserver einer früheren Version als 10.0.1 gestartet werden.</p> </div>

**Privilegien**

Keine.

**Bemerkungen**

Bei der Initialisierung werden mehrere Datenbankattribute festgelegt. Diese können später nicht geändert werden, es sei denn durch Entladen, Reinitialisieren und Neuaufbau der gesamten Datenbank. Die Datenbankattribute sind die Folgenden:

- Berücksichtigung von Groß-/Kleinschreibung oder nicht
- Akzent-Berücksichtigung oder nicht
- Berücksichtigung der Satzzeichen
- Behandeln von nachgestellten Leerzeichen in Vergleichen
- Seitengröße
- Zeichensatzkodierung oder Kollationssequenz
- Datenbankverschlüsselung
- Tabellenverschlüsselung

Zum Beispiel kann die Datenbank *test.db* mit der Seitengröße von 8192 Byte wie folgt erstellt werden:

```
dbinit -p 8192 test.db
```

Meldungen an den Client enthalten die Angabe, welcher Typ der Datenbankverschlüsselung für die Datenbank verwendet wird. Bei Verschlüsselung wird außerdem der verwendete Algorithmus angezeigt.

Sie können einer Datenbank nicht den Namen **utility\_db** geben. Dieser Name ist für die Dienstprogrammdatenbank reserviert. Siehe „[Die Dienstprogrammdatenbank](#)“ auf Seite 145.

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

Wenn Sie Optionen der Kollationsanpassung im Initialisierungsbefehl festlegen, können Sie nicht "Quaternär" bei der Berücksichtigung von Satzzeichen angeben, wenn die Datenbank keine Berücksichtigung von Groß-/Kleinschreibung und Akzenten hat.

Zusätzlich wird bei der Initialisierung ausgewählt, ob ein Transaktionslog und ein Transaktionslogspiegel verwendet werden. Diese Auswahl kann später mithilfe des Transaktionslog-Dienstprogramms oder der Anweisung ALTER DATABASE geändert werden.

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „[Getrennt lizenzierbare Komponenten](#)“ [*SQL Anywhere 16 - Einführung*].

Sie können eine Datenbank auch auf folgende Weisen erstellen:

- In Sybase Central verwenden Sie den **Assistenten zum Erstellen einer Datenbank**.
- Bei Interactive SQL verwenden Sie die CREATE DATABASE-Anweisung.

### Hinweis

Beim Deployment von Anwendungen ist der Personal Datenbankserver (dbeng16) erforderlich, um Datenbanken mithilfe des Dienstprogramms dbinit erstellen zu können. Er ist auch erforderlich, wenn Sie Datenbanken von Sybase Central aus auf dem lokalen Computer erstellen und keine anderen Datenbankserver ausgeführt werden.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlslag).

**Siehe auch**

- „Datenbanken erstellen (Dienstprogramm dbinit)“ auf Seite 126
- „Datenbanken erstellen (Sybase Central)“ auf Seite 125
- „Prozeduren und Funktionen zum Ausführen mit Eigentümer- oder Aufruferprivilegien einrichten“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]

**Beispiel**

Der folgende Befehl erstellt die Datenbank *spanish.db*, die die Groß- und Kleinschreibung berücksichtigt und die 1252spa-Kollation für Nicht-NCHAR-Daten verwendet. Für NCHAR-Daten werden die UCA-Kollation, die Sprachumgebung "es" und die Sortierung "LowerFirst" (Kleinbuchstaben zuerst) festgelegt.

```
dbinit -c -z 1252spa -zn uca(locale=es;case=LowerFirst) spanish.db
```

Der folgende Befehl erstellt eine Datenbank mit griechischer Kollation.

```
dbinit -z 1253ELL mydb.db
```

## Interactive SQL-Dienstprogramm (dbisql)

Führt in einer Datenbank SQL-Anweisungen und Skriptdateien aus.

**Syntax**

```
dbisql -c "connection-string" [ options ] [ dbisql-statement | dbisql-script-file ]
```

*dbisql-statement*: Eine SQL-Anweisung oder eine Reihe von durch ein Befehlstrennzeichen getrennten SQL-Anweisungen.

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.</p> <p>Wenn die Umgebungsvariable und die Konfigurationsdatei denselben Namen haben, wird die Umgebungsvariable verwendet. Siehe „Konfigurationsdateien“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922.</p>

Option	Beschreibung
<b>-c</b> <i>"keyword=value; ..."</i>	Legt Verbindungsparameter fest. Wenn Interactive SQL keine Verbindung herstellen kann, erscheint ein Fenster, in das Sie die Verbindungsparameter eingeben können. Wenn Sie keine Benutzer-ID und kein Kennwort angeben, werden die Standardbenutzer-ID <b>DBA</b> und das Standardkennwort <b>sql</b> verwendet. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
<b>-d</b> <i>delimiter</i>	Gibt ein Befehlstrennzeichen an. Anführungszeichen um das Trennzeichen sind optional und nur dann erforderlich, wenn die Befehlsebene selbst das Trennzeichen auf spezielle Art interpretiert.  Diese Option setzt die Einstellung der Option <code>command_delimiter</code> außer Kraft. Siehe „ <a href="#">command_delimiter-Option [Interactive SQL]</a> “ auf Seite 854.
<b>-d1</b>	Zeigt alle vom Benutzer explizit ausgeführten Anweisungen im Befehlsfenster an (STDOUT). Dadurch erhalten Sie nützliche Informationen bei der Fehlersuche in SQL-Skripten, oder wenn Interactive SQL umfangreiche SQL-Skripten verarbeitet. (Das letzte Zeichen ist die Ziffer 1 und nicht ein "L" in Kleinschreibung.) Diese Option ist nur verfügbar, wenn Sie SQL als Befehlszeilenprogramm ausführen.
<b>-datasource</b> <i>DSN-name</i>	Legt eine ODBC-Datenquelle zum Verbinden fest.

Option	Beschreibung
<b>-f</b> <i>filename</i>	<p>Öffnet die Datei <i>Dateiname</i> im Fensterausschnitt "SQL-Anweisungen" (führt sie aber nicht aus).</p> <p>Wenn die Option -f angegeben ist, wird die Option -c ignoriert, d.h. dass keine Verbindung zur Datenbank hergestellt wird.</p> <p>Der Dateiname kann in Anführungszeichen gesetzt sein. Dies <i>muss</i> erfolgen, wenn der Dateiname eine Leerstelle enthält.</p> <p>Wenn die Datei nicht vorhanden oder eigentlich ein Verzeichnis und keine Datei ist, gibt DBISQL eine Fehlermeldung aus und wird beendet.</p> <p>Wenn der Dateiname keine volle Laufwerks- und Pfadangabe enthält, wird angenommen, dass die Datei im aktuellen Verzeichnis liegt.</p> <p>Diese Option wird nur unterstützt, wenn Interactive SQL als Fensteranwendung ausgeführt wird.</p>
<b>-host</b> <i>hostname</i>	<p>Gibt den <i>hostnamen</i> oder die IP-Adresse des Computers an, auf dem der Datenbankserver läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen.</p>
<b>-nogui</b>	<p>Führt Interactive SQL als Konsolenanwendung aus, ohne das Fenster der Benutzeroberfläche zu verwenden. Dies ist für Batch-Vorgänge nützlich.</p> <p>Wenn Sie entweder <i>dbisql-statement</i> oder <i>dbisql-script-file</i> angeben, wird die Option -nogui angenommen.</p> <p>In diesem Modus setzt Interactive SQL den Code zum Beenden des Programms, um Erfolg oder Scheitern zu melden. Bei Windows-Betriebssystemen wird die Umgebungsvariable ERRORLEVEL auf den Code zum Beenden des Programms gesetzt. Siehe „Exit-Codes der Softwarekomponenten“ [<a href="#">SQL Anywhere Server - Programmierung</a>].</p>

Option	Beschreibung
<b>-onerror</b> { <b>continue</b>   <b>exit</b> }	<p>Steuert, was passiert, wenn während des Lesens von Anweisungen aus einer Skriptdatei ein Fehler auftritt. Dies ist von Vorteil, wenn Interactive SQL in Batch-Vorgängen verwendet wird. Diese Option setzt die Einstellung von <code>on_error</code> außer Kraft. Siehe „<a href="#">on_error-Option [Interactive SQL]</a>“ auf Seite 865.</p> <p>Definieren Sie einen der folgenden unterstützten Werte für das <i>Verhalten</i>:</p> <ul style="list-style-type: none"><li>● <b>Continue</b> Der Fehler wird ignoriert und Interactive SQL fährt mit der Ausführung der Anweisungen fort.</li><li>● <b>Exit</b> Interactive SQL wird beendet.</li></ul>
<b>-port</b> <i>port-number</i>	<p>Gibt die Portnummer des laufenden SQL Anywhere-Datenbankservers an. Die Standard-Portnummer für SQL Anywhere ist 2638.</p>
<b>-q</b>	<p>Unterdrückt die Ausgabe von Meldungen. Führt das Dienstprogramm im stillen Modus aus. Dies ist nur dann nützlich, wenn Sie Interactive SQL mit einer Anweisung oder einer Skriptdatei starten. Das Angeben dieser Option unterdrückt keine Fehlermeldungen, sondern Folgendes:</p> <ul style="list-style-type: none"><li>● Warnungen und andere nicht-schwerwiegende Meldungen</li><li>● Die Ausgabe von Ergebnismengen</li></ul>

Option	Beschreibung
<b>-ul</b>	<p>Gibt an, dass UltraLite-Datenbanken Standardvorgabe sind. Interactive SQL passt die Ihnen verfügbaren Optionen abhängig vom Typ der Datenbank an, mit der Sie verbunden sind.</p> <p>Standardmäßig nimmt Interactive SQL an, dass Sie mit SQL Anywhere-Datenbanken verbunden sind. Wenn Sie die Option -ul angeben, ändert sich der Standard zu UltraLite-Datenbanken. Unabhängig von dem als Standard festgelegten Datenbanktyp können Sie eine Verbindung zu einer SQL Anywhere- oder zu einer UltraLite-Datenbank herstellen, indem Sie den Datenbanktyp aus der Dropdown-Liste <b>Datenbanktyp ändern</b> im Fenster <b>Verbinden</b> auswählen.</p> <p>Weitere Hinweise zum Herstellen einer Verbindung mit UltraLite-Datenbanken von Interactive SQL aus finden Sie unter „<a href="#">Interactive SQL-Dienstprogramm für UltraLite (dbisql)</a>“ [<a href="#">UltraLite - Datenbankverwaltung</a>].</p>
<b>-version</b>	<p>Zeigt die Versionsnummer von Interactive SQL an. Sie können die Versionsnummer auch in Interactive SQL anzeigen, indem Sie im Menü <b>Hilfe</b> auf <b>Info über Interactive SQL</b> klicken.</p>
<b>-x</b>	<p>Durchsucht Anweisungen, führt sie aber nicht aus. Dies ist nützlich, um lange Skriptdateien auf Syntaxfehler zu überprüfen.</p> <p>Ausführliche Beschreibungen von SQL-Anweisungen und Anweisungen in Interactive SQL finden Sie unter „<a href="#">SQL-Sprachelemente</a>“ [<a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a>].</p>
<i>dbisql-statement</i>   <i>dbisql-script-file</i>	<p>Führt die SQL-Anweisung bzw. die angegebene <i>dbisql-Skriptdatei</i> aus.</p> <p>Wenn Sie weder <i>dbisql-statement</i> noch <i>dbisql-script-file</i> angeben, wechselt Interactive SQL in den interaktiven Modus, in dem Sie eine Anweisung in ein Befehlsfenster eingeben können.</p>

### Bemerkungen

Mit Interactive SQL können Sie die Datenbank durchsuchen sowie SQL-Anweisungen und Skriptdateien ausführen. Sie erhalten auch Rückmeldungen zu folgenden Elementen:

- Anzahl der betroffenen Zeilen
- Für jede Anweisung benötigte Zeit
- Ausführungsplan von Abfragen
- Etwaige Fehlermeldungen

Sie können sich nicht sowohl mit SQL Anywhere- als auch mit UltraLite-Datenbanken verbinden. Weitere Hinweise zum Herstellen einer Verbindung zu UltraLite-Datenbanken finden Sie unter „Interactive SQL-Dienstprogramm für UltraLite (dbisql)“ [[UltraLite - Datenbankverwaltung](#)].

Interactive SQL wird unter Windows, Solaris, Linux und Mac OS X unterstützt. Weitere Hinweise finden Sie unter <http://www.sybase.com/detail?id=1061806>.

Für Windows gibt es zwei Programmdateien:

1. Batch-Skripten sollten *dbisql* oder *dbisql.com* anstelle von *dbisql.exe* aufrufen. Die Programmdatei *dbisql.com* ist als Konsolenanwendung gelinkt.
2. Die Programmdatei *dbisql.exe* ist als Fensteranwendung gelinkt und blockiert die Befehls-Shell, aus der sie gestartet wurde, nicht. Wenn *dbisql.exe* aus einer Batchdatei ausgeführt wird, sehen Sie keine Ausgabedaten in der Standardausgabe oder in den Standard-Fehlerdateien.

Die Standardkodierung für Interactive SQL kann auch temporär mit der Option `default_isql_encoding` gesetzt werden. Siehe „[default\\_isql\\_encoding-Option \[Interactive SQL\]](#)“ auf Seite 856.

Sie können die Kodierung angeben, die zum Lesen und Schreiben von Dateien verwendet werden soll, indem Sie die `ENCODING`-Klausel der `INPUT`-, `OUTPUT`- oder `READ`-Anweisung verwenden. Siehe:

- „[INPUT-Anweisung \[Interactive SQL\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „[OUTPUT-Anweisung \[Interactive SQL\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „[READ-Anweisung \[Interactive SQL\]](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

Beendigungscode 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag). Beendigungscode ungleich Null werden nur verwendet, wenn Interactive SQL im Batchmodus verwendet wird (mit einer Befehlszeile, die eine SQL-Anweisung oder den Namen einer Skriptdatei verwendet). Siehe „[Exit-Codes der Softwarekomponenten](#)“ [[SQL Anywhere Server - Programmierung](#)].

Wenn Sie eine *reload.sql*-Datei mit Interactive SQL ausführen, müssen Sie den Chiffrierschlüssel als Parameter angeben. Wenn Sie den Schlüssel nicht in der `READ`-Anweisung übergeben, werden Sie von Interactive SQL aufgefordert, den Schlüssel bereitzustellen.

Sie können Interactive SQL auf folgende Arten starten:

- Von Sybase Central aus, indem Sie auf **Datei » Interactive SQL öffnen** klicken.
- Vom Menü **Start** aus, indem Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Interactive SQL** klicken.
- Indem Sie den dbisql-Befehl an einer Eingabeaufforderung ausführen.

### Siehe auch

- „SQL-Anweisungen für Interactive SQL“ auf Seite 821
- „Interactive SQL“ auf Seite 814

### Beispiel

Mit dem folgenden Befehl wird die Skriptdatei *mycom.sql* auf dem aktuellen Standardserver ausgeführt. Dabei werden die Benutzer-ID "DBA" und das Kennwort "sql" verwendet. Wenn in der Skriptdatei ein Fehler auftritt, wird der Prozess heruntergefahren.

```
dbisql -c "UID=DBA;PWD=sql" -onerror exit mycom.sql
```

Der folgende Befehl fügt einen Benutzer der aktuellen Standarddatenbank hinzu:

```
dbisql -c "UID=DBA;PWD=sql" CREATE USER joe IDENTIFIED BY passwd
```

## Schlüsselpaargenerator-Dienstprogramm (createkey)

Erstellt RSA-Schlüsselpaare, die bei der Ende-zu-Ende-Verschlüsselung von MobiLink verwendet werden.

### Syntax

**createkey**

### Bemerkungen

Wenn Sie createkey ausführen, werden Sie zur Eingabe der folgenden Informationen aufgefordert:

- **Länge des RSA-Schlüssels eingeben (512-16384)** Diese Eingabeaufforderung wird nur angezeigt, wenn Sie RSA-Verschlüsselung wählen. Sie können eine Länge zwischen 512 und 16.384 Bit wählen.
- **Dateipfad zum Speichern des öffentlichen Schlüssels eingeben** Geben Sie einen Dateinamen und einen Speicherort für den generierten, PEM- oder DER-kodierten öffentlichen Schlüssel an. Diese Datei wird auf dem MobiLink-Client mit der Protokolloption e2ee\_public\_key angegeben. Siehe „e2ee\_public\_key“ [[MobiLink - Clientadministration](#)].
- **Dateipfad zum Speichern des privaten Schlüssels eingeben** Geben Sie einen Dateinamen und einen Speicherort für den generierten, PEM- oder DER-kodierten privaten Schlüssel an. Diese Datei wird auf dem MobiLink-Server mit der Protokolloption e2ee\_private\_key angegeben. Siehe „mlsrv16-Option -x“ [[MobiLink - Serveradministration](#)].
- **Kennwort zum Schutz des privaten Schlüssels eingeben** Optional können Sie ein Kennwort zum Verschlüsseln des privaten Schlüssels angeben. Der private Schlüssel wird nicht verschlüsselt,

wenn Sie kein Kennwort angeben. Dieses Kennwort wird auf dem MobiLink-Server mit der Protokolloption `e2ee_private_key_password` angegeben. Siehe „[mlsrv16-Option -x](#)“ [*MobiLink - Serveradministration*].

**Privilegien**

Keine.

**Siehe auch**

- „Ende-zu-Ende-Verschlüsselung“ auf Seite 1459

**Beispiel**

Das folgende Beispiel erstellt ein RSA-Schlüsselpaar:

```
createkey
SQL Anywhere Schlüsselpaargenerator Version
16.0.1304 Verschlüsselungstyp wählen ((R)SA oder (E)CC): r
Länge des RSA-Schlüssels eingeben (512-16384): 2048
Schlüsselpaar wird generiert...
Dateipfad zum Speichern des öffentlichen Schlüssels eingeben: rsapublic.pem
Dateipfad zum Speichern des privaten Schlüssels eingeben: rsaprivate.pem
Kennwort zum Schutz des privaten Schlüssels eingeben: pwd
```

**Dienstprogramm für die Sprachauswahl (dblang)**

Gibt Auskunft über die Registrierungseinstellungen der von SQL Anywhere, Sybase Central und Interactive SQL verwendeten Sprachen und ändert sie.

**Syntax**

```
dblang [ options ] language-code
```

Option	Beschreibung
-m	Schreibt den Sprachcode in die Registrierung unter HKEY_LOCAL_MACHINE.
-q	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
-u	Schreibt den Sprachcode in die Registrierung unter HKEY_CURRENT_USER. Dies ist der Standardspeicherort.

Sprachcode	Sprache
EN	Englisch
DE	Deutsch
ES	Spanisch
FR	Französisch

Sprachcode	Sprache
IT	Italienisch
JA	Japanisch
KO	Koreanisch
LT	Litauisch
PL	Polnisch
PT	Portugiesisch
RU	Russisch
TW	Traditionelles Chinesisch
UK	Ukrainisch
ZH	Vereinfachtes Chinesisch

### Privilegien

Keine.

### Bemerkungen

Wenn Sie -m oder -u nicht angeben, wird der Sprachcode in die Registrierung unter HKEY\_CURRENT\_USER geschrieben. Sie können sowohl -m als -u angeben, um den Sprachcode in beide Registrierungsabschnitte zu schreiben.

Das Ausführen des Dienstprogramms dblang ohne Landescode gibt die aktuellen Einstellungen zurück. Das sind die folgenden:

- **SQL Anywhere** Diese Einstellung steuert, welche Sprachenressourcenbibliothek verwendet wird, um Meldungen und Fehlermeldungen des SQL Anywhere-Datenbankservers zu übermitteln. Die Sprachenressourcenbibliothek ist eine DLL mit einem Namen im Format *dblgXX16.dll*, wobei *XX* ein Sprachcode aus zwei Buchstaben ist.

Stellen Sie sicher, dass Sie die entsprechende Sprachenressourcenbibliothek auf Ihrem System installiert haben, wenn Sie die Einstellungen ändern.

- **Sybase Central und Interactive SQL** Diese Einstellung steuert die Ressourcen, die zur Anzeige von Elementen der Benutzeroberfläche bei Sybase Central und Interactive SQL verwendet werden.

#### Hinweis

Änderungen an Spracheinstellungen werden von Sybase Central oder Interactive SQL erst erkannt, wenn das grafische Administrationstool geschlossen und wieder geöffnet wird.

BeendigungsCodes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag).

Dieses Dienstprogramm akzeptiert den *-Parameter zum Einlesen von Optionen aus einer Konfigurationsdatei* nicht **@data**.

**Siehe auch**

- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]
- „SALANG-Umgebungsvariable“ auf Seite 473
- „Verbindungsparameter Language (LANG)“ auf Seite 368

**Beispiel**

Der folgende Befehl zeigt ein Fenster mit den neuen Einstellungen:

```
dblang
```

Der folgende Befehl ändert die Einstellungen auf Deutsch und zeigt ein Dialogfeld mit den vorherigen und den neuen Einstellungen an:

```
dblang de
```

# Dienstprogramm zur Logkonvertierung (dbtran)

Konvertiert ein Transaktionslog in eine SQL-Skriptdatei.

**Syntax**

Mit einem Datenbankserver ausführen:

```
dbtran [ options ] -c { connection-string } -n SQL-script-file
```

Mit einem Transaktionslog ausführen:

```
dbtran [ options ] [ transaction-log ] [ SQL-script-file ]
```

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>

Option	Beschreibung
<b>-a</b>	<p>Steuert, ob nicht festgeschriebene Transaktionen im Transaktionslog erscheinen.</p> <p>Standardmäßig enthält das Transaktionslog nur Änderungen, die festgeschrieben wurden. Änderungen, die zurückgesetzt oder nach dem letzten COMMIT durchgeführt wurden, sind nicht im Transaktionslog enthalten.</p> <p>Wenn die Option -a angegeben ist, werden alle im Transaktionslog gefundenen, nicht festgeschriebenen Transaktionen ausgegeben, gefolgt von einer ROLL-BACK-Anweisung.</p>
<b>-c</b> "key-word=value; ..."	Gibt die Verbindungszeichenfolge an, wenn das Dienstprogramm in einem Datenbankserver läuft. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
<b>-d</b>	Gibt an, dass die Transaktionen in der Reihenfolge von frühester bis letzter Transaktion geschrieben werden. Diese Funktion wird hauptsächlich dann verwendet, wenn ein Auditing der Datenbankaktivität durchgeführt wird. Die Ausgabe von dbtran darf nicht in einer Datenbank angewendet werden.
<b>-ek</b> key	<p>Gibt den Chiffrierschlüssel für stark verschlüsselte Datenbanken an. Wenn Sie mit einer stark verschlüsselten Datenbank arbeiten, müssen Sie den Chiffrierschlüssel angeben, bevor Sie die Datenbank oder das Transaktionslog verwenden können.</p> <p>Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie nicht den richtigen Chiffrierschlüssel angeben.</p> <p>Wenn Sie dbtran auf einem Datenbankserver unter Verwendung der Option -c ausführen, achten Sie darauf, dass Sie den Schlüssel mit einem Verbindungsparameter und nicht mit der Option -ek festlegen. Beispiel: Der folgende Befehl holt Transaktionslogdaten über die Datenbank <i>myenc.db</i> vom Server <b>sample</b> und speichert seine Ausgabe in <i>log.sql</i>.</p> <pre>dbtran -n log.sql -c "Server=sample;DBF=myenc.db; UID=DBA;PWD=sql;DBKEY=mykey"</pre>

Option	Beschreibung
<b>-ep</b>	<p>Fordert zur Eingabe des Chiffrierschlüssels auf. Diese Option öffnet ein Fenster, in das Sie den Chiffrierschlüssel eingeben. Diese zusätzliche Sicherheitsmaßnahme verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird.</p> <p>Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie nicht den richtigen Chiffrierschlüssel angeben.</p> <p>Wenn Sie dbtran auf einem Datenbankserver unter Verwendung der Option -c ausführen, achten Sie darauf, dass Sie den Schlüssel mit einem Verbindungsparameter und nicht mit der Option -ep festlegen. Beispiel: Der folgende Befehl holt Transaktionslogdaten über die Datenbank <i>myenc.db</i> vom Server <b>sample</b> und speichert seine Ausgabe in <i>log.sql</i>.</p> <pre>dbtran -n log.sql -c "Server=sample;DBF=myenc.db;UID=DBA;PWD=sql;DBKEY=mykey"</pre>
<b>-f</b>	Gibt nur Transaktionen aus, die seit dem letzten Checkpoint abgeschlossen wurden.
<b>-g</b>	<p>Fügt Audit-Daten dem Transaktionslog hinzu, wenn die auditing-Datenbankoption aktiviert ist. Sie können diese Informationen mit dieser Option in die Ausgabe datei als Kommentare eintragen. Siehe „<a href="#">auditing-Option</a>“ auf Seite 582.</p> <p>Die Option -g impliziert die Optionen -a, -d und -t.</p>
<b>-ir</b> <i>offset1,offset2</i>	Gibt einen Teil des Transaktionslogs zwischen zwei angegebenen Ausgangspunkten aus.
<b>-is</b> <i>source,...</i>	<p>Gibt Vorgänge in Zeilen aus, die durch Vorgänge von einer oder mehreren der folgenden Quellen geändert wurden. Angabe in einer durch Kommas unterteilten Liste:</p> <ul style="list-style-type: none"> <li>• <b>All</b> Alle Zeilen. Dies ist die Standardeinstellung.</li> <li>• <b>SQLRemote</b> Nur Zeilen einbeziehen, die mithilfe von SQL Remote geändert wurden. Sie können auch das kurze Format SR verwenden.</li> <li>• <b>Local</b> Nur Zeilen einbeziehen, die nicht repliziert werden.</li> </ul>
<b>-it</b> <i>owner.table,...</i>	Gibt die Vorgänge in der angegebenen kommasetrennten Liste von Tabellen aus. Jede Tabelle muss im folgenden Format angegeben werden: <i>owner.table</i> .

Option	Beschreibung
<b>-j</b> <i>date/time</i>	Konvertiert nur Transaktionen vom letzten Checkpoint vor einem angegebenen Datum und/oder einer angegebenen Uhrzeit. Das vom Benutzer angegebene Argument kann ein Datum, eine Zeit oder eine in Anführungszeichen eingeschlossene Angabe von Datum und Zeit sein. Wenn die Zeit nicht angegeben ist, wird die Zeit zu Beginn des Tages angenommen. Wenn das Datum nicht angegeben ist, wird der aktuelle Tag angenommen. Das folgende Format ist für Datum und Uhrzeit akzeptabel: <i>"JJJ/MMM/TTHH:NN"</i> .
<b>-k</b>	Verhindert, dass <i>.sql</i> -Teildateien gelöscht werden, wenn ein Fehler erkannt wird. Wenn während der Ausführung von dbtran ein Fehler erkannt wird, wird die bis dahin erstellte <i>.sql</i> -Teildatei normalerweise gelöscht, um sicherzugehen, dass nicht irrtümlich eine Teildatei verwendet wird. Diese Option kann nützlich sein, wenn Sie versuchen, Transaktionen aus einem beschädigten Transaktionslog zu retten.
<b>-m</b> <i>directory</i>	Gibt das Verzeichnis an, das Transaktionslogs enthält. Verwenden Sie die Option -m, wenn Transaktionen sich möglicherweise über mehrere Transaktionslogdateien erstrecken. Diese Option erfordert die Option -n.
<b>-n</b> <i>filename</i>	Gibt die SQL-Ausgabedatei an.
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-r</b>	Entfernt alle Transaktionen, die nicht festgeschrieben sind. Dies ist die Standardeinstellung.
<b>-s</b>	Steuert, wie UPDATE-Anweisungen generiert werden. Wenn die Option nicht verwendet wird und weder ein Primärschlüssel noch ein eindeutiger Index für die Tabelle vorhanden ist, generiert das Dienstprogramm zur Logkonvertierung im Fall von Duplikatzellen UPDATE-Anweisungen mit einem nicht standardmäßigen FIRST-Schlüsselwort. Wird die Option angegeben, dann wird das FIRST-Schlüsselwort für die Kompatibilität mit dem SQL-Standard weggelassen.
<b>-sr</b>	Schreibt generierte Kommentare, die beschreiben, wie SQL Remote Vorgänge an entfernte Standorte verteilt, in die Ausgabedatei.
<b>-t</b>	Steuert, ob Trigger in die Skriptdatei einbezogen werden. Standardmäßig werden von Triggern ausgeführte Aktionen nicht in die Skriptdatei einbezogen. Wenn die Skriptdatei in einer Datenbank ausgeführt wird und der entsprechende Trigger in der Datenbank vorhanden ist, führt der Trigger die Aktionen automatisch aus. Trigger-Aktionen müssen einbezogen werden, wenn der entsprechende Trigger nicht in der Datenbank vorhanden ist, in der die Skriptdatei ausgeführt werden soll.

Option	Beschreibung
<b>-u</b> <i>userid</i> ,...	Begrenzt die Ausgabe aus dem Transaktionslog auf die angegebenen Benutzer.
<b>-x</b> <i>userid</i> ,...	Begrenzt die Ausgabe aus dem Transaktionslog, indem die angegebenen Benutzer ausgeschlossen werden.
<b>-y</b>	Ersetzt vorhandene Skriptdateien, ohne Sie zur Bestätigung aufzufordern. Wenn Sie -q angeben, müssen Sie auch die Option -y angeben, sonst schlägt der Vorgang fehl.
<b>-z</b>	Bezieht Transaktionen, die von Triggern generiert wurden, nur als Kommentare in die Ausgabedatei ein.
<i>transaction-log</i>	Gibt die zu konvertierende Logdatei an. Kann nicht zusammen mit den Optionen -c oder -m verwendet werden.
<i>SQL-file</i>	Benennt die Ausgabedatei, die die konvertierten Informationen enthält. Nur zur Verwendung mit <i>Transaktionslog</i> .

## Privilegien

Sie müssen das BACKUP DATABASE-Systemprivileg haben, um dbtran auf einem Datenbankserver ausführen zu können. Privilegien sind nicht erforderlich, um dbtran auf eine Transaktionslogdatei anzuwenden.

## Bemerkungen

Das Dienstprogramm dbtran übernimmt die Daten aus einem Transaktionslog und setzt sie als SQL-Anweisungen und Kommentare in eine Ausgabedatei. Das Dienstprogramm kann auf folgende Arten ausgeführt werden:

- **Mit einem Datenbankserver** Wenn dbtran auf einem Datenbankserver ausgeführt wird, ist das Dienstprogramm eine Standard-Clientanwendung. Es stellt über eine Verbindungszeichenfolge eine Verbindung mit dem Datenbankserver her, die nach der Option -c angegeben wird, und schreibt die Ausgabe in eine Datei, die mit der Option -n festgelegt wird.

Der folgende Befehl übersetzt die Transaktionslogdaten des Servers **demo16** und setzt die Ausgabe in eine Datei namens *demo*.

```
dbtran -c "Server=demo16;DBN=demo;UID=DBA;PWD=sql" -n demo.sql
```

- **Mit einer Transaktionslogdatei** Wenn dbtran mit einem Transaktionslog ausgeführt wird, agiert das Dienstprogramm direkt mit der Transaktionslogdatei. Schützen Sie die Transaktionslogdatei gegen allgemeinen Zugriff, damit Benutzer nicht die Möglichkeit haben, diesen Befehl auszuführen.

```
dbtran demo.log demo.sql
```

Wenn das Dienstprogramm dbtran läuft, zeigt es das früheste Log-Offset im Transaktionslog an. Mit dieser Methode kann die Reihenfolge, in der mehrere Logs erstellt wurden, wirksam ermittelt werden.

Wenn die Option `-c` verwendet wird, versucht dbtran, die Online-Transaktionslogdatei und alle Offline-Transaktionslogdateien in demselben Verzeichnis wie die Online-Transaktionslogdatei zu konvertieren. Wenn das Verzeichnis Transaktionslogdateien für mehr als eine Datenbank enthält, gibt dbtran eventuell eine Fehlermeldung aus. Dieses Problem lässt sich vermeiden, indem darauf geachtet wird, dass jedes dieser Verzeichnisse jeweils nur Transaktionslogdateien einer Datenbank enthält.

Eine Transaktion kann mehrere Transaktionslogs umfassen. Wenn Transaktionslogdateien Transaktionen enthalten, die sich über mehrere Logdateien erstrecken, können diese aufgeteilten Transaktionen verloren gehen, wenn nur eine Transaktionslogdatei konvertiert wird (zum Beispiel `dbtran demo.log`). Verwenden Sie die Option `-m`, um vollständige Transaktionen zu generieren, wenn Transaktionen sich möglicherweise über mehrere Logdateien erstrecken. Durch die Option `-m` wird dbtran angewiesen, eine einzelne SQL-Datei zu generieren (benannt durch `-n`), die alle Transaktionen aus den Logs im angegebenen Verzeichnis enthält. Siehe „[Datenbankwiederherstellung mit mehreren Transaktionslogs](#)“ auf Seite 1053.

Sie können das Dienstprogramm zur Logkonvertierung folgendermaßen starten:

- In Sybase Central verwenden Sie den **Assistenten zum Übersetzen einer Logdatei**.
- An einer Eingabeaufforderung benutzen Sie den Befehl "dbtran". Das ist zum Integrieren in SQL-Skript- oder Befehlsdateien nützlich.

Beendigungscodes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag). Siehe „[Exit-Codes der Softwarekomponenten](#)“ [*SQL Anywhere Server - Programmierung*].

## Dienstprogramm für Performancestatistik (dbstats) (Unix)

Gibt statistischen Daten zur Performance für SQL Anywhere-Datenbankserver unter Unix zurück.

### Syntax

**dbstats** [ *options* ] [ *interval* ] [ *iterations* ]

Option	Beschreibung
<code>@data</code>	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
<code>-d statistic-definition-string</code>	<p>Gibt den Statistikenamen und den Bereich (Datenbankserver, Datenbank oder Verbindung) an, in dem die Statistik überwacht wird.</p> <p>Eine vollständige Liste der Statistiken, die überwacht werden können, finden Sie unter „<a href="#">Systemmonitor-Statistiken</a>“ [<i>SQL Anywhere Server - SQL-Benutzerhandbuch</i>].</p>

Option	Beschreibung
<b>-e</b> <i>server-definition-string</i>	Legt eine kommagetrennte Liste von Datenbankservernamen für die Überwachung fest. Wenn diese Option nicht angegeben wird, protokolliert das Dienstprogramm dbstats nur statistische Daten für den Standard-Datenbankserver.
<b>-l</b>	Zeigt eine Liste der Statistiken, die für die Überwachung zur Verfügung stehen.
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-v</b> <i>verbosity</i>	Protokolliert Nachrichten auf der angegebenen Stufe. Die unterstützten Werte sind <b>error</b> , <b>warning</b> und <b>info</b> . Der Standardwert ist "info".
<i>interval</i>	Legt fest, wie häufig, in Sekunden, die statistischen Daten protokolliert werden. Wenn Sie nur ein <i>Intervall</i> angeben, gibt das Dienstprogramm den Wert der Statistiken im angegebenen Intervall zurück, bis Sie die Berichterstellung zu Statistiken stoppen.
<i>iterations</i>	Gibt an, wie viel Mal Statistiken gemeldet werden. Sie müssen ein <i>Intervall</i> angeben, wenn Sie einen Wert für <i>Wiederholungen</i> festlegen.

## Privilegien

Keine.

## Bemerkungen

Das Dienstprogramm dbstats verwendet eine Verbindung mit einem gemeinsam genutzten Speicher für die Überwachung der SQL Anywhere-Server, die auf demselben Computer ausgeführt werden. Dieses Dienstprogramm kann nicht für die Überwachung von entfernten Datenbankservern verwendet werden.

Eine *statistic-definition-string* hat das folgende Format:

```
[ [ statistic-name ] [, [ statistic-name ], ... ] ] [ : [ database-servers ] / [ databases ] / [ connections ] ]
```

Die Werte *database-server*, *databases* und *connections* sind kommagetrennte Listen von zu überwachenden Datenbankservernamen, Datenbanknamen und Verbindungsnamen. Zusätzlich zur Festlegung einer kommagetrennten Liste von Namen können Sie ein Sternchen (\*) angeben, wodurch angegeben wird, dass alle Datenbankserver, Datenbanken und Verbindungen überwacht werden sollen. Wenn Sie keinen Wert für eine der unterstützten Bereiche angeben, wird dieser Bereich nicht überwacht.

Wenn keine Optionen für das Dienstprogramm dbstats zugewiesen werden, überwacht das Dienstprogramm automatisch die statistischen Daten ActiveReq, ConnCount, CurrentCacheSize, DiskRead, DiskWrite, MainHeapPages und UnschReq für alle Bereiche, in denen sie auftreten.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

## Siehe auch

- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]
- „Systemmonitor-Statistiken“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Verbindungs-, Datenbank- und Datenbankserveigenschaften“ auf Seite 710

## Beispiel

Nur die ActiveReq-Statistik für alle Datenbanken und Verbindungen auf dem Standard-Datenbankserver abfragen und anschließend beenden:

```
dbstats -c ActiveReq
```

Nur die ActiveReq-Statistik für alle Datenbanken und Verbindungen auf dem Standard-Datenbankserver abfragen, einmal pro Sekunde und unbegrenzt lange:

```
dbstats -c ActiveReq 1
```

Nur die ActiveReq-Statistik für alle Datenbanken und Verbindungen auf dem Standard-Datenbankserver fünf Mal abfragen, einmal pro Sekunde, und dann beenden:

```
dbstats -c ActiveReq 1 5
```

Nur die ActiveReq- und ConnCount-Statistiken für alle Datenbanken und Verbindungen abfragen und anschließend beenden:

```
dbstats -c "[ ActiveReq, ConnCount ]"
```

Nur die ActiveReq- und ConnCount-Statistiken im Datenbankserver-Bereich abfragen und anschließend beenden:

```
dbstats -c "[ActiveReq, ConnCount]:*"
```

Nur die ActiveReq- und ConnCount-Statistiken im Datenbank-Bereich für die Datenbanken "db1" und "db2", die auf dem Standardserver ausgeführt werden, abfragen und anschließend beenden:

```
dbstats -c "[ActiveReq, ConnCount]:/db1,db2/"
```

## Ping-Dienstprogramm (dbping)

Testet Verbindungen zu Datenbankservern und optional zu Datenbanken.

### Syntax

**dbping** [ *options* ]

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>

Option	Beschreibung
<b>-c</b> <i>"key-word=value; ..."</i>	Gibt die Verbindungsparameter an, die für die Verbindung mit dem Server und optional der Datenbank verwendet werden. Standardmäßig stellt dbping eine Verbindung zu einem laufenden Server her. Geben Sie die Option -d an, um eine Verbindung mit der Datenbank herzustellen. Siehe „ <a href="#">Fehlerbehandlung: Verbindungszeichenfolgen testen (dbping)</a> “ auf Seite 95.
<b>-d</b>	<p>Testet die Verbindung mit der Datenbank. Falls erforderlich, kann dbping automatisch den Server und die Datenbank starten. Bei -d verhält sich dbping wie eine reguläre Clientanwendung, die eine Verbindung herstellt.</p> <p>Wenn Sie die Option -d angeben, meldet dbping nur dann einen Erfolg, wenn das Dienstprogramm eine Verbindung mit dem Server und auch mit einer Datenbank aufnehmen kann. Wenn Sie die Option -d nicht angeben, meldet dbping einen Erfolg, wenn der Server gefunden wird.</p> <p>Wenn zum Beispiel die Beispieldatenbank auf einem Datenbankserver namens blair läuft, ist der folgende Befehl erfolgreich, da dbping eine Verbindung mit dem Server blair aufnehmen kann:</p> <pre>dbping -c "Server=blair;DBN=other"</pre> <p>Der folgende Befehl scheitert mit der Meldung Datenbank-Ping fehlgeschlagen - Angegebene Datenbank nicht gefunden, da die Datenbank "other" nicht läuft:</p> <pre>dbping -c "Server=blair;DBN=other" -d</pre>
<b>-en</b>	Gibt an, dass dbping mit einem Fehlschlag-Rückgabecode beenden soll, wenn NULL für eine der angegebenen Eigenschaften zurückgegeben wird. Standardmäßig gibt dbping NULL aus, wenn der Wert einer durch die Optionen -pc, -pd oder -ps angegebenen Eigenschaften unbekannt ist, und beendet mit einem Erfolgs-Rückgabecode. Diese Option kann nur zusammen mit den Optionen -pc, -pd und -ps verwendet werden.
<b>-l</b> <i>library</i>	<p>Gibt die zu verwendende ODBC-Bibliothek (ohne Dateierweiterung) an. Diese Option vermeidet die Verwendung des ODBC-Treibermanagers und ist daher unter Unix-Betriebssystemen nützlich.</p> <p>Beispiel: Der folgende Befehl lädt den ODBC-Treiber direkt:</p> <pre>dbping -m -c "DSN=SQL Anywhere 16 Demo" -l dbodbc16</pre> <p>Wenn Sie unter Unix eine Verbindungsbibliothek mit Threading verwenden möchten, müssen Sie die entsprechende Version des Ping-Dienstprogramms, dbping_r, verwenden.</p>
<b>-m</b>	Stellt eine Verbindung mithilfe von ODBC her. Standardmäßig stellt das Dienstprogramm die Verbindung unter Verwendung der Embedded SQL-Schnittstelle her.

Option	Beschreibung
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-pc</b> <i>property,...</i>	<p>Zeigt die angegebenen Verbindungseigenschaften. Geben Sie die Eigenschaften in einer von Kommas unterteilten Liste ein. Sie müssen ausreichende Verbindungsinformationen angeben, um eine Datenbankverbindung herzustellen, wenn Sie diese Option verwenden. Siehe „<a href="#">Liste der Verbindungseigenschaften</a>“ auf Seite 711.</p> <p>Beispiel: Der folgende Befehl zeigt die fire_triggers-Optionseinstellung, die als Verbindungseigenschaft verfügbar ist.</p> <pre>dbping -c ... -pc fire_triggers</pre>
<b>-pd</b> <i>property[@db-name],...</i>	<p>Zeigt die angegebenen Datenbankeigenschaften. Geben Sie die Eigenschaften in einer von Kommas unterteilten Liste ein. Siehe „<a href="#">Liste der Datenbankeigenschaften</a>“ auf Seite 767.</p> <p>Beispiel: Der folgende Befehl zeigt die Seitengröße an, die in der Datenbank verwendet wird.</p> <pre>dbping -c ... -pd PageSize</pre> <p>Optional können Sie den Namen einer Datenbank angeben, die auf dem Datenbankserver läuft, von dem Sie den Wert beziehen wollen. Wenn der Datenbankname nicht durch Anhängen von <i>@db-name</i> an die Eigenschaft angegeben wurde, wird bei jeder aufgelisteten Eigenschaft der für die vorherige Eigenschaft verwendete Datenbankname verwendet.</p> <p>Mit dem folgenden Befehl werden Seitengröße und Kollation der Datenbank mydb angezeigt:</p> <pre>dbping -c ... -pd PageSize@mydb,Collation</pre>
<b>-ps</b> <i>property,...</i>	<p>Zeigt die angegebenen Datenbankservereigenschaften. Geben Sie die Eigenschaften in einer von Kommas unterteilten Liste ein. Sie müssen ausreichende Verbindungsinformationen angeben, um eine Datenbankverbindung herzustellen, wenn Sie diese Option verwenden. Siehe „<a href="#">Liste der Datenbankservereigenschaften</a>“ auf Seite 745.</p> <p>Beispiel: Der folgende Befehl zeigt die Anzahl der lizenzierten Arbeitsplätze oder Prozessoren für den Datenbankserver an:</p> <pre>dbping -c ... -ps LicenseCount</pre>
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.

Option	Beschreibung
<b>-s</b>	Gibt Informationen über die Performance des Netzwerks zwischen dem Computer, auf dem dbping ausgeführt wird, und dem Computer, der den Datenbankserver ausführt, zurück. Angenäherte Verbindungsgeschwindigkeit, Wartezeit und Durchsatz werden angezeigt. Die Option -c wird üblicherweise benötigt, um die Verbindungsparameter zum Verbinden mit einer Datenbank auf dem Server anzugeben. Sie können "dbping -s" nur bei Embedded SQL-Verbindungen verwenden. Diese Option wird ignoriert, wenn ebenfalls die Option -m oder -l angegeben ist. Standardmäßig führt "dbping -s" Schleifen durch die Anforderung für zumindest eine Sekunde bei jeder gemessenen Statistik durch. Es werden höchstens 200 Verbindungsherstellungen und -abbrüche durchgeführt, unabhängig von ihrer Dauer, um den Verbrauch zu großer Ressourcen zu verhindern. Auf langsameren Netzwerken kann es mehrere Sekunden dauern, um die Mindestanzahl an Wiederholungen bei jeder Statistik durchzuführen. Die Performancestatistiken sind angenäherte Statistiken. Sie sind genauer, wenn sowohl der Client- und der Servercomputer verhältnismäßig untätig sind. Siehe „ <a href="#">Fehlerbehandlung: Leistungsfähigkeit von Embedded SQL- und Netzwerkverbindung testen (dbping)</a> “ auf Seite 96.
<b>-st time</b>	Diese Option gibt dieselben Informationen wie die Option -s zurück, nur dass die Option -st die Zeitspanne (in Sekunden) angibt, in der dbping die Anforderungen für die einzelnen Statistiken in Schleifen durchläuft. Diese Option ermöglicht es, genauere Zeitfolgeinformationen abzurufen als mit der Option -s. Siehe „ <a href="#">Fehlerbehandlung: Leistungsfähigkeit von Embedded SQL- und Netzwerkverbindung testen (dbping)</a> “ auf Seite 96.
<b>-z</b>	Zeigt die Netzwerkkommunikationsprotokolle, die verwendet werden, um eine Verbindung zu versuchen, sowie andere Diagnosemeldungen an. Diese Option steht nur zur Verfügung, wenn eine Embedded SQL-Verbindung hergestellt wird. Das heißt, sie kann nicht mit -m oder -l kombiniert werden.

## Privilegien

Keine.

## Bemerkungen

Das Dienstprogramm dbping ist ein Tool, das zur Fehlersuche bei Verbindungsproblemen bereitgestellt wird. Es übernimmt eine vollständige oder teilweise Verbindungszeichenfolge und gibt eine Meldung zurück, in der angegeben wird, ob der Versuch zur Ermittlung des Serverstandorts oder der Verbindung zur Datenbank erfolgreich war.

Das Dienstprogramm kann bei Embedded SQL- oder ODBC-Verbindungen verwendet werden. Es kann nicht bei jConnect (TDS)-Verbindungen benutzt werden.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlslag).

**Siehe auch**

- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]
- „Fehlerbehandlung: Leistungsfähigkeit von Embedded SQL- und Netzwerkverbindung testen (dbping)“ auf Seite 96
- „Fehlerbehandlung: Verbindungszeichenfolgen testen (dbping)“ auf Seite 95

## Skriptausführungs-Dienstprogramm (dbrunsql)

Ermöglicht es Ihnen, SQL-Anweisungen und Skriptdateien in Datenbanken auszuführen, die unter Windows Mobile laufen.

**Syntax**

**dbrunsql** [ *options* ] [ *SQL-script-file* | *SQL-statement* ]

Option	Beschreibung
<b>-c</b> " <i>keyword=value; ...</i> "	Legt Verbindungsparameter fest. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
<b>-d</b>	Schreibt aus Ergebnismengen exportierte Daten in die Ausgabedatei. Wenn Sie -d nicht angeben, wird die gesamte Ausgabe in die Ausgabedatei geschrieben.
<b>-e</b> [ <b>c</b>   <b>p</b>   <b>s</b> ]	Steuert das Verhalten, wenn bei Ausführen von Anweisungen ein Fehler auftritt. Standardmäßig fordert dbrunsql den Benutzer zur Eingabe auf, wenn ein Fehler auftritt. <ul style="list-style-type: none"> <li>• <b>c</b> Fehler ignorieren und mit der Ausführung von Anweisungen fortfahren</li> <li>• <b>p</b> Den Benutzer zu einer Entscheidung auffordern, ob er fortfahren möchte</li> <li>• <b>s</b> Die Ausführung von Anweisungen stoppen</li> </ul>
<b>-f</b> [ <b>f</b>   <b>a</b> ]	Gibt das Datenformat an, das dbrunsql benutzt, um Ergebnismengen zu exportieren. Sie können einen der folgenden Werte festlegen: <ul style="list-style-type: none"> <li>• <b>a</b> TEXT-Format beim Datenexport verwenden</li> <li>• <b>f</b> FIXED-Format beim Datenexport verwenden. Dies ist das Standardformat.</li> </ul>
<b>-g</b> [ +   - ]	Verhindert das Erscheinen der grafischen Benutzeroberfläche. Standardmäßig wird die dbrunsql-GUI verwendet.

Option	Beschreibung
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Unterdrückt die Ausgabe von Meldungen. Dies ist nur dann nützlich, wenn Sie Interactive SQL mit einer Anweisung oder einer Skriptdatei starten. Das Angeben dieser Option unterdrückt keine Fehlermeldungen, sondern Folgendes: <ul style="list-style-type: none"><li>• Warnungen und andere nicht-schwerwiegende Meldungen</li><li>• Die Ausgabe von Ergebnismengen</li></ul>
<b>-qc</b>	Schließt das dbrunsql-Fenster, wenn die Anweisung bzw. Skriptdatei ausgeführt wurde.
<b>-s</b> <i>number</i>	Gibt die maximale Anzahl der Bytes an, die pro Spalte abgerufen werden, wenn Ergebnismengen mit dem FIXED-Format exportiert werden. Der Standardwert ist 255.
<b>-v</b>	Bezieht alle Zeilen aller SQL-Anweisungen in die dbrunsql-Ausgabe ein. Andernfalls wird bei der Ausführung einer Skriptdatei die Nummer der Zeile ausgegeben, die derzeit ausgeführt wird.

**Privilegien**

Keine.

**Bemerkungen**

Mit dem Dienstprogramm dbrunsql können Sie in einer Datenbank SQL-Anweisungen oder Skriptdateien ausführen. Das SQL Anywhere-Dienstprogramm für die Skriptausführung (dbrunsql) wird nur unter Windows Mobile unterstützt.

## Dienstprogramm für die Serverauflistung (dblocate)

Ermittelt die Position von Datenbankservern im TCP/IP-Netzwerk

**Syntax**

**dblocate** [ *options* ] [ *host* ]

Option	Beschreibung
<i>@data</i>	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
<b>-d</b>	<p>Listet den Servernamen und die Adresse für jeden gefundenen Server auf, gefolgt von einer kommagetrennten Liste der Datenbanken, die auf diesem Server laufen. Wenn die Liste 160 Zeichen überschreitet, wird sie gekürzt und endet mit drei Punkten (...).</p> <p>Datenbanken, die auf SQL Anywhere 9.0.2 und früher laufen oder mit der Datenbankoption -dh gestartet wurden, werden nicht aufgelistet. Siehe „<a href="#">Datenbankoption -dh</a>“ auf Seite 326.</p>
<b>-dn</b> <i>database-name</i>	<p>Listet den Servernamen und die Adresse von Servern auf, die eine Datenbank mit dem angegebenen Namen ausführen. Wenn die Liste 160 Zeichen überschreitet, wird sie gekürzt und endet mit drei Punkten (...).</p> <p>Datenbanken, die auf SQL Anywhere 9.0.2 und früher laufen oder mit der Datenbankoption -dh gestartet wurden, werden nicht aufgelistet. Siehe „<a href="#">Datenbankoption -dh</a>“ auf Seite 326.</p>
<b>-dv</b>	<p>Zeigt den Servernamen und die Adresse für jeden gefundenen Server mit einer Liste aller auf diesem Server laufenden Datenbanken in einer eigenen Zeile. Die Liste wird nicht gekürzt, daher kann diese Option verwendet werden, um Listen anzuzeigen, die unter Verwendung der Option -d gekürzt werden.</p> <p>Datenbanken, die auf SQL Anywhere 9.0.2 und früher laufen oder mit der Datenbankoption -dh gestartet wurden, werden nicht aufgelistet. Siehe „<a href="#">Datenbankoption -dh</a>“ auf Seite 326.</p>

Option	Beschreibung
<b>-n</b>	Listet in der Ausgabe keine Computernamen, sondern IP-Adressen. Damit kann die Performance erhöht werden, weil die Suche nach Computernamen zeitaufwändig sein kann.
<b>-o filename</b>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-p port-number</b>	Zeigt den Servernamen und die Adresse nur bei Servern an, die die angegebene TCP/IP-Portnummer verwenden. Die TCP/IP-Portnummer muss zwischen 1 und 65535 liegen.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-s name</b>	Zeigt den Servernamen und die Adresse nur bei Servern mit dem angegebenen Servernamen an. Wenn diese Option verwendet wird, sollte die Option -ss nicht verwendet werden (wenn beide Optionen verwendet werden, ist es wahrscheinlich, dass keine entsprechenden Server gefunden werden).
<b>-ss substr</b>	Zeigt den Servernamen und die Adresse nur bei Servern an, die die angegebene Teilzeichenfolge im Servernamen enthalten. Wenn diese Option verwendet wird, sollte die Option -s nicht verwendet werden (wenn beide Optionen verwendet werden, ist es wahrscheinlich, dass keine entsprechenden Server gefunden werden).
<b>-v</b>	<p>Zeigt den vollständigen Servernamen an. Standardmäßig kürzt dblocate Datenbankservernamen, die länger als 40 Byte sind.</p> <p>Clients der Version 9.0.2 und früher, einschließlich dblocate, können sich nicht mit Datenbankservern der Version 10.0.0 und höher verbinden, wenn deren Namen länger als 40 Byte sind.</p>

Option	Beschreibung
<i>host</i>	<p>Führt nur solche Datenbankserver auf, die auf dem Computer mit der angegebenen IP-Adresse bzw. mit dem angegebenen Hostnamen ausgeführt werden. Mit dem folgenden Befehl können Sie beispielsweise nach Servern auf dem Computer jfrancis suchen:</p> <pre>dblocate jfrancis</pre> <p>Der Hostname und die IP-Adresse können ein beliebiges Format haben, unabhängig davon, ob die Option -n angegeben ist. Wenn ein Server z.B. auf myhost.mycompany.com ausgeführt wird, der die IP-Adresse 1.2.3.4 hat, und Sie auf einem beliebigen Computer mit der Domäne mycompany.com nur Server auflisten wollen, die auf diesem Computer ausgeführt werden, können Sie <code>dblocate myhost</code>, <code>dblocate myhost.mycompany.com</code> oder <code>dblocate 1.2.3.4</code> verwenden.</p>

**Privilegien**

Keine.

**Bemerkungen**

Das Dienstprogramm für die Serverauflistung (dblocate) ermittelt jeden SQL Anywhere-Datenbankserver, der über TCP/IP auf dem nächstgelegenen Netzwerk läuft, und gibt eine Liste von Datenbankservern und ihre Adresse aus. Diese Liste umfasst alternative Servernamen. Siehe „[Datenbankoption -sn](#)“ auf Seite 332.

Anhängig von Ihrem Netzwerk kann es mehrere Sekunden dauern, bis dblocate Ergebnisse anzeigt.

**Hinweis**

Wenn ein Datenbankserver einen anderen TCP/IP-Port als 2638 unter Mac OS X verwendet, findet ihn dblocate nicht, selbst wenn die Option -p verwendet wird, um den TCP/IP-Port anzugeben. Siehe „[ServerPort-Protokolloption \(PORT\)](#)“ auf Seite 416.

Datenbankserver in unterschiedlichen Subnetzen können nur gefunden werden, wenn dbns16 bereits verwendet wird. Siehe „[Fehlerbehandlung: Datenbankserver mithilfe des Broadcast Repeater-Dienstprogramms suchen](#)“ auf Seite 85.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

Der Datenbankserver kann sich selbst bei einem LDAP-Server anmelden, der alle Server im Unternehmen registriert. Damit können Clients und dblocate alle Server finden, gleichgültig ob sie sich auf einem WAN oder LAN befinden, über Firewalls hinweg und ohne Angabe von IP-Adressen. LDAP wird nur mit TCP/IP und nur auf Netzwerkservers verwendet.

Wenn ein Datenbankservername mehr als einmal gefunden wird, zeigt dblocate die IP-Adressen der einzelnen Hosts an, auch wenn die Option -n nicht angegeben wurde. Ein Servername kann mehrfach auftreten, wenn ein Server auf einem Computer mit mehreren IP-Adressen ausgeführt wird (zum Beispiel, wenn der Computer mit mehreren Netzwerkkarten ausgestattet ist) oder wenn ein Netzwerkserver auf einem entfernten Computer und ein Personal Server mit demselben Namen auf dem lokalen Computer ausgeführt wird.

Datenbankserver, die mit -sb 0 gestartet wurden, werden von dblocate nicht gefunden.

**Siehe auch**

- „Verbindungen mit LDAP als Namensserver“ auf Seite 109
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]
- „Fehlerbehandlung: Datenbankserver suchen“ auf Seite 83
- „db\_string\_ping\_server-Funktion“ [*SQL Anywhere Server - Programmierung*]

# Dienstprogramm für die Serverlizenzierung (dblic)

Wendet Ihre Software-Lizenz auf Ihren SQL Anywhere-Datenbank- oder MobiLink-Server an

**Syntax**

**dblic** [ *options* ] *license-file* [ "*user-name*" "*company-name*" ]

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>

Option	Beschreibung
<b>-l type</b>	<p>Gibt den Lizenztyp an, der dem Lizenzmodell entspricht, das in Ihrer Software-Lizenzvereinbarung beschrieben wird. Die folgenden Lizenztypen werden unterstützt:</p> <ul style="list-style-type: none"> <li> <b>Perseat</b> Eine Perseat-Lizenz begrenzt die Anzahl der Clientverbindungen zum Datenbankserver. Bei Perseat-Lizenzierung kann der Netzwerk-Datenbankserver alle auf dem Computer verfügbaren CPUs nutzen, aber nicht mehr als die bei Ihrer SQL Anywhere-Edition maximal zulässige Anzahl. Wenn eine CPU mehrere Prozessorkerne oder Threads enthält, können alle Prozessorkerne und Threads der CPU genutzt werden. <p>Der Personal Server ist auf vier Prozessorkerne in einer CPU beschränkt. Wenn ein Prozessorkern mehrere Threads enthält, können alle Threads dieses Prozessorkerns verwendet werden.</p> </li> <li> <b>Prozessor</b> Eine Prozessor-Lizenz beschränkt die Anzahl der separaten physischen Prozessoren, die vom Datenbankserver verwendet werden können. Bei CPU-basierter Lizenzierung nutzt der Netzwerk-Datenbankserver höchstens die in Ihrer Lizenz angegebene Anzahl von CPUs, aber nicht mehr als die bei Ihrer SQL Anywhere-Edition maximal zulässige Anzahl. Wenn eine CPU mehrere Prozessorkerne oder Threads enthält, können alle Prozessorkerne und Threads der CPU genutzt werden. <p>Bei diesem Lizenztyp behandelt der Datenbankserver jeden physischen Prozessor als eine CPU und einen Dual-Core- oder Hyperthread-Prozessor nicht als mehrere Prozessoren. Wenn Sie eine Prozessor-Lizenz haben, gibt es keine Einschränkungen auf die Anzahl der Clientverbindungen zum Datenbankserver.</p> <p>Der Personal Server ist auf vier Prozessorkerne in einer CPU beschränkt. Wenn ein Prozessorkern mehrere Threads enthält, können alle Threads dieses Prozessorkerns verwendet werden.</p> <p>Sie können den Datenbankserver mit folgenden Mitteln weiter einschränken:</p> <ul style="list-style-type: none"> <li>-gt-Datenbankserveroption</li> <li>-gta-Datenbankserveroption</li> <li>-gtc-Datenbankserveroption</li> <li>sa_server_option-Systemprozedur mit der ProcessorAffinity-Option</li> </ul> <p>Diese Option kann nicht mit der Option -k verwendet werden.</p> </li> </ul>

Option	Beschreibung
<b>-k</b> <i>registration-key</i>	Gibt einen SQL Anywhere-Lizenzschlüssel an. Mit dieser Option können Sie die Edition Ihres Datenbankservers ändern. Wenn Sie beispielsweise die Developer Edition haben und auf die Workgroup Edition umstellen möchten, können Sie den Registrierungsschlüssel der Workgroup Edition angeben.  Diese Option kann nicht mit der Option -l verwendet werden.
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-u</b> <i>license-number</i>	Gibt die Gesamtzahl der Benutzer oder Prozessoren für die Lizenz an. Wenn Sie weitere Lizenzen hinzufügen, ist dies die Gesamtzahl und <i>nicht</i> die Anzahl der zusätzlichen Lizenzen.
<i>license-file</i>	Gibt den Pfad- und Dateinamen des auszuführenden Servers oder der Lizenzdatei für den Personal Datenbankserver, das Netzwerk-Datenbankserver-Programm oder den MobiLink-Server an, die Sie lizenzieren.  Sie können die aktuellen Lizenzinformationen eines Servers auch anzeigen, indem Sie nur den Lizenzdateinamen eingeben.
<i>user-name</i>	Gibt den Benutzernamen für die Lizenz an. Dieser Name wird im Meldungsfenster des Datenbankservers beim Starten angezeigt. Wenn im Namen Leerzeichen enthalten sind, stellen Sie ihn zwischen Anführungszeichen.
<i>company-name</i>	Gibt das Unternehmen für die Lizenz an. Dieser Name wird im Meldungsfenster des Datenbankservers beim Starten angezeigt. Wenn im Namen Leerzeichen enthalten sind, stellen Sie ihn zwischen Anführungszeichen.

**Privilegien**

Keine.

**Bemerkungen**

Das Dienstprogramm für die Serverlizenzierung fügt Ihrem SQL Anywhere-Datenbank- oder MobiLink-Server lizenzierte Benutzer oder lizenzierte Prozessoren hinzu. Sie dürfen dieses Dienstprogramm nur in Übereinstimmung mit Ihrer Lizenzvereinbarung verwenden, um der Anzahl der Benutzer oder Prozessoren, die Ihnen zusteht, Lizenzen zu erteilen. Das Ausführen dieses Befehls erteilt Ihnen keine Lizenz. Wie viele CPUs der Datenbankserver nutzen kann, wird möglicherweise auch beeinflusst durch Ihre SQL Anywhere-Edition, die Datenbankserveroption -gt, -gtc oder -gta sowie die sa\_server\_option-Systemprozedur mit der ProcessorAffinity-Option.

Dieses Dienstprogramm ändert auch die Benutzer- und Firmennamen, die beim Start von Personal Datenbankservern, Netzwerk-Datenbankservern und dem MobiLink-Server angezeigt werden.

Sie können dieses Dienstprogramm auch verwenden, um die aktuelle Lizenzinformationen für einen Personal oder Netzwerk-Datenbankserver anzuzeigen, indem Sie nur den Lizenzdateinamen angeben.

Die Lizenzinformationen werden jetzt in einer *.lic*-Datei gespeichert, die sich in demselben Verzeichnis wie die Serverprogrammdatei befindet. Der Server sucht nach einer *.lic*-Datei, die denselben Basisdateinamen hat wie die Programmdatei, die ausgeführt wird. Wenn z.B. der Name des ausführbaren Datenbankservers *myserver.exe* ist, dann sucht der Server nach einer Lizenzdatei namens *myserver.lic*. Standardmäßig werden folgende Namen verwendet:

Programmdatei	Lizenzdateiname
Personal Datenbankserver (dbeng16)	<i>dbeng16.lic</i>
Netzwerk-Datenbankserver (dbsrv16)	<i>dbsrv16.lic</i>
MobiLink-Server (mlsrv16)	<i>mlsrv16.lic</i>

Wenn Sie versuchen, einen Server zu starten, und die entsprechende *.lic*-Datei nicht verfügbar ist, wird der Server nicht gestartet. Die Lizenzdatei wird vom SQL Anywhere-Installationsprogramm erstellt. Das Dienstprogramm *dblic* ändert nur vorhandene Lizenzen, kann aber keine neuen Lizenzdateien erstellen.

Beendigungscodes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

Unter Unix ist das Datenbankserver-Programm standardmäßig schreibgeschützt, daher schlägt eine Verwendung des Serverlizenzierungs-Dienstprogramms (*dblic*) fehl. Achten Sie darauf, dass das Programm nicht schreibgeschützt ist (z.B. mit `chmod +w`), bevor Sie das Serverlizenzierungs-Dienstprogramm verwenden.

Im Cache abgelegte Verbindungen werden bei der Arbeitsplatzlizenzierung gezählt.

Weitere Hinweise zur SQL Anywhere-Lizenzierung finden Sie unter <http://www.sybase.com/detail?id=1056242>.

### Siehe auch

- „Editionen und Lizenzierung“ [*SQL Anywhere 16 - Einführung*]
- „Datenbankserveroption -gt“ auf Seite 251
- „Datenbankserveroption -gtc“ auf Seite 253
- „Datenbankserveroption -gta“ auf Seite 252
- ProcessorAffinity-Option: „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]

### Beispiel

Der folgende Befehl, der im gleichen Verzeichnis ausgeführt wird wie das Datenbankserver-Programm, wendet eine Lizenz für 50 gleichzeitige Benutzer im Namen von "Sys Admin" für das Unternehmen "My Co" auf einem Microsoft Windows-Netzwerk-Datenbankserver an. Der Befehl muss in einer Zeile eingegeben werden:

```
dblic -l perseat -u 50 "c:\Program Files\SQL Anywhere 12\Bin32\dsrv16.lic"  
"Sys Admin" "My Co"
```

Die folgenden Meldungen werden bei einer erfolgreichen Lizenzierung am Bildschirm angezeigt:

```
SQL Anywhere-Dienstprogramm Serverlizenzierung, Version 16.0.0.1403  
Lizenz erfolgreich angewendet.  
Advanced Edition  
Add-On: Hochverfügbarkeit  
Add-On: In-Memory-Modus  
Add-On: Scale-Out-Knoten  
Lizenzierte Knoten: 50  
Benutzer: Sys Admin  
Firma: My Co  
Installationsschlüssel:
```

Der folgende Befehl gibt Informationen über die Lizenz für einen Datenbankserver zurück:

```
dblic "C:\Program Files\SQL Anywhere 16\Bin32\dsrv16.lic"
```

## Dienstprogramm für Dienste (dbsvc) für Linux

Erstellt, ändert und löscht SQL Anywhere-Dienste

### Syntax

```
dbsvc [ modifier-options ] -d svc  
dbsvc [ modifier-options ] -g svc  
dbsvc [ modifier-options ] -l  
dbsvc [ modifier-options ] -status svc  
dbsvc [ modifier-options ] -u svc  
dbsvc [ modifier-options ] creation-options -w svc [ options ]  
dbsvc [ modifier-options ] -x svc
```

Hauptoption	Beschreibung
-d <i>service-name</i>	Entfernt den betreffenden Dienst aus der Liste der Dienste. Wenn Sie -y angeben, wird der Dienst ohne Bestätigung gelöscht.
-g <i>service-name</i>	Gibt die Definition des Diensts an
-l	Listet die verfügbaren SQL Anywhere-Dienste auf
-u <i>service-name</i>	Startet einen Dienst namens <i>service-name</i> .

Hauptoption	Beschreibung
<b>-w</b> <i>executable parameters</i>	<p>Erstellt einen neuen Dienst oder überschreibt einen eventuell bereits vorhandenen Dienst desselben Namens. Wenn Sie -y angeben, wird der bestehende Dienst ohne Bestätigung überschrieben. Sie können einen Dienst nicht löschen, während er ausgeführt wird.</p> <p>Sie müssen geeignete Parameter für den zu erstellenden Dienst angeben.</p> <p>Siehe:</p> <ul style="list-style-type: none"> <li>• <b>dbsrv16 und dbeng16</b> „Syntax des SQL Anywhere-Datenbankservers“</li> <li>• <b>mlsrv16</b> „MobiLink-Serveroptionen“ [<i>MobiLink - Serveradministration</i>]</li> <li>• <b>dbmlsync</b> „dbmlsync-Syntax“ [<i>MobiLink - Clientadministration</i>]</li> <li>• <b>dbremote</b> „SQL Remote-Nachrichtenagent-Dienstprogramm (dbremote)“ [<i>SQL Remote</i>]</li> <li>• <b>dbns16</b> „Broadcast Repeater-Dienstprogramm (dbns16)“</li> <li>• <b>rshost</b> „Relay Server-Status-Manager“ [<i>Relay Server</i>]</li> <li>• <b>rsoe</b> „Outbound Enabler“ [<i>Relay Server</i>]</li> </ul>
<b>-x</b> <i>service-name</i>	Stoppt einen Dienst namens <i>service-name</i> .

Erstellungsoption	Beschreibung
<b>-a</b> <i>acct</i>	Benennt das Konto. Alle Dienste werden über ein Linux-Konto ausgeführt. Wenn Sie ein von Ihnen erstelltes Konto verwenden, müssen Sie das Konto mit der Option -a benennen.
<b>-as</b>	Führt den Dienst unter dem Linux-Daemon-Konto aus. Alle Dienste werden über ein Linux-Konto ausgeführt. Es ist kein Kennwort erforderlich. Es muss entweder die Option -a oder die Option -as verwendet werden.
<b>-od</b>	Gibt den Standort der Systeminformationsdatei an (falls erforderlich).
<b>-pr</b>	Setzt den Nice-Level für den Linux-Prozess.

Erstellungsoption	Beschreibung
<b>-rl</b>	Gibt die Ausführungsstufe (Runlevel) an, auf der der Dienst gestartet wird.
<b>-rs</b> <i>service-name</i>	<p>Fügt den Dienst der Diensteliste im Required-Start-Header des von dbsvc generierten init-Skripts hinzu. Dieser Header unterstützt das Betriebssystem dabei, die Reihenfolge zu ermitteln, in der Dienste gestartet werden.</p> <p>Angegebene Dienstnamen werden überprüft, um festzustellen, ob sie bereits vorhanden sind. Die Namenskonvention für den Dienst lautet <b>SA_</b><i>service-name</i>.</p>
<b>-s</b> <i>startup</i>	Legt das Startverhalten der Dienste von SQL Anywhere fest. Sie können das Startverhalten auf "automatisch" oder "manuell" einstellen. Der Standardwert ist "Manuell".
<b>-status</b>	Gibt den Status zurück, in dem der Dienst läuft.

Erstellungsoption	Beschreibung
<b>-t type</b>	<p>Gibt den Typ für diesen Dienst an. Sie können unter den folgenden Typen auswählen (der alternative Name wird in Klammern aufgeführt):</p> <ul style="list-style-type: none"> <li>• <b>Network</b> Erstellt einen Dienst für den SQL Anywhere-Netzwerk-Datenbankserver (dbsrv16). Siehe „<a href="#">Syntax des SQL Anywhere-Datenbankservers</a>“ auf Seite 203.</li> <li>• <b>Personal (Standalone)</b> Dies ist der Standardwert, der einen Dienst für den Personal Datenbankserver von SQL Anywhere erstellt (dbeng16). Siehe „<a href="#">Syntax des SQL Anywhere-Datenbankservers</a>“ auf Seite 203.</li> <li>• <b>DBRemote</b> Erstellt einen Dienst für den SQL Remote-Nachrichtenagenten. Siehe „<a href="#">SQL Remote-Nachrichtenagent-Dienstprogramm (dbremote)</a>“ [<a href="#">SQL Remote</a>].</li> <li>• <b>MobiLink</b> Erstellt einen Dienst für den MobiLink-Server (mlsrv16). Siehe „<a href="#">mlsrv16-Syntax</a>“ [<a href="#">MobiLink - Serveradministration</a>].</li> <li>• <b>DBMLSync (MLSync)</b> Erstellt einen Dienst für den MobiLink-Synchronisationsclient (dbmlsync). Siehe „<a href="#">dbmlsync-Syntax</a>“ [<a href="#">MobiLink - Clientadministration</a>].</li> <li>• <b>DBNS</b> Erstellt einen Dienst für das Broadcast Repeater-Dienstprogramm (dbns16). Siehe „<a href="#">Broadcast Repeater-Dienstprogramm (dbns16)</a>“ auf Seite 891.</li> <li>• <b>RSHOST</b> Erstellt einen Dienst für den Relay Server Status-Manager. Siehe „<a href="#">Befehlszeilensyntax des Relay Server Status-Managers (rshost)</a>“ [<a href="#">Relay Server</a>].</li> <li>• <b>RSOE</b> Erstellt einen Dienst für den Outbound Enabler. Siehe <a href="#">Outbound Enabler-Syntax</a> [<a href="#">Relay Server</a>].</li> </ul>

Änderungsoption	Beschreibung
<b>-cm</b>	Zeigt den Befehl an, der zum Erstellen des Dienstes verwendet wurde. Mit dieser Option kann der Erstellungsbefehl in eine Datei ausgegeben werden, die verwendet werden kann, um den Dienst auf einem anderen Computer zu installieren oder den ursprünglichen Zustand eines Dienstes wiederherzustellen, sofern er geändert wurde. Sie müssen die Optionen -g oder -l zusammen mit der Option -cm verwenden, andernfalls schlägt der Befehl fehl. Die Angabe der Option -g zeigt den Erstellungsbefehl für den angegebenen Dienst an, während die Angabe der Option -l den Erstellungsbefehl für alle Dienste anzeigt.
<b>-q</b>	Unterdrückt Meldungen im Meldungsfenster des Datenbankservers. Wenn Sie beim Ändern oder Löschen eines existierenden Dienstes diese Option angeben, müssen Sie auch die Option -y angeben, sonst schlägt der Vorgang fehl.
<b>-y</b>	Führt den Vorgang automatisch aus, ohne eine Bestätigung zu verlangen. Diese Option kann mit der Option -w oder -d verwendet werden. Wenn Sie beim Ändern oder Löschen eines existierenden Dienstes die Option -q angeben, müssen Sie auch -y angeben, sonst schlägt der Vorgang fehl.

## Privilegien

Keine

## Bemerkungen

Ein Dienst führt einen Datenbankserver oder eine andere Anwendung aus, indem er die eingegebenen Optionen berücksichtigt. Dieses Dienstprogramm bietet eine umfassende Möglichkeit, SQL Anywhere-Dienste unter Linux zu verwalten.

Da Dienste üblicherweise in einer anderen Umgebung ausgeführt werden, wird empfohlen, dass Sie den Namen der Datenbankdatei voll qualifizieren, wenn Sie einen Dienst erstellen. Überdies wird empfohlen, dass Sie in Datenquellennamen keine Leerstellen verwenden.

Sie müssen über die Berechtigungen für das Verzeichnis */etc/init.d* verfügen, um Dienste zu erstellen, zu bearbeiten oder zu löschen.

Wenn ein SQL Anywhere-Dienst unter Linux läuft, wird im Verzeichnis */var/run* eine PID-Datei erstellt. Diese Datei enthält die PID des dbsvc-Prozesses. Die Datei erhält den Namen *SA\_service-name.pid*. Diese Datei kann von anderen Linux-Tools verwendet werden, um den Prozess zu finden und den Dienst zu überwachen.

Wie die meisten Linux-Dienste erstellt das Dienstprogramm dbsvc Dateien in */etc/init.d*. Die Namenskonvention für den Dienst lautet **SA\_service-name**. Beispiel: Wenn Sie einen Dienst namens "myserv" erstellt haben, können Sie den folgenden Befehl ausgeben, um den Dienst zu starten:

```
/etc/init.d/SA_myserv start
```

Der folgende Befehl gibt den Status des Dienstes zurück:

```
/etc/init.d/SA_myserv status
```

Der folgende Befehl gibt Nutzungsinformationen für den Dienst zurück:

```
/etc/init.d/SA_my SERV
```

**Hinweis**

Wenn der db svc-Befehl Shell-spezifische Zeichen enthält (wie etwa Semikola oder Klammern), ist es empfehlenswert, eine Konfigurationsdatei für die Parameter für Ihren Dienst zu verwenden. Siehe [„Konfigurationsdateien“ auf Seite 882](#).

**Beispiel**

Erstellen Sie den Personal Server myserv, der den angegebenen Server mit den angegebenen Parametern startet. Der Server läuft als LocalSystem-Benutzer:

```
db svc -as -w myserv -n myeng -c 8m "/tmp/demo.db"
```

Erstellen Sie einen Netzwerkserverdienst namens mynetworkserv. Der Server läuft unter dem lokalen Konto und startet automatisch, wenn der Computer wieder hochgefahren wird:

```
db svc -as -t network -w mynetworkserv -x tcpip -c 8m "/tmp/demo.db"
```

Listen Sie alle Details über den myserv-Dienst auf:

```
db svc -g myserv
```

Löschen Sie den Dienst myserv, ohne dass eine Bestätigung verlangt wird:

```
db svc -y -d myserv
```

Erstellen Sie den Dienst mysyncservice:

```
db svc -as -t dbmlsync -w mysyncservice -c "/tmp/CustDB.db" -o syncinfo.txt
```

Generieren Sie den Befehl, den Dienst "service\_1" zu erstellen und auf der Konsole auszugeben:

```
db svc -cm -g service_1
```

Die Konsole enthält das Folgende:

```
'db svc -t Standalone -as -y -w "service_1" -n'
```

Starten Sie einen Dienst mit db svc:

```
db svc -u myserv
```

Stoppen Sie einen Dienst mit db svc:

```
db svc -x myserv
```

Rufen Sie den Status eines Dienstes mit db svc ab:

```
db svc -status myserv
```

# Dienstprogramm für Dienste (dbsvc) für Windows

Erstellt, ändert und löscht SQL Anywhere-Dienste

## Syntax

```
dbsvc [ modifier-options ] -d svc
dbsvc [ modifier-options ] -g svc
dbsvc [ modifier-options ] -l
dbsvc [ modifier-options ] -u svc
dbsvc [ modifier-options ] creation-options -w svc details
dbsvc [ modifier-options ] -x svc
```

details:

```
<full-executable-path> [ options ]
```

Hauptoption	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
-d service-name	Entfernt den betreffenden Dienst aus der Liste der Dienste. Wenn Sie -y angeben, wird der Dienst ohne Bestätigung gelöscht.
-g service-name	Listet die Definition des Dienstes auf. Das Kennwort wird nicht ausgegeben.
-l	Listet die verfügbaren SQL Anywhere-Dienste auf
-u service-name	Startet den Dienst service-name
-x service-name	Stoppt den Dienst service-name

Hauptoption	Beschreibung
<b>-w</b> <i>executable parameters</i>	<p>Erstellt einen neuen Dienst oder überschreibt einen eventuell bereits vorhandenen Dienst desselben Namens. Wenn Sie -y angeben, wird der bestehende Dienst ohne Bestätigung überschrieben. Sie können einen Dienst nicht löschen, während er ausgeführt wird.</p> <p>Sie müssen den vollständigen Pfad zum Programm angeben, das Sie als Dienst verwenden wollen, weil das Konto, unter dem der Dienst läuft, möglicherweise nicht das entsprechende SQL Anywhere-Installationsverzeichnis in seinem Pfad enthält.</p> <p>Sie müssen geeignete Parameter für den zu erstellenden Dienst angeben.</p> <p>Siehe:</p> <ul style="list-style-type: none"> <li>• <b>dbsrv16 und dbeng16</b> „Syntax des SQL Anywhere-Datenbankservers“ auf Seite 203</li> <li>• <b>mlsrv16</b> „MobiLink-Serveroptionen“ [<i>MobiLink - Serveradministration</i>]</li> <li>• <b>dbmlsync</b> „dbmlsync-Syntax“ [<i>MobiLink - Clientadministration</i>]</li> <li>• <b>dblsn</b> „MobiLink Listener-Dienstprogramm für Windows-Geräte (dblsn)“ [<i>MobiLink - Serverinitiierte Synchronisation</i>]</li> <li>• <b>dbremote</b> „SQL Remote-Nachrichtenagent-Dienstprogramm (dbremote)“ [<i>SQL Remote</i>]</li> <li>• <b>dbns</b> „Broadcast Repeater-Dienstprogramm (dbns16)“ auf Seite 891</li> <li>• <b>rshost</b> „Relay Server-Status-Manager als Dienst“ [<i>Relay Server</i>]</li> <li>• <b>rsoe</b> „Outbound Enabler als Dienst“ [<i>Relay Server</i>]</li> <li>• <b>dbvss16</b> „SQL Anywhere-Volumeschattenkopie-Dienst (VSS)“ auf Seite 1042</li> <li>• <b>mlagent</b> „MobiLink-Agenten“ [<i>MobiLink - Serveradministration</i>]</li> </ul>

Erstellungsoption	Beschreibung
<b>-a</b> <i>acct</i>	<p>Benennt das Microsoft Windows-Konto. Alle Dienste werden über ein Microsoft Windows-Konto ausgeführt. Wenn Sie sie unter einem von Ihnen erstellten Konto ausführen, müssen Sie das Konto mit der Option -a benennen und mit der Option -p ein Kennwort angeben.</p> <p>Die Berechtigung "Als Dienst anmelden" ist bei allen Konten außer dem LocalSystem-Konto erforderlich. Wenn für ein Konto die Berechtigung "Als Dienst anmelden" nicht aktiviert ist, werden Sie aufgefordert, sie zu aktivieren. Wenn die Option -y ebenfalls angegeben ist, versucht dbsvc, die Berechtigung "Als Dienst anmelden" zu erteilen, ohne dass Sie zur Eingabe aufgefordert werden. Wenn die Option -q ohne die Option -y angegeben ist, werden Sie nicht aufgefordert, die Berechtigung "Als Dienst anmelden" zu erteilen, und dbsvc schlägt fehl.</p>
<b>-as</b>	<p>Führt den Dienst unter dem LocalSystem-Konto von Microsoft Windows aus. Es ist kein Kennwort erforderlich. Es muss entweder die Option -a oder die Option -as verwendet werden. Alle Dienste werden über ein Microsoft Windows-Konto ausgeführt.</p>
<b>-i</b>	<p>Zeigt ein Symbol an, auf das Sie doppelklicken können, um das Meldungsfenster des Datenbankservers anzuzeigen.</p>
<b>-p</b> <i>password</i>	<p>Gibt das Kennwort für das Konto an, unter dem der Dienst läuft. Verwenden Sie diese Option mit der Option -a.</p>
<b>-rg</b> <i>dependency,...</i>	<p>Gibt eine oder mehrere Lade-Sortiergruppen an, die gestartet sein müssen, bevor der erstellte Dienst gestartet werden kann.</p>
<b>-rs</b> <i>dependency,...</i>	<p>Gibt an, dass alle Dienste in der Liste gestartet sein müssen, bevor der zu erstellende Dienst gestartet werden kann.</p> <p>Sie können entweder den Anzeigenamen oder den Dienstnamen angeben. Dienstnamen werden überprüft, um festzustellen, ob sie bereits vorhanden sind. Wenn der angegebene Dienstname nicht gefunden werden kann, prüft das Dienstprogramm für Dienste (dbsvc), ob es einen Dienst mit einem übereinstimmenden Anzeigenamen gibt.</p> <p>Es wird empfohlen, eine Abhängigkeit von der TDI-Schnittstelle (Transport Data Interface) für TCP/IP zu erstellen, um sicherzustellen, dass die Verbindung richtig gestartet wird. Weitere Hinweise zur TDI-Schnittstelle finden Sie unter <a href="http://msdn.microsoft.com/en-us/library/ms797340.aspx">http://msdn.microsoft.com/en-us/library/ms797340.aspx</a>.</p>
<b>-s</b> <i>startup</i>	<p>Steuert das Startverhalten der Dienste von SQL Anywhere. Sie können das Startverhalten auf "automatisch", "manuell" oder "deaktiviert" setzen. Der Standardwert ist "manuell".</p>

Erstellungsoption	Beschreibung
<b>-sd</b> <i>description</i>	Liefert eine Beschreibung des Dienstes. Die Beschreibung wird im manager angezeigt.
<b>-sn</b> <i>name</i>	<p>Liefert einen Namen für den Dienst. Dieser Name wird im manager angezeigt. Wenn Sie die Option -sn nicht angeben, lautet der Standard-Dienstname SQL Anywhere - <i>svc</i>. Beispiel: Der folgende Dienst wird standardmäßig "SQL Anywhere - myserv" benannt.</p> <pre>dbsvc -as -w myserv "C:\Program Files\SQL Anywhere 16\Bin32\dbeng16.exe"</pre> <p>Damit der Dienstname "myserv" im Windows-Dienst-Manager angezeigt wird, müssen Sie Folgendes ausführen (auf einer Zeile eingegeben):</p> <pre>dbsvc -as -sn myserv -w myserv "C:\Program Files\SQL Anywhere 16\Bin32\dbeng16.exe"</pre>

Erstellungsoption	Beschreibung
<b>-t type</b>	<p>Gibt den Typ für diesen Dienst an. Sie können unter den folgenden Typen auswählen (der alternative Name wird in Klammern aufgeführt):</p> <ul style="list-style-type: none"> <li>• <b>Network</b> Erstellt einen Dienst für den SQL Anywhere-Netzwerk-Datenbankserver (dbsrv16). Siehe „<a href="#">Syntax des SQL Anywhere-Datenbankservers</a>“ auf Seite 203.</li> <li>• <b>Personal (Standalone)</b> Dies ist der Standardwert, der einen Dienst für den Personal Datenbankserver von SQL Anywhere erstellt (dbeng16). Siehe „<a href="#">Syntax des SQL Anywhere-Datenbankservers</a>“ auf Seite 203.</li> <li>• <b>DBRemote</b> Erstellt einen Dienst für den SQL Remote-Nachrichtenagenten. Siehe „<a href="#">SQL Remote-Nachrichtenagent-Dienstprogramm (dbremote)</a>“ [<a href="#">SQL Remote</a>].</li> <li>• <b>MobiLink</b> Erstellt einen Dienst für den MobiLink-Server (mlsrv16). Siehe „<a href="#">mlsrv16-Syntax</a>“ [<a href="#">MobiLink - Serveradministration</a>].</li> <li>• <b>DBMLSync (MLSync)</b> Erstellt einen Dienst für den MobiLink-Synchronisationsclient (dbmlsync). Siehe „<a href="#">dbmlsync-Syntax</a>“ [<a href="#">MobiLink - Clientadministration</a>].</li> <li>• <b>DBNS</b> Erstellt einen Dienst für das Broadcast Repeater-Dienstprogramm (dbns16). Siehe „<a href="#">Broadcast Repeater-Dienstprogramm (dbns16)</a>“ auf Seite 891.</li> <li>• <b>DBLSN (LSN)</b> Erstellt einen Dienst für das MobiLink Listener-Dienstprogramm. Siehe „<a href="#">MobiLink Listener-Dienstprogramm für Windows-Geräte (dblsn)</a>“ [<a href="#">MobiLink - Serverinitiierte Synchronisation</a>].</li> <li>• <b>DBVSS (VSS)</b> Erstellt einen Dienst für das SQL Anywhere VSS-Schreibprogramm. Siehe „<a href="#">SQL Anywhere-Volumeschattenkopie-Dienst (VSS)</a>“ auf Seite 1042.</li> <li>• <b>RSHOST</b> Erstellt einen Dienst für den Relay Server Status-Manager. Siehe „<a href="#">Befehlszeilensyntax des Relay Server Status-Managers (rshost)</a>“ [<a href="#">Relay Server</a>].</li> <li>• <b>RSOE</b> Erstellt einen Dienst für den Outbound Enabler. Siehe <a href="#">Outbound Enabler-Syntax</a> [<a href="#">Relay Server</a>].</li> <li>• <b>MLAGENT</b> Erstellt einen Dienst für den MobiLink-Agent. Siehe „<a href="#">MobiLink-Agenten</a>“ [<a href="#">MobiLink - Serveradministration</a>].</li> </ul>

Erstellungsoption	Beschreibung
	<ul style="list-style-type: none"> <li>• <b>OData</b> Erstellt einen Dienst für das OData Server-Dienstprogramm. Siehe „<a href="#">OData Server-Dienstprogramm (dbosrv16.exe)</a>“ [<a href="#">SQL Anywhere Server - Programmierung</a>].</li> </ul>

Änderungsoption	Beschreibung
<b>-cm</b>	<p>Zeigt den Befehl an, der zum Erstellen des Dienstes verwendet wurde. Mit dieser Option kann der Erstellungsbefehl in eine Datei ausgegeben werden, die verwendet werden kann, um den Dienst auf einem anderen Computer zu installieren oder den ursprünglichen Zustand eines Dienstes wiederherzustellen, sofern er geändert wurde. Sie müssen die Optionen -g oder -l zusammen mit der Option -cm verwenden, andernfalls schlägt der Befehl fehl. Die Angabe der Option -g zeigt den Erstellungsbefehl für den angegebenen Dienst an, während die Angabe der Option -l den Erstellungsbefehl für alle Dienste anzeigt.</p> <p>Wenn der angegebene Dienst nicht existiert, wird der Befehl zum Löschen des Dienstes generiert. Beispiel: Wenn service_1 auf dem Computer nicht existiert, würde <code>dbsvc -cm -g service_1</code> den folgenden Befehl zurückgeben, um den service_1-Dienst zu löschen:</p> <pre>dbsvc -y -d "service_1"</pre> <p>Wenn der Dienst nicht das LocalSystem-Konto verwendet, gibt es keine Möglichkeit, das Kennwort abzurufen, daher wird es nicht in den Befehl aufgenommen, der generiert wird. Wenn Sie den Dienst mit <code>-a user -p password</code> erstellt haben, wird nur <code>-a user</code> in die Ausgabe aufgenommen.</p>
<b>-o filename</b>	<p>Schreibt die Ausgabe aus dem Dienstprogramm für Dienste (dbsvc) in die angegebene Datei. Die Option -o muss vor den Optionen -d, -g, -l, -u, -w und -x angegeben werden. Zum Beispiel:</p> <pre>dbsvc -o out1.txt -y -as -w mysrv "%SQLANY16%\bin32\dbosrv16" -n mysrv -o c:\out2.txt</pre> <p>In diesem Fall wird die Ausgabe aus dbsvc in <code>out1.txt</code> protokolliert, während die Ausgabe vom Datenbankserver beim Starten des Datenbankservers in <code>c:\out2.txt</code> protokolliert wird.</p>
<b>-q</b>	<p>Unterdrückt Meldungen im Meldungsfenster des Datenbankservers. Wenn Sie die Option -q angeben, sollten Sie auch unter Verwendung der Option -o eine Datei angeben, in der die Meldungen protokolliert werden. Wenn Sie beim Ändern oder Löschen eines existierenden Dienstes diese Option angeben, müssen Sie auch die Option -y angeben, sonst schlägt der Vorgang fehl.</p>

Änderungsoption	Beschreibung
<b>-y</b>	Führt den Vorgang automatisch aus, ohne eine Bestätigung zu verlangen. Diese Option kann mit der Option -w oder -d verwendet werden. Wenn Sie beim Ändern oder Löschen eines existierenden Dienstes die Option -q angeben, müssen Sie auch -y angeben, sonst schlägt der Vorgang fehl.

## Bemerkungen

Ein Dienst führt einen Datenbankserver oder eine andere Anwendung aus, indem er die eingegebenen Optionen berücksichtigt. Dieses Dienstprogramm bietet eine umfassende Möglichkeit, SQL Anywhere-Dienste unter Windows zu verwalten. Um das Dienstprogramm für Dienste (dbsvc) verwenden zu können, müssen Sie Mitglied der Administratorengruppe für den lokalen Computer sein.

Sie können das Dienstprogramm für Dienste folgendermaßen starten:

- In Sybase Central verwenden Sie den **Assistenten zum Erstellen eines neuen Dienstes**.
- An einer Eingabeaufforderung verwenden Sie das Dienstprogramm für Dienste (dbsvc).

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag).

## Siehe auch

- „Windows-Dienste erstellen (Sybase Central)“ auf Seite 182
- „Windows-Dienste“ auf Seite 181
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]

## Beispiel

Erstellen Sie den Personal Server myserv, der den angegebenen Server mit den angegebenen Parametern startet. Der Server läuft als LocalSystem-Benutzer:

```
dbsvc -as -w myserv
"C:\Program Files\SQL Anywhere 16\Bin32\dbeng16.exe"
-n myeng -c 8m "c:\temp\mysample.db"
```

Erstellen Sie einen Netzwerkserverdienst namens mynetworkserv. Der Server läuft unter dem lokalen Konto und startet automatisch, wenn der Computer wieder hochgefahren wird:

```
dbsvc -as -s auto -t network -w mynetworkserv
"C:\Program Files\SQL Anywhere 16\Bin32\dsrv16.exe"
-x tcpip -c 8m "c:\temp\mysample.db"
```

Listen Sie alle Details über den myserv-Dienst auf:

```
dbsvc -g myserv
```

Löschen Sie den Dienst myserv, ohne dass eine Bestätigung verlangt wird:

```
dbsvc -y -d myserv
```

Einen Dienst erstellen, der vom Workstation-Dienst und der TDI-Gruppe abhängt:

```
dbsvc -rs lanmanworkstation -rg TDI -w ...
```

Erstellen Sie den Dienst mysyncservice:

```
dbsvc -as -s manual -t dbmlsync -w mysyncservice  
"C:\Program Files\SQL Anywhere 16\Bin32\dbmlsync.exe"  
-c "SQL Anywhere 16 CustDB"
```

Generieren Sie den Befehl zum Erstellen des service\_1-Dienstes und geben Sie ihn in eine Datei namens *restoreservice.bat* aus:

```
dbsvc -cm -g service_1 > restoreservice.bat
```

Die Datei *restoreservice.bat* enthält Folgendes:

```
dbsvc -t Standalone -s Manual -as -y -w "service_1"  
"C:\Program Files\SQL Anywhere 16\Bin32\dbeng16.exe"
```

Erstellen Sie einen MobiLink Listener-Dienst, der manuell gestartet wird:

```
dbsvc -as -i -w myListener  
"C:\Program Files\SQL Anywhere 16\Bin32\dblsn.exe" "@c:\temp\dblsn.opt"
```

Starten Sie den myListener-Dienst:

```
dbsvc -u myListener
```

Stoppen Sie den myListener-Dienst:

```
dbsvc -x myListener
```

Erstellen Sie einen Volume-Schattenkopiedienst (VSS), der automatisch gestartet wird, wenn der Datenbankserver startet:

```
dbsvc -as -s Automatic -t vss -w SAVSSWriter  
"C:\Program Files\SQL Anywhere 16\Bin32\dbvss16.exe"
```

Erstellen Sie einen OData-Dienst mit den in der Datei *server.properties* angegebenen Optionen:

```
dbsvc -as -t OData -w MyODataServer "C:\Program Files\SQL Anywhere  
16\Bin64\dbosrv16.exe" "C:\server.properties"
```

## SQL Anywhere-Konsolendienstprogramm (dbconsole)

Stellt Verwaltungs- und Monitoring-Funktionen für Datenbankserver-Verbindungen zur Verfügung

### Syntax

**dbconsole** [ *options* ]

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „ <a href="#">Konfigurationsdateien</a> “ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „ <a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a> “ auf Seite 922.
-c "key-word=value; ..."	Legt Verbindungsparameter fest. Siehe „ <a href="#">Verbindungsparameter</a> “ auf Seite 337.
-datasource DSN-name	Legt eine ODBC-Datenquelle zum Verbinden fest. Es ist nicht erforderlich, den SQL Anywhere JDBC-Treiber zu benutzen, um diese Option verwenden zu können.
-host hostname	Gibt <i>hostname</i> oder die IP-Adresse des Computers an, auf dem der Datenbankserver läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen.
-port port-number	Gibt die Portnummer des laufenden Datenbankservers an. Die Standard-Portnummer für SQL Anywhere ist <b>2638</b> .

### Privilegien

Keine.

### Bemerkungen

Mit dem SQL Anywhere-Konsolendienstprogramm können Sie den Server von einem Clientsystem aus überwachen. Dieses Dienstprogramm wird auch Netzwerkserver-Monitor genannt. Sie können damit verfolgen, wer an einem Datenbankserver in Ihrem Netzwerk angemeldet ist. Sie können auch die Datenbankserver- und die Clientstatistik auf Ihrem lokalen Bildschirm anzeigen, Benutzerverbindungen trennen und den Datenbankserver konfigurieren. Die SQL Anywhere-Konsole kann Informationen für mehrere Verbindungen anzeigen.

Die SQL Anywhere-Konsole steht für alle unterstützten Plattformen ausgenommen Windows Mobile, IBM AIX, HP-UX und HP-UX Itanium zur Verfügung. Auf diesen Plattformen können Sie die Eigenschaften der Verbindungsebene, der Serverebene und der Datenbankebene verwenden, um Informationen zu erhalten oder um Ihren Server von einem Computer aus zu überwachen, der ein Betriebssystem ausführt, das die SQL Anywhere-Konsole unterstützt (wie Windows, Mac OS X oder Linux).

Weitere Hinweise zum Bezug von Eigenschaftswerten finden Sie unter „[Verbindungs-, Datenbank- und Datenbankserveigenschaften](#)“ auf Seite 710.

### Siehe auch

- „[SQL Anywhere-Konsolendienstprogramm \(dbconsole\)](#)“ auf Seite 877

**Beispiel**

Mit dem folgenden Befehl verbinden Sie sich unter Benutzer-ID "DBA" und Kennwort "sql" mit der Standarddatenbank:

```
dbconsole -c "UID=DBA;PWD=sql"
```

## Dienstprogramm für den Serverstart im Hintergrund (dbspawn)

Startet einen Datenbankserver im Hintergrund

**Syntax**

**dbspawn** [ *options* ] *server-command*

Option	Beschreibung
@ <i>data</i>	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Wenn beide mit demselben Namen vorhanden sind, wird die Umgebungsvariable verwendet.</p> <p>Das Dienstprogramm für den Serverstart im Hintergrund (dbspawn) ermöglicht die Angabe einer Referenz auf eine Konfigurationsdatei im zu erstellenden Befehl, aber es ist nicht möglich, eine Konfigurationsdatei mit Optionen für das dbspawn-Dienstprogramm anzugeben. Der erste Befehl unten wird beispielsweise unterstützt, aber der zweite Befehl wird <i>nicht</i> unterstützt:</p> <pre>dbspawn dbeng16 @myconfig.ini</pre> <pre>dbspawn @spawnopts.ini dbeng16 demo.db</pre> <p>Weitere Hinweise finden Sie unter „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
<b>-f</b>	Zwingt dbspawn, einen Datenbankserver zu starten, auch wenn ein Standarddatenbankserver bereits vorhanden ist.
<b>-p</b>	<p>Gibt an, dass nach dem Starten des Datenbankservers die Prozesskennung des Betriebssystems für den Datenbankserver-Prozess zurückgegeben werden soll. Zum Beispiel:</p> <pre>Neue Prozess-ID ist 306</pre>
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.

Option	Beschreibung
<i>server-command</i>	Gibt die Befehlszeile zum Starten des Datenbankservers an. Siehe „ <a href="#">Syntax des SQL Anywhere-Datenbankservers</a> “ auf Seite 203.

## Privilegien

Keine.

## Bemerkungen

Das Dienstprogramm dbspawn wird bereitgestellt, um einen Server im Hintergrund zu starten. dbspawn startet den Server im Hintergrund und gibt einen Exitcode "0" (Erfolg) oder Nicht-Null (Fehlgeschlag) zurück. Wenn ein neuer Server erfolgreich gestartet wurde, gibt dbspawn keine Rückmeldung aus, bis die Initialisierung des Datenbankservers abgeschlossen und er bereit ist, Anforderungen anzunehmen.

Standardmäßig kann dbspawn keinen neuen Server auf einem Computer starten, auf dem ein Standard-Datenbankserver ausgeführt wird. Um einen Server auf einem Computer zu starten, auf dem ein Standard-Datenbankserver läuft, geben Sie die Option -f an.

Weitere Informationen zu Beendigungscodes finden Sie unter „[Exit-Codes der Softwarekomponenten](#)“ [[SQL Anywhere Server - Programmierung](#)].

Das Dienstprogramm dbspawn ist beim Starten eines Servers mithilfe einer Batchdatei von Nutzen, vor allem wenn nachfolgende Befehle in der Batchdatei es erfordern, dass ein Server Anforderungen akzeptiert.

Wenn der angegebene Pfad zumindest eine Leerstelle enthält, müssen Sie ihn in Anführungszeichen setzen. Zum Beispiel:

```
dbspawn dbeng16 "c:\my databases\mysalesdata.db"
```

Wenn der angegebene Pfad keine Leerstellen enthält, sind keine Anführungszeichen erforderlich.

# Serverstopp-Dienstprogramm (dbstop)

Stoppt eine Datenbank oder einen Datenbankserver

## Syntax

**dbstop** [ *options* ] [ *server-name* ]

Option	Beschreibung
<i>@data</i>	Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.

Option	Beschreibung
<b>-c</b> "key-word=value; ..."	Gibt eine Verbindungszeichenfolge an. Beim Stoppen eines Netzwerkserver muss die Verbindungszeichenfolge eine Benutzer-ID enthalten, die die Berechtigung zum Stoppen des Servers besitzt. Standardmäßig ist zum Stoppen eines Netzwerkserver das SERVER OPERATOR-Systemprivileg erforderlich und alle Benutzer können einen Personal Server herunterfahren. Mit der Serveroption -gk kann dies jedoch geändert werden.  Wenn Sie Verbindungsparameter eingeben, dürfen Sie keinen Servernamen angeben.
<b>-d</b>	Der Datenbankserver wird nicht gestoppt. Nur die in der Verbindungszeichenfolge angegebene Datenbank wird gestoppt. Die Serveroption -gd steuert die erforderlichen Berechtigungen zum Stoppen einer Datenbankdatei.
<b>-o</b> filename	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-x</b>	Der Server wird nicht gestoppt, wenn noch aktive Verbindungen mit dem Server bestehen. Das Verwenden dieser Option verhindert, dass dbstop eine Bestätigung anfordert, wenn aktive Verbindungen bestehen.
<b>-y</b>	Der Server wird gestoppt, selbst wenn weiterhin aktive Verbindungen mit dem Server bestehen. Dies entspricht der Aufnahme von Unconditional=YES in die Verbindungsparameter.
server-name	Gibt den Namen des Datenbankserver an, der auf dem aktuellen Computer läuft. Der Datenbankserver muss so gestartet werden, dass keine Berechtigungen erforderlich sind, um ihn herunterzufahren. Der Personal Datenbankserver startet standardmäßig in diesem Modus. Für den Netzwerk-Datenbankserver müssen Sie die Option <b>-gk all</b> angeben.  Wenn Sie einen Servernamen eingeben, dürfen Sie keine Verbindungsparameter verwenden.

## Privilegien

Beim Stoppen eines Netzwerkserver müssen Sie eine Verbindungszeichenfolge mit einer Benutzer-ID angeben, die Berechtigungen zum Stoppen des Servers besitzt. Standardmäßig ist zum Stoppen des Netzwerkserver das SERVER OPERATOR-Systemprivileg erforderlich. Alle Benutzer können einen Personal Server herunterfahren. Sie können die Server-Befehlszeilenoption -gk verwenden, um das Standardverhalten zu ändern.

## Bemerkungen

Das Serverstopp-Dienstprogramm stoppt einen Datenbankserver. Sie können die Option -d benutzen, um eine bestimmte Datenbank zu stoppen.

Das Serverstopp-Dienstprogramm kann nur von der Eingabeaufforderung aus ausgeführt werden. In Windows-Umgebungen können Sie einen Datenbankserver stoppen, indem Sie auf **Herunterfahren** im Meldungsfenster des Datenbankservers klicken.

Mit Optionen können Sie steuern, ob ein Server gestoppt wird, auch wenn er aktive Verbindungen hat, und ob der gesamte Server oder nur eine Datenbank gestoppt werden soll.

Das Verhalten von dbstop kann gesteuert werden, falls aktive Verbindungen auf dem Server bestehen. Wenn aktive Verbindungen bestehen, zeigt dbstop eine Eingabeaufforderung zum Herunterfahren des Servers an. Mit den Optionen -x und -y können Sie dieses Verhalten ändern.

Wenn dbstop in der Lage ist, den Datenbankserver zu stoppen, wird dbstop erst beendet, wenn alle Datenbanken gestoppt wurden und der Datenbankserver so weit heruntergefahren wurde, dass ein anderer Server mit demselben Namen und denselben Datenbanken gestartet werden kann. Wenn dbstop erfolgreich beendet, läuft der Datenbankserver-Prozess möglicherweise weiter, und einige seiner Ressourcen, wie z.B. die mit der Option -o angegebene Ausgabedatei, sind weiterhin in Verwendung.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

Wenn Sie die SQLCONNECT-Umgebungsvariable mit dbstop verwenden möchten, geben Sie die Option -c an. Anderenfalls könnten Sie unerwartete Ergebnisse erhalten.

### Siehe auch

- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]
- „STOP SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Konfigurationsdateien“ auf Seite 882
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Verbindungsparameter“ auf Seite 337
- „Verbindungsparameter Unconditional (UNC)“ auf Seite 386
- „Datenbankserveroption -gd “ auf Seite 240
- „Datenbankserveroption -gk “ auf Seite 242

### Beispiel

Sie betreiben den Server "myserver" ohne Datenbank. Um den Server zu stoppen, geben Sie die Dienstprogrammdateiabank als einen Verbindungsparameter DatabaseName (DBN) an:

```
dbstop -c "UID=DBA;PWD=sql;Server=myserver;DBN=utility_db"
```

Sie betreiben den Server "myserver" mit der gestarteten Datenbank *demo.db*. So stoppen Sie den Server und die Datenbank:

```
dbstop -c "UID=DBA;PWD=sql;Server=myserver"
```

Sie betreiben einen Personal Server namens "myserver". So stoppen Sie den Server und die Datenbanken, selbst wenn es Verbindungen gibt:

```
dbstop -y myserver
```

Sie betreiben einen Server "myserver" mit der gestarteten Datenbank *demo.db*. Um nur die Datenbank namens "demo" zu stoppen, ohne andere Datenbanken oder den Server selbst zu stoppen, führen Sie den folgenden Befehl aus:

```
dbstop -c "UID=DBA;PWD=sql;Server=myserver;DBN=demo" -d
```

## Dienstprogramm für Supportanfragen (dbsupport)

Sendet Performancedaten zu Fehlern und Diagnoseinformationen an den technischen Support.

### Syntax

**dbsupport** [ *options* ] *operation* [ *operation-specific-option* ]

**dbsupport** *configuration-options*

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „Konfigurationsdateien“ auf Seite 882.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien (dbhide) auf die Konfigurationsdatei anwenden. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbhide)“ auf Seite 922.
-o filename	Sendet Log-Ausgabemeldungen in die angegebene Datei.
-q	Zeigt nur kritische Log-Ausgabemeldungen an.

Vorgang	Beschreibung
-e configuration-option	<p>Zeigt die Einstellung für die angegebene Konfigurationsoption an. Beispiel: Angenommen, Sie haben folgenden Befehl ausgeführt, um dbsupport zur Eingabeaufforderung zu konfigurieren, wenn dies möglich ist:</p> <pre>dbsupport -cc promptdefy</pre> <p>Wenn Sie den Befehl dbsupport -ecc ausführen werden folgende Einstellungen zurückgegeben:</p> <pre>-cc "promptdefy"</pre> <p>Wenn der aktuelle Wert der Konfigurationsoption nie explizit gesetzt wurde, wird kein Echo zurückgegeben.</p>
-is submission-ID [ -rr N ]	<p>Prüft den Status eines Crash-Berichts, der an den technischen Support gesendet wurde.</p> <p>Der folgende Befehl gibt beispielsweise den Status der Einsende-ID 66 zurück:</p> <pre>dbsupport -is 66</pre>

Vorgang	Beschreibung
<b>-iu</b> [ <b>-r</b> <i>N</i> ]	<p>Sucht nach Updates für Ihren Software-Build. Zu den Updates gehört Folgendes:</p> <ul style="list-style-type: none"><li>• <b>Supportpakete</b> Ein Supportpaket ist eine Teilmenge der Software mit einer oder mehreren Fehlerbehebungen. Die Fehlerbehebungen werden in den Versionshinweisen für das Update aufgelistet. Updates zu Fehlerbehebungen können nur in eine installierte Software mit derselben Versionsnummer übernommen werden. Obwohl einige Tests der Software vorgenommen wurden, sollten Sie diese Dateien nicht mit Ihrer Anwendung verteilen, es sei denn, Sie haben Ihre Anwendung gründlich mit der Software getestet.</li><li>• <b>Minor Releases</b> Eine Minor Release ist eine vollständige Software, mit der ein Upgrade der installierten Software von einer älteren Version mit derselben Hauptversionsnummer durchgeführt wird. (Das Versionsnummernformat lautet <i>Hauptversion.Minor_Release.Build</i>). Fehlerbehebungen und andere Änderungen werden in den Versionshinweisen für das Upgrade aufgelistet.</li></ul> <p>Sie können auch mit Interactive SQL, Sybase Central und dem SQL Anywhere-Konsolendienstprogramm (dbconsole) nach Updates suchen. Siehe „<a href="#">Software-Updates</a>“ auf Seite 879.</p>
<b>-lc</b>	<p>Generiert eine Liste aller Crash-Berichte, die nicht an den technischen Support gesendet wurden. Die aufgelisteten Berichtsnamen können mit der Option -sc verwendet werden.</p>

Vorgang	Beschreibung
<b>-ls</b>	<p>Generiert eine Liste der Einsende-IDs für alle Berichte, die gesendet wurden. Zum Beispiel:</p> <pre>dbsupport -ls</pre> <p>Dieser Befehl gibt Informationen ähnlich den folgenden zurück:</p> <pre>SQL Anywhere Support Utility Version 16.0.2040 Submission ID: 217756   reported: Wed Jul 30 15:54:43 2011 Submission ID: 217757   reported: Wed Jul 30 15:57:07 2011 Submission ID: 217759   reported: Wed Jul 30 16:14:24 2011 Submission ID: 217760   reported: Wed Jul 30 16:14:30 2011 Submission ID: 217761   reported: Wed Jul 30 16:28:12 2011 Submission ID: 221030   reported: Mon Sep 08 12:34:59 2011 Submission ID: 221031   reported: Mon Sep 08 12:35:05 2011</pre>
<b>-pc</b> <i>filename</i>	Zeigt Crash-Berichtsinformationen an. Sie können diese Option verwenden, um Informationen anzuzeigen, bevor sie eingesendet werden.
<b>-pd</b>	Zeigt die gesammelten Diagnoseinformationen an. Sie können diese Option verwenden, um Informationen anzuzeigen, bevor sie eingesendet werden.
<b>-ps</b> <i>submission-ID</i>	<p>Zeigt Informationen zu einem bestimmten Bericht an, der eingesendet wurde. Der Befehl <code>dbsupport -ps 4</code> gibt beispielsweise Informationen zu Einsendung 4 zurück:</p> <pre>SQL Anywhere Support Utility Version 16.0.2040 Submission ID: 217756   reported: Wed Jul 30 15:54:43 2012</pre>
<b>-sa</b> [ <b>-r</b> <i>number-of-submission-retries</i> ]	Sendet alle im Diagnoseverzeichnis gespeicherten Crash-Berichte und Diagnoseinformationen ein.

Vorgang	Beschreibung
<b>-sc</b> <i>reportname</i> [ <b>-r</b> <i>number-of-submission-retries</i> ] [ <b>-nr</b>   <b>-rr</b> <i>N</i> ]	<p>Sendet einen Crash-Bericht und Diagnoseinformationen ein. Zum Beispiel:</p> <pre>dbsupport -sc SA16_20051220_133828_32116</pre> <p>Verwenden Sie die Option <b>-lc</b>, um eine Liste der Berichte zu generieren, die nicht eingesendet wurden.</p>
<b>-sd</b> [ <b>-r</b> <i>number-of-submission-retries</i> ]	<p>Sendet nur Diagnoseinformationen ein.</p> <p>Weitere Hinweise zum Diagnoseverzeichnis finden Sie unter „<a href="#">SADIAGDIR-Umgebungsvariable</a>“ auf Seite 473.</p>

Konfigurationsoption	Beschreibung
<b>-cc [ autosubmit   no   promptDefY   promptDefN ]</b>	<p>Ändert das Bedieneraufforderungsverhalten von dbsupport. Sie können eine der folgenden Optionen angeben:</p> <ul style="list-style-type: none"> <li>• <b>autosubmit</b> Crash-Berichte automatisch ein-senden und Diagnoseberichte regelmäßig senden.</li> <li>• <b>no</b> Nicht zur Eingabe der Berechtigung, Berichte einzusenden, auffordern. Berichte wer-den nicht eingesendet.</li> <li>• <b>promptDefY</b> Wenn möglich zur Eingabe der Berechtigung, den Bericht einzusenden, auffor-dern. Wenn keine Antwort gegeben wird, wird der Bericht eingesendet.</li> <li>• <b>promptDefN</b> Wenn möglich zur Eingabe der Berechtigung, den Bericht einzusenden, auffor-dern. Wenn keine Antwort gegeben wird, wird der Bericht nicht eingesendet. Dies ist die Standard-einstellung.</li> </ul> <p>Wenn Sie beispielsweise Embedded SQL Anyw-here in einer Anwendung verwenden, kann es sinnvoll sein, das Dienstprogramm für Supportan-fragen so zu konfigurieren, dass keine Berichte eingesendet werden.</p> <p>Wenn Sie die Option -cc angeben, wird ihr Wert vom Dienstprogramm für Supportanfragen (dbsupport) als Standardwert verwendet. Die Einstellung wird in der Datei <i>dbsupport.ini</i> im Diagnoseverzeichnis gespei-chert.</p> <p>Der folgende Befehl konfiguriert das Dienstpro-gramm für Supportanfragen dergestalt, dass keine Berichte eingesendet werden und der Benutzer nie-mals aufgefordert wird, Berichte einzusenden:</p> <pre>dbsupport -cc no</pre> <p>Siehe „Regelmäßig Performancedaten sen-den“ auf Seite 1108.</p>

Konfigurationsoption	Beschreibung
<b>-cd</b> <i>retry-delay</i>	<p>Gibt die Verzögerung bei Neuversuchen (in Sekunden) für die Einsendung eines Berichts an, wenn der vorherige Versuch fehlgeschlagen ist. Der Standardverzögerung ist 30 Sekunden.</p> <p>Wenn Sie diese Option angeben, wird ihr Wert vom Dienstprogramm für Supportanfragen als Standardwert verwendet. Die Einstellung wird in der Datei <i>dbsupport.ini</i> im Diagnoseverzeichnis gespeichert.</p> <p>Der folgende Befehl legt fest, dass fehlgeschlagene Einsendungen alle drei Sekunden bis zu einem Maximum von vier Versuchen erneut versucht werden sollen, bis aufgegeben wird:</p> <pre>dbsupport -cr 4 -cd 3</pre>
<b>-ce</b> <i>email-address;email-server[:port ][;user-id:password ]</i>	<p>Gibt die Adresse an, an die die E-Mail nach einem Crash geschickt werden soll. Die E-Mail wird über den SMTP-Server <i>E-Mail-Server</i> verschickt. Optional können Sie den zu verwendenden Port sowie Benutzer-ID und Kennwort für die Authentifizierung beim SMTP-Server angeben.</p>
<b>-cet</b>	<p>Testet die mit der Option -ce angegebenen E-Mail-Einstellungen.</p>
<b>-cid</b> <i>customer-id</i>	<p>Gibt eine Zeichenfolge an, durch die Sie im Einsendebericht identifiziert werden. Wenn Sie diese Option angeben, wird ihr Wert vom Dienstprogramm für Supportanfragen als Standardwert verwendet. Die Konfiguration wird in der <i>dbsupport.ini</i>-Datei im Diagnoseverzeichnis gespeichert.</p> <p>Das folgende Beispiel legt eine Kunden-Identifizierungszeichenfolge für dbsupport fest:</p> <pre>dbsupport -cid myid@company.com</pre> <pre>dbsupport -cid "MyClientApp 1.0"</pre>
<b>-cid-</b>	<p>Entfernt die Zeichenfolge für die Kundenidentifizierung aus der Datei <i>dbsupport.ini</i>.</p>

Konfigurationsoption	Beschreibung
<b>-cp</b> { <i>host</i> [ <i>:port</i> ]   <b>autodetect</b> }	<p>Konfiguriert den HTTP-Proxy-Host und den Port, die zum Einsenden von Fehlerberichten verwendet werden. Der Standardport ist 80.</p> <p>Wenn Sie <code>-cp autodetect</code> unter Windows angeben und ein Proxy-Server und -Port für Internet Explorer eingestellt wurden, konfiguriert dbsupport seinen Proxy-Server und -Port mit den Systemeinstellungen.</p> <p>Wenn Sie <code>-cp autodetect</code> unter Unix angeben und die <code>HTTP_PROXY</code>-Umgebungsvariable gesetzt ist, konfiguriert dbsupport seinen Proxy-Server und -Port mit der Einstellung der Umgebungsvariablen.</p>
<b>-cp-</b>	Entfernt die HTTP-Proxy-Host- und Port-Einstellungen aus der Datei <i>dbsupport.ini</i> .
<b>-cr</b> <i>number-of-submission-retries</i>	<p>Gibt an, wie viel Mal eine fehlgeschlagene Einsendung wiederholt werden soll.</p> <p>Wenn Sie diese Option angeben, wird ihr Wert vom Dienstprogramm für Supportanfragen als Standardwert verwendet. Die Einstellung wird in der Datei <i>dbsupport.ini</i> im Diagnoseverzeichnis gespeichert.</p> <p>Der folgende Befehl legt fest, dass fehlgeschlagene Vorgänge alle drei Sekunden bis zu einem Maximum von vier Versuchen erneut versucht werden sollen, bis aufgegeben wird:</p> <pre>dbsupport -cr 4 -cd 3</pre>
Vorgangsspezifische Option	Beschreibung
<b>-ac</b>	Fügt der Übertragung einen Kommentar hinzu.
<b>-af</b>	Fügt der Übertragung eine Datei hinzu. Sie können die Option <code>-af</code> mehr als einmal angeben, um der Übertragung mehrere Dateien hinzuzufügen.

Vorgangsspezifische Option	Beschreibung
<b>-nr</b>	<p>Gibt an, dass dbsupport den Datenbankserver nicht auf den Status der Einsendung prüft. Der folgende Befehl z.B. sendet den Bericht ein, überprüft aber nicht den Status der neuen Einsendung:</p> <pre>dbsupport -nr -sc SA16_20051220_133828_32116</pre> <p>Standardmäßig überprüft dbsupport, ob es bereits eine Lösung für das eingesendete Problem gibt.</p>
<b>-r</b> <i>number-of-submission-retries</i>	Gibt an, wie oft dbsupport maximal versuchen soll, die Übertragung zu wiederholen. Die Angabe 0 bedeutet unbegrenzte Neuversuche. Der Standardwert ist 10. Die Angabe der Option -r setzt den in der Datei <i>dbsupport.ini</i> gespeicherten Wert -cr außer Kraft, falls vorhanden.
<b>-rd</b> <i>retry-delay</i>	Gibt an, wie viele Sekunden dbsupport zwischen den Neuversuchen zur Übermittlung des Berichts wartet. Der Standardwert ist 30. Die Angabe der Option -rd setzt den in der Datei <i>dbsupport.ini</i> gespeicherten Wert -cd außer Kraft, falls vorhanden.
<b>-rr</b> <i>number-of-submission-response-retries</i>	Gibt an, wie oft dbsupport maximal versuchen soll, eine Antwort auf die Übermittlung zu erhalten. Die Angabe 0 bedeutet unbegrenzte Neuversuche. Der Standardwert ist 10.

## Privilegien

Keine.

## Bemerkungen

Performancedaten, z.B. Crash-Berichte und Diagnoseinformationen, tragen zur Verbesserung des Produkts bei.

Wenn in einem SQL Anywhere-Programm ein schwerwiegender Fehler oder ein Absturz auftritt, wird ein Fehlerbericht erstellt, der technische Informationen über das Programm zum Zeitpunkt des Fehlers enthält. Nach dem Erstellen eines Fehlerberichts werden Sie aufgefordert, diesen Bericht an den technischen Support zu senden.

Sie können diesen Bericht auch mithilfe des Dienstprogramms für Supportanfragen (dbsupport) senden. Das Einsenden von Fehlerberichten hilft bei der Diagnose der Ursache von schwerwiegenden Fehlern oder Assertions. Sobald ein Fehlerbericht eingesendet wurde, erhalten Sie eine Einsende-ID, die Sie beim technischen Support angeben können. Wenn Sie das Problem dem technischen Support melden, kann das Senden dieser Fehlerdatei dessen Bearbeitung beschleunigen. Es wird empfohlen, dass Sie Fehler- und

Diagnoseberichte einsenden, um zur Verbesserung des Produkts beizutragen, auch wenn Sie sich nicht an den technischen Support wenden möchten.

Das Dienstprogramm für Supportanfragen (dbsupport) kann für die folgenden Aufgaben verwendet werden:

- Diagnoseinformationen und Crash-Berichte einsenden
- Funktionsstatistiken einsenden
- Informationen über eingesendete und nicht-eingesendete Crash-Berichte auflisten
- Informationen über eingesendete und nicht-eingesendete Crash-Berichte drucken
- Den Status einer Einsendung abfragen
- Abfragen, ob Software-Updates für Ihre Version von SQL Anywhere verfügbar sind
- Das Verhalten von dbsupport für den Fall konfigurieren, dass ein schwerwiegender Fehler (Assertion/ Absturz) erkannt wird. Es kann z.B. so konfiguriert werden, dass ein bestimmtes Handler-Programm jedes Mal ausgeführt wird, wenn der Datenbankserver einen Fehlerbericht einsendet. Diese Funktion ist nützlich, um Ihre eigenen benutzerdefinierten Aktionen dem Fehlerbehandlungsprozess hinzuzufügen.
- Konfigurieren, wie oft das Senden eines Berichts wiederholt werden soll. Beim Einsenden eines Berichts kann es z.B. so konfiguriert werden, dass der Vorgang in 30 Sekunden erneut versucht wird, bis zu einem Maximum von zehn Versuchen. Diese Funktion ist nützlich, wenn der Dienst möglicherweise zeitweilig nicht verfügbar ist.

Einstellungen für das Dienstprogramm für Supportanfragen werden in der *dbsupport.ini*-Datei im Diagnoseverzeichnis gespeichert.

Die vorgangsspezifischen Optionen sind nützlich, um das Standardverhalten außer Kraft zu setzen, einschließlich von jenen Optionen, die in der Datei *dbsupport.ini* gespeichert sind:

Die grafischen Administrationstools können so konfiguriert werden, dass die Option die zum Einsenden von Fehlerberichten entfernt wird. Siehe „[Konfiguration der Administrationstools](#)“ [*SQL Anywhere Server - Programmierung*].

Wenn Sie einen Fehlerbericht nicht einsenden, verbleibt er im Diagnoseverzeichnis auf Ihrer Festplatte. Dieses Verzeichnis wird von den Softwareprogrammen automatisch erstellt und dient nur dazu, Fehlerberichte sowie Einstellungen des Dienstprogramms für Supportanfragen (dbsupport) zu speichern.

**Speicherort des Diagnoseverzeichnisses** Der Speicherort des Diagnoseverzeichnisses hängt von der Plattform ab.

Der Datenbankserver sucht in der folgenden Reihenfolge an den angegebenen Speicherorten nach dem Diagnoseverzeichnis:

- **Windows (außer Windows Mobile)**

1. Das durch die SADIAGDIR-Umgebungsvariable angegebene Verzeichnis, falls diese gesetzt wurde.
2. Der Standardspeicherort des Diagnoseverzeichnisses:
  - Unter Windows XP *%ALLUSERSPROFILE%\Application Data\SQL Anywhere 16\diagnostics*
  - Unter Windows Vista und höher *%ALLUSERSPROFILE%\SQL Anywhere 16\diagnostics*
3. Das aktuelle Verzeichnis.
4. Das temporäre Verzeichnis. Siehe SATMP-Umgebungsvariable sowie Umgebungsvariablen TMP, TMPDIR und TEMP.

Unter Windows befindet sich das Diagnoseverzeichnis an einem Speicherort, auf den alle Benutzer des Computers Schreibzugriff haben. Wenn ein Computer über eine Anzahl von Benutzerkonten verfügt und Sie die Fehlerberichte eines Benutzers von denen anderer Benutzer getrennt halten möchten, setzen Sie die SADIAGDIR-Umgebungsvariable für jeden Benutzer auf ein Verzeichnis, auf das nur der jeweilige Benutzer Lese- und Schreibzugriff hat. Siehe „[SADIAGDIR-Umgebungsvariable](#)“ auf Seite 473.

### ○ **Windows Mobile**

1. Das Verzeichnis der Programmdatei.
2. Das aktuelle Verzeichnis.
3. Das temporäre Verzeichnis. Siehe „[Registrierungseinstellungen unter Windows Mobile](#)“.

### ○ **Unix, Linux, OS X**

1. Das durch die SADIAGDIR-Umgebungsvariable angegebene Verzeichnis, falls diese gesetzt wurde.
2. Das Standard-Diagnoseverzeichnis: *\$HOME/.sqlanywhere16/diagnostics*.
3. Das aktuelle Verzeichnis.
4. Das temporäre Verzeichnis. Siehe SATMP-Umgebungsvariable sowie Umgebungsvariablen TMP, TMPDIR und TEMP.

#### **Hinweis**

Unter Unix ist das Schreiben von Crash-Berichten in das Stammverzeichnis des Benutzers nicht empfehlenswert, wenn die Datenbank oder der MobiLink-Server als Daemon ausgeführt wird oder wenn der Benutzer "root/nobody" ist.

**Namen von Fehlerberichtsdateien**    Namen von Fehlerberichtsdateien setzen sich aus folgenden Komponenten zusammen:

- Einem Präfix, das die Anwendung kennzeichnet:

Anwendungspräfix	Anwendung
DBCONSOLE	SQL Anywhere-Konsolendienstprogramm
ISQL	Interactive SQLDienstprogramm
LSN	Listener-Dienstprogramm
MLC	MobiLink-Client
MLS	MobiLink-Server
ML_MON	MobiLink-Profiler
SA	Personal oder Netzwerk-Datenbankserver
SCJ	Sybase Central
SR	SQL Remote

- Einem Wert, der die Softwareversion angibt
- Zwei mit Unterstrichen verbundenen Feldern, die den Zeitstempel für den Zeitpunkt darstellen, an dem der Bericht erstellt wurde
- Dem Anwendungsbezeichner
- Der Erweiterung *.dmp*

Beispiel: Die Datei *SA16\_20110620\_133828\_32116.dmp* ist ein Fehlerbericht eines SQL Anywhere-Datenbankservers der Version 16 vom 20.06.2011, 13:38:28 Uhr, aus Prozess 32116.

### Siehe auch

- [„SADIAGDIR-Umgebungsvariable“ auf Seite 473](#)

### Beispiel

1. Sie können das Standardverhalten von "dbsupport" mit der Option -cc ändern:
  - Der folgende Befehl konfiguriert dbsupport so, dass Fehlerberichte ohne Eingabeaufforderung an den Benutzer eingesendet werden:

```
dbsupport -cc autosubmit
```

- Der folgende Befehl konfiguriert dbsupport so, dass Berichte automatisch eingesendet werden und eine Benachrichtigung per E-Mail an *myemail@company.com* (über den E-Mail-Server *emailserver.company.com*) gesendet wird:

```
dbsupport -cc autosubmit -ce  
"myemail@company.com"; "emailserver.company.com:25"
```

- Der folgende Befehl deaktiviert die automatische Einsendung von Berichten:

```
dbsupport -cc no
```

2. Sie können mit der Option -lc eine Liste der Fehlerberichte anzeigen. Der folgende Befehl generiert eine Liste aller Crash-Berichte, die nicht eingesendet wurden:

```
dbsupport -lc
```

3. Sie können die Fehlerberichte mit der Option -sa, -sc oder -sd manuell einsenden. Der folgenden Befehl sendet alle Berichte, die im Diagnoseverzeichnis gespeichert sind:

```
dbsupport -sa
```

4. Sie können Kommentare und Dateien in den Fehlerbericht einbeziehen, indem Sie die Option -ac bzw. -af verwenden:

```
dbsupport -sc SA16_20080901_113308_3360 -ac "The message.txt file
provides more
information about this error report." -af c:\scenario.txt -af c:
\message.txt
```

## Transaktionslog-Dienstprogramm (dblog)

Verwaltet das Transaktionslog einer Datenbank

### Syntax

**dblog** [ *options* ] *database-file*

Option	Beschreibung
@data	Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.  Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.
-ek <i>key</i>	Gibt den Chiffrierschlüssel für stark verschlüsselte Datenbanken im Befehl an. Wenn Sie mit einer stark verschlüsselten Datenbank arbeiten, müssen Sie den Chiffrierschlüssel angeben, bevor Sie die Datenbank oder das Transaktionslog verwenden können. Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie bei einer stark verschlüsselten Datenbank nicht den richtigen Schlüssel angeben.
-ep	Gibt an, dass Sie zur Eingabe des Chiffrierschlüssel aufgefordert werden wollen. Diese Option öffnet ein Fenster, in das Sie den Chiffrierschlüssel eingeben. Diese zusätzliche Sicherheitsmaßnahme verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird. Bei stark verschlüsselten Datenbanken müssen Sie entweder -ek oder -ep, dürfen aber nicht beide angeben. Der Befehl schlägt fehl, wenn Sie bei einer stark verschlüsselten Datenbank nicht den richtigen Schlüssel angeben.

Option	Beschreibung
<b>-ir</b>	Setzt das SQL Remote-Log-Offset zurück, das für die delete_old_logs-Option verwaltet wird, sodass Transaktionslogs gelöscht werden können, wenn sie nicht mehr benötigt werden. Verwenden Sie diese Option, wenn Sie SQL Remote für diese Datenbank nicht mehr verwenden, aber weiterhin die MobiLink-Synchronisation benutzen.
<b>-is</b>	Setzt das MobiLink-Log-Offset zurück, das für die Option delete_old_logs verwaltet wird, sodass Transaktionslogs gelöscht werden können, wenn sie nicht mehr benötigt werden. Verwenden Sie diese Option, wenn Sie die MobiLink-Synchronisation für diese Datenbank nicht mehr verwenden, aber weiterhin SQL Remote benutzen.
<b>-m</b> <i>mirror-name</i>	Gibt den Dateinamen für eine neue Transaktionslog-Spiegeldatei an. Wenn die Datenbank gerade keinen Transaktionslogspiegel benutzt, verwendet sie ab jetzt einen. Wenn die Datenbank bereits einen Transaktionslogspiegel verwendet, wechselt sie nun zur neuen Datei als Transaktionslogspiegel.
<b>-n</b>	Beendet die Verwendung eines Transaktionslogs und einer Transaktionslog-Spiegeldatei. Ohne Transaktionslog kann die Datenbank nicht länger an einer Datenreplikation teilnehmen und das Transaktionslog nicht bei der Wiederherstellung von Daten verwenden. Wenn ein SQL Remote- oder dbmlsync-Kürzungs-Offset existiert, kann das Transaktionslog nur entfernt werden, wenn auch die entsprechende Ignorierungsoption (-ir für SQL Remote bzw. -is für dbmlsync) angegeben ist. Sie müssen das Transaktionslog weiterhin verwenden, wenn das Auditing für die Datenbank aktiviert ist (Sie können das Auditing deaktivieren).
<b>-o</b> <i>filename</i>	Schreibt Ausgabemeldungen in die benannte Datei.
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt.
<b>-r</b>	Beendet die Verwendung eines Transaktionslog-Spiegels und verwaltet nur noch eine einzelne Transaktionslogdatei.
<b>-t</b> <i>log-name</i>	Gibt den Dateinamen für ein neues Transaktionslog an. Wenn die Datenbank gerade kein Transaktionslog benutzt, verwendet sie ab jetzt eines. Wenn die Datenbank bereits ein Transaktionslog verwendet, benutzt sie ab jetzt die neue Datei als Transaktionslog.
<b>-x</b> <i>n</i>	Setzt den aktuellen relativen Offset des Transaktionslogs auf <i>n</i> zurück, sodass die Datenbank an der Replikation teilnehmen kann. Diese Option wird verwendet, um konsolidierte SQL Remote-Datenbanken neu zu laden.
<b>-z</b> <i>n</i>	Setzt den aktuellen Start-Offset des Transaktionslogs auf <i>n</i> zurück, sodass die Datenbank an der Replikation teilnehmen kann. Diese Option wird verwendet, um konsolidierte SQL Remote-Datenbanken neu zu laden.

**Privilegien**

Keine.

## Bemerkungen

Mit dem Dienstprogramm dblog können Sie den Namen des einer Datenbank zugeordneten Transaktionslogs oder Transaktionslogspiegels anzeigen oder ändern. Sie können eine Datenbank davon abhalten oder sie dazu auffordern, ein Transaktionslog oder einen Spiegel zu führen.

Ein Transaktionslogspiegel ist eine Kopie eines Transaktionslogs. Beide werden von einer Datenbank simultan geführt.

Der Name des Transaktionslogs wird zuerst gesetzt, wenn die Datenbank initialisiert wird. Das Transaktionslog-Dienstprogramm arbeitet mit Datenbankdateien. Der Datenbankserver muss nicht auf dieser Datenbank laufen, wenn der Dateiname des Transaktionslogs geändert wird (oder eine Fehlermeldung angezeigt wird).

Das Dienstprogramm zeigt folgende zusätzliche Informationen über das Transaktionslog an:

- Versionsnummer
- Der Name der Transaktionslogdatei
- Der Name der Transaktionslog-Spiegeldatei, falls vorhanden
- Der aktuelle relative Log-Offset

Sie können das Transaktionslog-Dienstprogramm folgendermaßen starten:

- In Sybase Central verwenden Sie den **Assistenten zum Ändern der Einstellungen für die Logdatei**.
- In Interactive SQL verwenden Sie die Anweisung `ALTER DATABASE Datenbankdatei ALTER LOG`.
- An einer Eingabeaufforderung benutzen Sie den Befehl `dblog`.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlschlag).

## Siehe auch

- „Konfigurationsdateien“ auf Seite 882
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „Extraktion von entfernten Datenbanken in eine Reload-Datei“ [[SQL Remote](#)]
- „Speicherorte von Transaktionslogs ändern (Sybase Central)“ auf Seite 136
- „Speicherorte von Transaktionslogs ändern (Befehlszeile)“ auf Seite 137
- „ALTER DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Exit-Codes der Softwarekomponenten“ [[SQL Anywhere Server - Programmierung](#)]

## Dienstprogramm zum Entladen (dbunload)

Entlädt eine Datenbank in eine SQL-Skriptdatei.

## Syntax

**dbunload** [ *options* ] [ *directory* ]

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariablen oder Konfigurationsdatei ein. Siehe „<a href="#">Konfigurationsdateien</a>“ auf Seite 882.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden. Siehe „<a href="#">Dienstprogramm zum Verschleiern von Dateien (dbfhide)</a>“ auf Seite 922.</p>
-ac "key-word=value; ..."	<p>Stellt eine Verbindung mit einer bestehenden Datenbank her und entlädt die Daten direkt in sie, wodurch der Vorgang einer Datenbankentladung und des Neuladens der Ergebnisse in eine bestehende Datenbank kombiniert wird. Diese Option wird unter Windows Mobile nicht unterstützt.</p> <p>Sie könnten beispielsweise eine neue Datenbank mit dem Dienstprogramm dbinit erstellen und sie dann mit dieser Option aktualisieren. Diese Methode ist nützlich, wenn Sie Initialisierungsoptionen ändern wollen.</p> <p>Der folgende Befehl (in einer Zeile eingegeben) lädt eine Kopie der Datenbank <i>c:\mydata.db</i> in eine bestehende Datenbankdatei namens <i>c:\mynewdata.db</i>:</p> <pre>dbunload -c "UID=DBA;PWD=sql;DBF=c:\mydata.db"          -ac "UID=DBA;PWD=sql;DBF=c:\mynewdata.db"</pre> <p>Wenn die neue Datenbank denselben Dateinamen wie die ursprüngliche Datenbank haben muss, verwenden Sie den DBN-Verbindungsparameter zur Angabe der richtigen Datenbanknamen. Siehe „<a href="#">Verbindungsparameter DatabaseName (DBN)</a>“ auf Seite 354.</p> <p>Der folgende Befehl (in einer Zeile eingegeben) lädt eine Kopie der alten Datenbank in eine neue Datenbank mit demselben Dateinamen <i>mydata.db</i>.</p> <pre>dbunload -c "UID=DBA;PWD=sql;DBN=old;DBF=c:\old_directory\mydata.db"          -ac "UID=DBA;PWD=sql;DBN=new;DBF=c:\new_directory\mydata.db"</pre> <p>Wenn die ursprüngliche Datenbank mit der Version 9 oder früher von SQL Anywhere erstellt wurde und die neue Datenbank noch nicht läuft, müssen Sie den Datenbankservernamen mit der Option -ac angeben. Zum Beispiel:</p> <pre>dbunload -c "UID=DBA;PWD=sql;DBF=c:\mydata.db"          -ac "UID=DBA;PWD=sql;DBF=c:\mynewdata.db;Server=newserver"</pre> <p>Wenn Sie diese Option verwenden, wird keine Zwischenkopie der Daten auf der Festplatte angelegt. Sie geben daher im Befehl kein Entladeverzeichnis an. Dies bietet größere Sicherheit für Ihre Daten.</p>

Option	Beschreibung
<b>-an data-base</b>	<p>Kombiniert die Vorgänge "Entladen einer Datenbank", "Erstellen einer neuen Datenbank" und "Laden der Daten" mit dieser Option. Diese Option wird unter Windows Mobile, oder wenn Sie Datenbanken der Version 9 oder früher unter Mac OS X für Intel neu aufbauen, nicht unterstützt.</p> <p>Die Optionen, die Sie bei der Erstellung der Quell-Datenbank angegeben haben, werden verwendet, um die neue Datenbank zu erstellen. Sie können aber die Initialisierungsoptionen ändern, indem Sie andere unterstützte dbunload-Optionen eingeben (wie -ap zum Ändern der Seitengröße oder -et zur Aktivierung der Tabellenverschlüsselung).</p> <p>Mit dem folgenden Befehl (in einer Zeile eingegeben) erstellen Sie beispielsweise eine neue Datenbankdatei namens <i>mydatacopy.db</i> und kopieren das Schema und die Daten von <i>mydata.db</i> hinein:</p> <pre>dbunload -c "UID=DBA;PWD=sql;DBF=c:\mydata.db" -an c:\mydatacopy.db</pre> <p>Wenn Sie diese Option verwenden, wird keine Zwischenkopie der Daten auf der Festplatte angelegt. Sie geben daher im Befehl kein Entladeverzeichnis an. Dies bietet größere Sicherheit für Ihre Daten.</p> <p>Beim Erstellen der neuen Datenbank wird an den DBSpace-Dateinamen ein "R" angehängt, um Dateinamenskonflikte zu vermeiden, wenn die DBSpace-Datei für die neue Datenbank in demselben Verzeichnis wie der DBSpace für die ursprüngliche Datenbank erstellt wird. Beispiel: Wenn eine entladene Datenbank einen DBSpace namens "library" in der Datei <i>library.db</i> hat, lautet der library-DBSpace für die neue Datenbank <i>library.dbR</i>.</p> <p>Die mit der Option -an angegebene Datei ist relativ zum Datenbankserver.</p>
<b>-ap size [ k ]</b>	<p>Legt die Seitengröße der neuen Datenbank fest. Diese Option wird ignoriert, wenn nicht auch die Option -an oder -ar verwendet wird. Die Seitengröße für eine Datenbank (in Byte) kann 2048, 4096, 8192, 16384 oder 32768 betragen, wobei der Standardwert die Seitengröße der ursprünglichen Datenbank ist. Verwenden Sie <b>k</b>, um die Einheit in KByte festzulegen (zum Beispiel, -ap 4k). Sie müssen mit dieser Option entweder die Option -an oder -ar angeben. Falls auf dem Datenbankserver bereits Datenbanken ausgeführt werden, muss die Seitengröße des Servers (festgelegt mit der Option -gp) groß genug für diese neue Seitengröße sein. Siehe „<a href="#">Datenbankserveroption -gp</a>“ auf Seite 249.</p>

Option	Beschreibung
<b>-ar</b> [ <i>directory</i> ]	<p>Erstellt eine neue Datenbank mit denselben Einstellungen wie bei der alten Datenbank, aktualisiert sie und ersetzt die alte Datenbank. Sie können aber die Initialisierungsoptionen ändern, indem Sie andere unterstützte dbunload-Optionen eingeben (wie -ap zum Ändern der Seitengröße oder -et zur Aktivierung der Tabellenverschlüsselung).</p> <p>Wenn Sie diese Option verwenden, darf es keine anderen Verbindungen zu der Datenbank geben und die Datenbankverbindung muss lokal (nicht über ein Netzwerk) aufgenommen werden. Diese Option wird unter Windows Mobile, oder wenn Sie Datenbanken der Version 9 oder früher unter Mac OS X für Intel neu aufbauen, nicht unterstützt.</p> <p>Wenn Sie <i>directory</i> angeben (optional), werden die Transaktionslog-Offsets für Replikationszwecke zurückgesetzt und das Transaktionslog aus der alten Datenbank wird in das angegebene Verzeichnis verschoben. Das benannte Verzeichnis muss das Verzeichnis sein, das die alten Transaktionslogs enthält, die vom Nachrichtenagenten verwendet werden. Die Transaktionslog-Verarbeitung findet nur statt, wenn die Datenbank in einer Replikation verwendet wird: Wenn es keinen SQL Remote-Publikationseigentümer gibt, wird das alte Transaktionslog nicht benötigt und daher gelöscht, anstatt in das angegebene Verzeichnis kopiert zu werden. Siehe „<a href="#">Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung</a>“ auf Seite 1068.</p> <p>Beim Erstellen der neuen Datenbank wird an den DBSpace-Dateinamen ein "R" angehängt, um Dateinamenskonflikte zu vermeiden, wenn die DBSpace-Datei für die neue Datenbank in demselben Verzeichnis wie der DBSpace für die ursprüngliche Datenbank erstellt wird. Beispiel: Wenn eine entladene Datenbank einen DBSpace namens "library" in der Datei <i>library.db</i> hat, lautet der library-DBSpace für die neue Datenbank <i>library.dbR</i>.</p> <p>Wenn Sie eine verschlüsselte Datenbank neu aufbauen, muss der Chiffrierschlüssel für die ursprüngliche und die neue Datenbank derselbe sein.</p> <p>Wenn Sie die -ar-Option verwenden, werden die Datenbankkürzungspunkt auf Null zurückgesetzt.</p>
<b>-c</b> "key-word=value; ..."	<p>Gibt die Verbindungsparameter für die Quelldatenbank an. Siehe „<a href="#">Verbindungsparameter</a>“ auf Seite 337.</p> <p>Die folgende Anweisung entlädt zum Beispiel die Beispieldatenbank und verbindet sich unter Verwendung der Benutzer-ID "DBA" und des Kennworts "sql": Die Daten werden in das Verzeichnis <i>c:\unload</i> entladen.</p> <pre>dbunload -c "DBF=%SQLANYSAMPLE%\demo.db;UID=DBA;PWD=sql" c:\unload</pre>

Option	Beschreibung
<b>-cm { sql   dbinit }</b>	<p>Zeigt die CREATE DATABASE-Anweisung oder den dbinit-Befehl im Meldungsfenster des Servers an, um eine Datenbank zu erstellen, die mit der entladenen Datenbank identisch ist. Wenn auch die Option -an angegeben wird, ist der angezeigte Befehl derjenige mit dem die neue Datenbank erstellt wird.</p> <ul style="list-style-type: none"> <li>• <b>sql</b> Zeigt die CREATE DATABASE-Anweisung an, die in die <i>reload.sql</i>-Datei geschrieben wird.</li> <li>• <b>dbinit</b> Zeigt den Befehl für das Dienstprogramm dbinit an.</li> </ul> <p>Wenn die Anweisung oder der Befehl für eine bestehende Datenbank mit starker Verschlüsselung (Option -an ist nicht angegeben) angezeigt wird, kann der Chiffrierschlüssel aus der Datenbank nicht bezogen werden und daher wird ein Fragezeichen (?) in der ENCRYPTED-Klausel oder der Option -ek angezeigt.</p> <p>Der Befehl oder die Anweisung zum Erstellen wird nicht angezeigt, wenn Sie eine Datenbank entladen, die mit einem Datenbankserver der Version 10 oder früher erstellt wurde.</p>
<b>-cp</b>	Komprimiert Tabellendaten-Ausgabedateien, indem das Schlüsselwort COMPRESSED an die ausgeführten UNLOAD TABLE-Anweisungen angehängt wird. Diese Option hat keine Wirkung, wenn sie mit der Option -an oder -ar angegeben wird.
<b>-d</b>	Generiert keine der Datenbankdefinitionsanweisungen (CREATE TABLE, CREATE INDEX usw.). Die Datei <i>reload.sql</i> enthält nur Anweisungen zum Aktualisieren der Daten.
<b>-dc</b>	<p>Erzwingt eine Neuberechnung aller berechneten Spalten in der Datenbank. Standardmäßig werden berechnete Spalten nicht neu berechnet. Wenn die Option -dc angegeben ist, wird dem Skript <i>reload.sql</i> ein neuer Abschnitt hinzugefügt, um berechnete Spalten neu zu berechnen. Es werden Anweisungen der folgenden Form hinzugefügt.</p> <pre>ALTER TABLE "owner"."table-name" ALTER "computed-column" SET COMPUTE (compute-expression);</pre> <p>Wenn Ihre Tabellen Kontext-abhängige berechnete Werte enthalten, wie z.B. CURRENT DATE, wird empfohlen, dass Sie die ALTER TABLE-Anweisung und nicht die Option -dc verwenden, um berechnete Spaltenwerte neu zu berechnen. Siehe „<a href="#">ALTER TABLE-Anweisung</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>

Option	Beschreibung
<b>-e</b> <i>table, ...</i>	<p>Schließt die angegebenen Tabellen aus der Datei <i>reload.sql</i> aus. Tabellennamen berücksichtigen nie die Groß- und Kleinschreibung, auch in Datenbanken, die die Groß- und Kleinschreibung berücksichtigen.</p> <p>Eine Datei <i>reload.sql</i>, die mit der Option -e erstellt wurde, darf nicht benutzt werden, um eine Datenbank neu zu erstellen, weil die Datei nicht alle Tabellen der Datenbank enthält. Wenn eine Tabelle sie referenzierende Fremdschlüssel hat, kann die Datenbank nicht ohne den Inhalt der Tabelle neu aufgebaut werden.</p> <p>Es wird empfohlen, dass Sie die Option -e mit der Option -d nur verwenden, um Daten aus allen Tabellen außer jenen durch -e festgelegten Tabellen zu entladen.</p>
<b>-ea algo-</b> <i>rithm</i>	<p>Gibt den Verschlüsselungsalgorithmus für die Datenbank- oder Tabellenverschlüsselung an (-et). Geben Sie <i>-ea simple</i> für die einfache Verschlüsselung an (nicht -ek oder -ep). Eine einfache Verschlüsselung ist gleichbedeutend mit der Verschleierung und dient nur dazu, die Daten bei einem zufälligen Direktzugriff auf die Datenbankdatei zu verbergen, wobei das Entschlüsseln der Daten in Ihrer Datenbank mithilfe eines Festplatten-Dienstprogramms erschwert wird.</p> <p>Um die Sicherheit zu erhöhen, geben Sie AES oder AES256 für starke 128-Bit- bzw. 256-Bit-Verschlüsselung an. Geben Sie AES_FIPS oder AES256_FIPS für FIPS-zertifizierte 128-Bit- bzw. 256-Bit-Verschlüsselung an. Bei starker Verschlüsselung müssen Sie auch die Option -ek oder -ep angeben. Weitere Hinweise zur starken Verschlüsselung finden Sie unter „<a href="#">Einfache Verschlüsselung und starke Verschlüsselung</a>“ auf Seite 1425.</p> <p>Um eine nicht verschlüsselte Datenbank zu erstellen, geben Sie <i>-ea none</i> an oder geben die Option -ea nicht an (und geben weder -e, -et, -ep noch -ek an).</p> <p>Wenn Sie die Option -ea nicht angeben, ist das Standardverhalten wie folgt:</p> <ul style="list-style-type: none"> <li>• -ea none, wenn -ek, -ep oder -et nicht angegeben ist</li> <li>• -ea AES, wenn -ek oder -ep angegeben ist (mit oder ohne -et)</li> <li>• -ea simple, wenn -et ohne -ek oder -ep verwendet wird</li> </ul> <p>Algorithmusnamen berücksichtigen die Groß- und Kleinschreibung nicht.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>Hinweis</b> Erforderliche getrennt lizenzierbare Komponenten.</p> <p>FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.</p> <p>Siehe „<a href="#">Getrennt lizenzierbare Komponenten</a>“ [<i>SQL Anywhere 16 - Einführung</i>].</p> </div>

Option	Beschreibung
<b>-ek</b> <i>key</i>	<p>Gibt einen Chiffrierschlüssel im dbunload-Befehl für die neu erstellte Datenbank an, wenn Sie eine Datenbank entladen und erneut laden (unter Verwendung der Option -an). Wenn Sie eine stark verschlüsselte Datenbank erstellen, müssen Sie den Chiffrierschlüssel liefern, um die Datenbank oder das Transaktionslog überhaupt verwenden zu können. Der für die Verschlüsselung verwendete Algorithmus ist der, den Sie mit der Option -ea angeben. Wenn Sie die Option -ek angeben, ohne -ea anzugeben, wird der AES-Algorithmus verwendet. Siehe „<a href="#">Einfache Verschlüsselung und starke Verschlüsselung</a>“ auf Seite 1425.</p> <p>Achten Sie auf Ihren Schlüssel. Speichern Sie eine Kopie Ihres Schlüssels an einem sicheren Ort. Ein verlorener Schlüssel führt zu einer nicht benutzbaren Datenbank, die sich nicht wiederherstellen lässt.</p>
<b>-ep</b>	<p>Fordert zur Angabe eines Chiffrierschlüssels für die neu erstellte Datenbank auf, wenn Sie Ihre Datenbank entladen und erneut unter Verwendung der Option -an laden. Diese zusätzliche Sicherheitsmaßnahme verhindert, dass der Chiffrierschlüssel in lesbarer Form angezeigt wird. Wenn Sie die Option -ep ohne -an angeben, wird die -ep ignoriert. Wenn Sie die Optionen -ep und -an angeben, müssen Sie den Chiffrierschlüssel zur Bestätigung der Eingabe ein zweites Mal eingeben. Wenn die Eingaben nicht übereinstimmen, schlägt das Entladen fehl. Siehe „<a href="#">Einfache Verschlüsselung und starke Verschlüsselung</a>“ auf Seite 1425.</p>
<b>-er</b>	<p>Entfernt die Verschlüsselung aus verschlüsselten Tabellen während eines Entladevorgangs.</p> <p>Beim Neuaufbau einer Datenbank mit aktivierter Tabellenverschlüsselung müssen Sie entweder -er oder -et angeben, um anzuzeigen, ob bei der neuen Datenbank die Tabellenverschlüsselung aktiviert ist. Sonst erhalten Sie einen Fehler, wenn Sie versuchen, Daten in die neue Datenbank zu laden.</p> <p>Der folgende Befehl entlädt eine Datenbank (<i>mydata.db</i>) mit verschlüsselten Tabellen in eine neue Datenbank (<i>mydatacopy.db</i>), bei der die Tabellenverschlüsselung nicht aktiviert ist, wobei die Verschlüsselung von verschlüsselten Tabellen entfernt wird:</p> <pre>dbunload -an c:\mydatacopy.db -er -c "UID=DBA;PWD=sql; DBF=c:\mydata.db; DBKEY=29bN8cj1z"</pre>

Option	Beschreibung
<b>-et</b>	<p>Aktiviert die Datenbanktabellen-Verschlüsselung in der neuen Datenbank (-an oder -ar muss auch angegeben sein). Wenn Sie die Option -et ohne die Option -ea angeben, wird der AES-Algorithmus verwendet. Wenn Sie die Option -et angeben, müssen Sie auch die Optionen -ep oder -ek angeben. Sie können die Tabellenverschlüsselungs-Einstellungen für die neue Datenbank ändern, sodass sie sich von den Einstellungen der entladenen Datenbank unterscheiden.</p> <p>Beim Neuaufbau einer Datenbank mit aktivierter Tabellenverschlüsselung müssen Sie entweder -er oder -et angeben, um anzuzeigen, ob bei der neuen Datenbank die Tabellenverschlüsselung aktiviert ist. Sonst erhalten Sie einen Fehler, wenn Sie versuchen, Daten in die neue Datenbank zu laden.</p> <p>Das folgende Beispiel entlädt eine Datenbank (<i>mydata.db</i>), die Tabellen hat, die mit dem Algorithmus für einfache Verschlüsselung chiffriert sind, in eine neue Datenbank (<i>mydatacopy.db</i>), bei der die Tabellenverschlüsselung aktiviert ist, und verwendet AES_FIPS-Verschlüsselung mit dem Schlüssel 34jh:</p> <pre>dbunload -an c:\mydatacopy.db -et -ea AES_FIPS         -ek 34jh         -c "UID=DBA;PWD=sql;DBF=c:\mydata.db"</pre>
<b>-g</b>	<ul style="list-style-type: none"> <li> <b>Materialisierte Ansichten</b> Standardmäßig werden als MANUAL REFRESH definierte materialisierte Ansichten nach einem Neuladen nicht initialisiert. Wenn Sie festlegen wollen, dass diese materialisierten Ansichten im Zuge des Neuladeverfahrens initialisiert werden, geben Sie die Option -g an. Wenn Sie -g angeben, ruft der Datenbankserver die sa_refresh_materialized_views-Systemprozedur auf. Siehe <a href="#">„sa_refresh_materialized_views-Systemprozedur“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a>. <p>Bei der Verwendung der Option -g sollten Sie bedenken, dass die Initialisierung aller materialisierten Ansichten dazu führen kann, dass der Neuladeprozess signifikant länger dauert. Andererseits bewirkt ein Weglassen der Option -g, dass die erste Abfrage, die eine nicht initialisierte Ansicht zu verwenden versucht, warten muss, während der Datenbankserver die Ansicht initialisiert, was zu einer unerwarteten Verzögerung führen kann. Wenn Sie die Option -g nicht verwenden, können Sie die materialisierten Ansichten auch manuell initialisieren, nachdem das Neuladen abgeschlossen ist. Siehe <a href="#">„Initialisieren einer materialisierten Ansicht“ [SQL Anywhere Server - SQL-Benutzerhandbuch]</a>.</p> </li> <li> <b>Textindizes</b> Standardmäßig werden als MANUAL REFRESH definierte Textindizes nach einem Neuladen nicht initialisiert. Wenn Sie definieren möchten, dass Textindizes im Zuge des Neuladeverfahrens initialisiert werden, geben Sie die Option -g an. Wenn Sie -g angeben, ruft der Datenbankserver die sa_refresh_text_indexes-Systemprozedur auf. Siehe <a href="#">„sa_refresh_text_indexes-Systemprozedur“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a>. </li> </ul>

Option	Beschreibung
<b>-ii</b>	Verwendet die UNLOAD-Anweisung, um Daten aus der Datenbank zu extrahieren, und die LOAD-Anweisung in der Datei <i>reload.sql</i> , um die Datenbank wieder mit Daten zu füllen. Dies ist die Standardeinstellung.
<b>-ix</b>	Verwendet die UNLOAD-Anweisung, um Daten aus der Datenbank zu extrahieren, und die INPUT-Anweisung von Interactive SQL in der Datei <i>reload.sql</i> , um die Datenbank wieder mit Daten zu füllen.
<b>-k</b>	Fügt Daten in die sa_diagnostic_auxiliary_catalog-Tabelle ein. Diese Tabelle ordnet Objekt-IDs für Tabellen, Benutzer, Prozeduren usw. aus der Quelldatenbank der Protokollierungsdatenbank zu. Es werden auch alle Histogramme entladen/neugeladen. Diese Option wird bei der Erstellung einer Protokollierungsdatenbank verwendet, d.h. eine Datenbank, die Diagnoseprotokollierungsinformationen erhält. Außerdem stellt diese Option sicher, dass Auditing in der Protokollierungsdatenbank deaktiviert ist, auch wenn das Auditing in der Produktionsdatenbank aktiviert ist. Die Tabelle sa_diagnostic_auxiliary_catalog ermöglicht es dem Server, Bedingungen zu simulieren, die vorherrschten, als Protokollierungsdaten aufgezeichnet wurden (z.B. für die Verwendung mit dem Indexberater oder bei einer Anwendungsprofilerstellung). Diese Option ist besonders zusammen mit der Option -n nützlich. Siehe „Diagnoseprotokollierung“ [ <a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a> ] und „sa_diagnostic_auxiliary_catalog-Tabelle“ [ <a href="#">SQL Anywhere Server - SQL-Referenzhandbuch</a> ].
<b>-kd</b>	Lädt die Datenbank erneut in eine einzige DBSpace-Datei. Mit dieser Option können Sie eine Protokollierungsdatenbank erstellen, wenn der Computer, auf dem die Datenbank erstellt wird, nicht dieselbe Verzeichnisstruktur wie die Produktionsdatenbank hat. Siehe „Erstellen einer externen Protokollierungsdatenbank (Sybase Central)“ [ <a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a> ].

Option	Beschreibung
<b>-l</b>	<p>Erzwingt, dass der aktuelle Wert von SYSTABCOL.max_identity bei einem Wiederaufbau der Datenbank erhalten bleibt.</p> <p>Standardmäßig gilt: Wenn eine Datenbank mit Tabellen, die AUTOINCREMENT-Spalten enthalten, neu aufgebaut wird, berechnet der Datenbankserver den nächsten verfügbaren Wert für jede AUTOINCREMENT-Spalte anhand des aktuellen Inhalts der Tabellen. In den meisten Fällen ist dies ausreichend. Wenn allerdings Zeilen am Ende des Wertebereichs gelöscht wurden, können Werte wieder verwendet werden, was nicht wünschenswert ist.</p> <p>Wenn Sie die Option -l angeben, werden für jede Tabelle, die einen AUTOINCREMENT-Wert enthält, Aufrufe der sa_reset_identity-Systemprozedur in das generierte Skript <i>reload.sql</i> eingefügt, sodass der aktuelle Wert von SYSTABCOL.max_identity erhalten bleibt.</p> <p>Siehe auch:</p> <ul style="list-style-type: none"> <li>• <a href="#">Neuladen von Tabellen mit AUTOINCREMENT-Spalten [SQL Anywhere 16 - Änderungen und Upgrades]</a></li> <li>• <a href="#">„SYSTABCOL-Systemansicht“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a></li> <li>• <a href="#">„sa_reset_identity-Systemprozedur“ [SQL Anywhere Server - SQL-Referenzhandbuch]</a></li> </ul>
<b>-m</b>	Behält keine Benutzer-IDs für Datenbanken bei, die in eine Replikation einbezogen sind.
<b>-n</b>	Entlädt keine Datenbankdaten. <i>reload.sql</i> enthält SQL-Anweisungen, die nur die Struktur der Datenbank aufbauen. Wenn die Datei <i>reload.sql</i> LOAD TABLE- oder INPUT-Anweisungen enthalten soll, verwenden Sie stattdessen die Option -nl.
<b>-nl</b>	Entlädt die Struktur (dasselbe Verhalten wie bei der Option -n), aber die resultierende Datei <i>reload.sql</i> umfasst auch LOAD TABLE- oder INPUT-Anweisungen für jede Tabelle. Wenn diese Option verwendet wird, werden keine Benutzerdaten entladen. Wenn Sie die Option -nl angeben, müssen Sie auch ein Datenverzeichnis aufnehmen, damit die LOAD/INPUT-Anweisungen generiert werden können, auch wenn keine Dateien in dieses Verzeichnis geschrieben werden. Mit dieser Option können Sie ein Entlade-Skript generieren, ohne dass Daten entladen werden. Sie können die Daten entladen, indem Sie die Option -d angeben. Wenn eine Datenbank eine Tabelle enthält, deren Daten nicht entladen werden sollen, kann das Entladen der Daten bei dieser Tabelle übersprungen werden, indem <code>dbunload -d -e table-name</code> verwendet wird.

Option	Beschreibung
<b>-no</b>	<p>Entlädt Datenbankobjekte nach Namen geordnet. Standardmäßig generiert dbunload Objekte in der Reihenfolge, in der sie erstellt wurden. Wenn Sie die -no-Option eingeben, können Sie Datenbankschemas vergleichen, wenn die Datenbanken dieselben Objekte enthalten, die aber zu unterschiedlichen Zeitpunkten erstellt wurden.</p> <p>Die Objektdefinitionen sind nach Objekttypen in alphabetischer Reihenfolge in der Datei <i>reload.sql</i> geordnet, wenn -no angegeben wird:</p> <ul style="list-style-type: none"> <li>• Benutzer</li> <li>• Gruppenmitgliedschaften</li> <li>• Tabellen</li> <li>• Indizes und Fremdschlüssel</li> <li>• Ansichten</li> <li>• Prozeduren</li> <li>• Funktionen</li> <li>• Trigger</li> <li>• Ereignisse</li> <li>• Webdienste</li> </ul> <p>Die Objektdefinitionen werden in der Reihenfolge Eigentümer,Name ausgegeben. Manchmal wird ein drittes Element, wie zum Beispiel einen Fremdschlüssel, Rollennamen oder Triggername, in die Reihenfolge aufgenommen.</p> <p>Die Option -no kann mit den Optionen -n, -nl, -ar, -an oder -ac nicht verwendet werden. Zur Vereinfachung von Vergleichen wird empfohlen, dass Sie die Option -no verwenden, wenn Sie die Reload-Skripten für Datenbanken vergleichen, die mit derselben Version des Datenbankservers erstellt wurden, da es bei den Objektdefinitionen kleinere Unterschiede geben kann.</p> <div style="border: 1px solid black; padding: 5px;"> <p><b>Vorsicht</b></p> <p>Die generierte Datei sollte nicht verwendet werden, um eine neue Datenbank zu erstellen, weil die Reihenfolge der Objekterstellung bedeutsam ist. Beispiel: Wenn die Prozedur "p2" die Prozedur "p1" aufruft und "p1" eine Ergebnismenge zurückgibt, kann es wichtig sein, "p1" vor "p2" zu definieren. Wenn versucht wird, eine mit der Option -no erstellte <i>reload.sql</i>-Skriptdatei auszuführen, wird ein Fehler gemeldet.</p> </div>
<b>-o filename</b>	Schreibt Ausgabemeldungen in die benannte Datei. Der Standort dieser Datei ist relativ zu dbunload.
<b>-p char</b>	Ersetzt bei externen Entladevorgängen (dbunload-Option -x) das Standard-Escapezeichen (\) durch ein anderes Zeichen. Diese Option ist nur verfügbar, wenn Sie dieses Dienstprogramm über eine Eingabeaufforderung ausführen.

Option	Beschreibung
<b>-q</b>	Läuft im stillen Modus - Meldungen werden nicht angezeigt. Diese Option ist nur verfügbar, wenn Sie dieses Dienstprogramm über eine Eingabeaufforderung ausführen. Wenn Sie die Option -q angeben, müssen Sie auch die Option -y angeben, sonst schlägt das Entladen fehl, wenn <i>reload.sql</i> bereits vorhanden ist.
<b>-qc</b>	Schließt das Meldungsfenster, wenn der Entladevorgang abgeschlossen ist. Standardmäßig bleibt das dbunload-Meldungsfenster geöffnet, bis es von einem Benutzer geschlossen wird. Diese Option ist nur unter Windows Mobile verfügbar.
<b>-qr</b>	Unterdrückt die Erstellung und Anzeige von Fortschrittsmeldungen beim Laden von Tabellen und Erstellen von Indizes.
<b>-r reload-file</b>	Ändert den Namen und das Verzeichnis der generierten Reload-SQL-Skriptdatei. Standardwert ist <i>reload.sql</i> im aktuellen Verzeichnis. Das Verzeichnis ist relativ zum aktuellen Verzeichnis der Clientanwendung und nicht des Servers.
<b>-ss</b>	Unterdrückt die Ausgabe von Spaltenstatistiken in die Reload-SQL-Skriptdatei.
<b>-t table,...</b>	<p>Gibt eine Liste von Tabellen zum Entladen an. Standardmäßig werden alle Tabellen entladen. Zusammen mit der Option -n haben Sie die Möglichkeit, nur eine Gruppe von Tabellendefinitionen zu entladen. Tabellennamen berücksichtigen nie die Groß- und Kleinschreibung, auch in Datenbanken, die die Groß- und Kleinschreibung berücksichtigen.</p> <p>Eine Datei <i>reload.sql</i>, die mit der Option -t erstellt wurde, darf nicht benutzt werden, um eine Datenbank neu zu erstellen, weil die Datei nicht alle Tabellen der Datenbank enthält. Wenn eine Tabelle sie referenzierende Fremdschlüssel hat, kann die Datenbank nicht ohne den Inhalt der Tabelle neu aufgebaut werden.</p> <p>Es wird empfohlen, dass Sie die Option -t mit der Option -d nur verwenden, um Daten aus den durch "-t" festgelegten Tabellen zu entladen.</p>
<b>-u</b>	Verhindert die Verwendung eines Indexes zur Sortierung von Daten. Verwenden Sie diese Option, wenn Sie eine Datenbank mit einem beschädigten Index entladen, damit der beschädigte Index nicht zum Sortieren der Daten verwendet wird. Normalerweise werden Daten in jeder Tabelle anhand des Primärschlüssels oder Clustered-Indexes sortiert, falls er für die Tabelle definiert ist.
<b>-v</b>	Zeigt den Namen der Tabelle an, die entladen wird, sowie die Anzahl der entladenen Zeilen. Diese Option ist nur verfügbar, wenn Sie dbunload über eine Eingabeaufforderung ausführen.
<b>-xi</b>	Führt ein externes Entladen durch, indem Daten in den dbunload-Client entladen werden, und verwendet anschließend die LOAD-Anweisung in der generierten Reload-Skriptdatei <i>reload.sql</i> , um die Datenbank wieder mit Daten zu füllen.

Option	Beschreibung
<b>-xx</b>	Führt ein externes Entladen durch, indem Daten in den dbunload-Client entladen werden, und verwendet anschließend die Interactive SQL-Anweisung INPUT in der generierten Reload-SQL-Skriptdatei <i>reload.sql</i> , um die Datenbank wieder mit Daten zu füllen.
<b>-y</b>	Ersetzt vorhandene Skriptdateien, ohne zur Bestätigung aufzufordern. Wenn Sie die Option -q angeben, müssen Sie auch -y angeben. Andernfalls schlägt das Entladen fehl, wenn dbunload erkennt, dass bereits eine Skriptdatei vorhanden ist.  Beim Entladen von Datenbanken, die in ein Replikationssystem eingebunden sind, gibt es besondere Punkte zu beachten. Siehe „ <a href="#">Extraktion von entfernten Datenbanken</a> “ [ <a href="#">SQL Remote</a> ] und „ <a href="#">SQL Remote-Upgrades</a> “ [ <a href="#">SQL Anywhere 16 - Änderungen und Upgrades</a> ].
<i>directory</i>	Gibt das Verzeichnis an, in dem die entladenen Daten gespeichert werden sollen. Die Skriptdatei <i>reload.sql</i> ist immer relativ zum aktuellen Verzeichnis des Benutzers.

## Privilegien

Für einen Entladevorgang ohne Neuladen müssen Sie das SELECT ANY TABLE-Systemprivileg haben.

Für einen Entladevorgang ohne Neuladen müssen Sie die Systemprivilegien SELECT ANY TABLE und SERVER OPERATOR haben.

## Bemerkungen

### Hinweis

Stellen Sie sicher, dass keine aktiven Transaktionen (einschließlich DDL) in der Datenbank laufen, wenn Sie das Dienstprogramm dbunload ausführen.

### Hinweis

Hinweise zum Neuaufbau einer bestehenden Datenbank in einer Datenbank der Version 16 finden Sie unter „[SQL Anywhere-Server-Upgrades](#)“ [[SQL Anywhere 16 - Änderungen und Upgrades](#)].

Wenn Sie dbunload mit einer Datenbank der Version 10.0.0 oder höher verwenden, muss die Version von dbunload mit der Version des Datenbankservers übereinstimmen, der für den Zugriff auf die Datenbank verwendet wird. Wenn eine ältere Version von dbunload mit einem neueren Datenbankserver verwendet wird oder umgekehrt, wird ein Fehler gemeldet.

Mit dem Dienstprogramm zum Entladen können Sie eine Datenbank entladen und eine Gruppe von Datendateien in ein genanntes Verzeichnis legen. Das Dienstprogramm Entladen erstellt eine Interactive SQL-Skriptdatei für den Neuaufbau Ihrer Datenbank. Es entlädt ebenfalls alle Daten aus Ihren Tabellen in Dateien im angegebenen Verzeichnis in einem Format mit Kommas als Trennzeichen. Binärdaten werden korrekt durch Escape-Sequenzen repräsentiert.

Ein interner Entlade-/Ladevorgang entlädt Informationen über den aktuellen Status jedes Benutzers durch das Ausführen von UPDATE ISYSUSER-Anweisungen. Externes Entladen/Laden enthält diese Informationen nicht und der Status aller Benutzer wird zurückgesetzt. Siehe „[Login-Richtlinien](#)“ auf Seite 535.

Wenn Sie eine Datenbank durch Entladen und Neuladen neu aufsetzen, wird die neue Datenbank möglicherweise kleiner sein als die ursprüngliche. Dies kann auf Indexänderungen in SQL Anywhere zurückzuführen sein und weist nicht auf ein Problem oder einen Datenverlust hin.

Wenn Sie den Neuaufbau einer Datenbank der Version 11 oder früher mit dem Dienstprogramm zum Entladen (dbunload) durchführen, sind für die neue Datenbank globale Prüfsummen standardmäßig aktiviert, auch wenn für die ursprüngliche Datenbank Prüfsummen deaktiviert waren. Wenngleich dies nicht empfohlen wird, können Sie globale Prüfsummen für eine Datenbank mit der ALTER DATABASE-Anweisung deaktivieren. Siehe „[ALTER DATABASE-Anweisung](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)] und „[Erkennung von Beschädigungen mithilfe von Prüfsummen](#)“ auf Seite 1084.

**Hinweis**

Datenbanken bis zur Version 9, für die eine Wiederherstellung erforderlich ist, können ab Version 10 des Dienstprogramms zum Entladen (dbunload) nicht neu geladen werden. Sie müssen die Datenbank mit dbunload Version 9 oder früher neu laden.

Mit dem Dienstprogramm zum Entladen können Sie außerdem eine neue Datenbank direkt aus einer bestehenden erstellen. Dies vermeidet mögliche Sicherheitsprobleme, wenn der Inhalt der Datenbank in eine gewöhnliche Datei geschrieben wird.

Wenn Sie nur Tabellendaten entladen wollen, können Sie das in einem Schritt durchführen, indem Sie das Fenster **Daten entladen** in Sybase Central verwenden.

Weitere Hinweise finden Sie unter „[Exportieren von Daten mit dem Fenster Daten entladen](#)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].

Beim Entladen von Datenbanken, die in ein Replikationssystem eingebunden sind, gibt es besondere Punkte zu beachten. Siehe „[Extraktion von entfernten Datenbanken](#)“ [[SQL Remote](#)].

Sie können das Dienstprogramm zum Entladen folgendermaßen starten:

- In Sybase Central verwenden Sie den **Assistenten zum Entladen einer Datenbank**. Siehe „[Tipps zum Exportieren von Daten mit dem Assistenten zum Entladen einer Datenbank](#)“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)].
- An der Eingabeaufforderung benutzen Sie den Befehl dbunload. Das ist zum Integrieren in Batch- oder Befehlsdateien nützlich.

Die Option -gl des Datenbanksservers steuert die Berechtigungen, die zum Entladen von Daten aus der Datenbank erforderlich sind. Siehe „[Datenbankserveroption -gl](#)“ auf Seite 242.

Der Benutzer-ID "dbo" gehören eine Reihe von Systemobjekten in einer Datenbank, wie Ansichten und gespeicherte Prozeduren.

Das Dienstprogramm zum Entladen entlädt die für die Benutzer-ID "dbo" während der Erstellung der Datenbank erzeugten Objekte nicht. Änderungen an diesen Objekten, wie das Neudefinieren einer Systemprozedur, gehen beim Entladen der Datenbank verloren. Alle Objekte, die von der Benutzer-ID "dbo" seit der Initialisierung der Datenbank erstellt wurden, werden vom Dienstprogramm zum Entladen entladen und diese Objekte bleiben so erhalten.

Wenn Sie eine Datenbank entladen, werden Änderungen bei Berechtigungen für Systemobjekte nicht entladen. Sie müssen diese Berechtigungen in der neuen Datenbank erneut erteilen bzw. entziehen.

### **Tipp**

Bevor Sie Ihre Datenbank neu aufbauen, wird empfohlen, dass Sie den Neuladeprozess validieren, indem Sie die Datenbank ohne Daten mit einem Befehl der folgenden Art neu laden:

```
dbunload -n -an new.db -c "UID=your-user-id;PWD=your-password;DBF=original-  
database-file"
```

Beheben Sie die erkannten Probleme in der ursprünglichen Datenbank, bevor Sie sie neu aufbauen.

Im Standardmodus bzw. wenn -ii bzw. -ix verwendet wird, ist das von dbunload für die Daten verwendete Verzeichnis relativ zum Datenbankserver und nicht zum aktuellen Verzeichnis des Benutzers.

Wenn -xi oder -xx verwendet wird, ist das Verzeichnis relativ zum aktuellen Verzeichnis des Benutzers.

Weitere Hinweise zum Angeben eines Dateinames und Suchpfads in diesem Modus finden Sie unter „UNLOAD-Anweisung“ [\[SQL Anywhere Server - SQL-Referenzhandbuch\]](#).

Wenn keine Tabellenliste angegeben ist, wird die gesamte Datenbank entladen. Wenn eine Tabellenliste angegeben wird, werden nur diese Tabellen entladen.

Entladene Daten enthalten die Spaltenliste für die LOAD TABLE-Anweisungen, die in der Datei *reload.sql* generiert wurden. Das Entladen der Spaltenliste erleichtert die Neuordnung der Spalten in einer Tabelle. Tabellen können gelöscht oder neu erstellt und die Daten anschließend mit *reload.sql* übernommen werden.

Die von dbunload generierten LOAD TABLE-Anweisungen deaktivieren Prüf-Integritätsregeln und berechnete Spalten.

BeendigungsCodes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag). Siehe „Exit-Codes der Softwarekomponenten“ [\[SQL Anywhere Server - Programmierung\]](#).

### **Hinweis**

Es wird empfohlen, dass Sie materialisierte Ansichten in Ihrer Datenbank aktualisieren, nachdem die Datenbank neu aufgebaut wurde. Siehe „Materialisierten Ansichten manuell aktualisieren“ [\[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).

### **Hinweis**

Protokollierungsdaten werden nicht als Teil eines Vorgangs zur Datenbank-Entladung oder -Aktualisierung entladen. Wenn Sie Protokollierungsinformationen aus einer Datenbank in eine andere übertragen möchten, müssen Sie dies manuell tun, indem Sie den Inhalt der sa\_diagnostic\_\*-Tabellen kopieren. Dies wird jedoch nicht empfohlen.

## **Vergleich von externem Entladen und Neuladen**

Die folgenden Optionen bieten Kombinationen von internem und externem Entladen und Neuladen: -ii, -ix, -xi und -xx. Sie können eine deutliche Performancesteigerung erzielen, indem Sie interne

Anweisungen (UNLOAD/LOAD) statt externe Anweisungen (INPUT- und OUTPUT-Anweisungen von Interactive SQL) verwenden. Interne Anweisungen werden jedoch vom Server ausgeführt, sodass Datei- und Verzeichnispfade relativ zum Speicherort des Datenbankservers sind. Wenn externe Befehle verwendet werden, sind Datei- und Verzeichnispfade relativ zum aktuellen Verzeichnis des Benutzers.

In Sybase Central können Sie angeben, ob Sie relativ zum Server oder zum Client entladen wollen. Siehe „UNLOAD-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Wenn Sie das externe Entladen und Neuladen verwenden, um eine Datenbank zu entladen, neu zu laden oder neu aufzubauen, und der Zeichensatz der Datenbank inkompatibel mit dem Zeichensatz auf dem Hostsystem ist, auf dem dbunload ausgeführt wird, führt die Zeichensatzkonvertierung möglicherweise zu einer Beschädigung der Daten, da sie zwischen dem Datenbank-Zeichensatz und dem Zeichensatz des Hostsystems konvertiert werden.

Um dieses Problem zu vermeiden, geben Sie den Datenbank-Zeichensatz in der Verbindungszeichenfolge für die Datenbank (Optionen -c und -ac) an. Wenn der Datenbank-Zeichensatz beispielsweise UTF-8 ist, nehmen Sie "charset=utf-8" in die Verbindungszeichenfolgen auf:

```
dbunload -c UID=user-ID;PWD=password;  
CHARSET=utf-8;DBF=filename -ac UID=user-ID;  
PWD=password;CHARSET=utf-8;Host=host-name -xx
```

Wenn Sie ein externes Entladen durchführen, enthält der Beginn der Datei *reload.sql* eine auskommentierte CREATE DATABASE-Anweisung. Diese Anweisung kann verwendet werden, um eine Datenbank zu erstellen, die mit der entladenen Datenbank übereinstimmt.

Wenn die entladene Datenbank mit Version 9 oder einer früheren Version von SQL Anywhere erstellt wurde und eine benutzerdefinierte Kollation hatte, wird die COLLATION-Klausel wie folgt angezeigt:

```
COLLATION collation-label DEFINITION collation-definition
```

Dabei gilt: *Kollationsdefinition* ist eine Zeichenfolge, die die benutzerdefinierte Kollation angibt.

Die einzige Möglichkeit, eine benutzerdefinierte Kollation beizubehalten, besteht in einem Neuaufbau der Datenbank in einem einzigen Schritt (internes Entladen). Wenn Sie wählen, die Datenbank zu entladen und dann das Schema und die Daten in eine erstellte Datenbank zu laden, müssen Sie eine der unterstützten Kollationen verwenden.

Wenn die entladene Datenbank mit starker Verschlüsselung erstellt wurde, wird der Wert des KEY-Schlüssels in der CREATE DATABASE-Anweisung in Form von drei Fragezeichen (???) angezeigt.

## Fehlgeschlagene Entladevorgänge

Wenn ein Fehler während eines internen Neuaufbaus einer Datenbank unter Verwendung der Option -ar oder -an auftritt, nachdem die Tabellendaten neu geladen und etwaige Indizes auf der Tabelle neu aufgebaut wurden, erstellt dbunload eine Datei namens *unprocessed.sql* im aktuellen Verzeichnis. Diese Datei enthält alle Anweisungen, die aufgrund des Fehlers nicht ausgeführt wurden, sowie die Anweisung, die den Fehler verursachte, als Kommentar. Das Folgende ist ein Beispiel für die Datei *unprocessed.sql*:

```
-- The database reload failed with the following error:  
-- ***** SQL error: the-SQL-error  
-- This script contains the statements that were not executed as a  
-- result of the failure. The statement that caused the failure is
```

```
-- commented out below. To complete the reload, correct the failing
-- statement, remove the surrounding comments and execute this script.
/*
the failing statement
go

*/

setuser "DBA"
go

... the remainder of the statements to be processed
```

In dieser Datei können Sie die fehlerhaften Anweisungen korrigieren, entfernen oder verändern. Die Datei *unprocessed.sql* wird nur erstellt, nachdem alle Tabellendaten und referenziellen Integritätsregeln neu geladen wurden. Über Interactive SQL können Sie sich mit der neuen Datenbank verbinden und die aktualisierte Datei *unprocessed.sql* ausführen. Damit können Sie den Neuaufbau der Datenbank abschließen, ohne den Neuaufbau mehrfach durchführen zu müssen. Damit sparen Sie möglicherweise viel Zeit.

Wenn die Datei *unprocessed.sql* generiert wird, stoppt dbunload und gibt einen Fehlercode aus, um andere Tools und Skripten vom fehlgeschlagenen Neuaufbau zu verständigen.

Wenn während eines internen Neuaufbaus einer Datenbank mit der Option *-ar* ein Fehler auftritt, haben die neue Datenbank und die Transaktionslogdatei die Dateierweiterungen *.dbr* bzw. *.logr*. Führen Sie die folgenden Schritte durch, um die Datei *unprocessed.sql* zu übernehmen und den Neuladevorgang manuell zu beenden:

1. Starten Sie die neue Datenbank.
2. Übernehmen Sie die aktualisierte Datei *unprocessed.sql*.
3. Fahren Sie die Datenbank herunter.
4. Verschieben Sie die Dateien *original-name.db* und *original-name.log* in ein neues Verzeichnis.
5. Benennen Sie die Dateien *original-name.dbr* und *original-name.logr* in *original-name.db* bzw. *original-name.log* um.
6. Führen Sie den folgenden Befehl aus:

```
dblog -t original-name.log original-name.db
```

### Verschlüsselte Datenbanken

Beim Neuaufbau einer Datenbank mit aktivierter Tabellenverschlüsselung müssen Sie entweder *-er* oder *-et* angeben, um anzuzeigen, ob bei der neuen Datenbank die Tabellenverschlüsselung aktiviert ist. Andernfalls erhalten Sie einen Fehler, wenn Sie versuchen, Daten in die neue Datenbank zu laden.

Wenn Sie eine stark verschlüsselte Datenbank entladen möchten, müssen Sie den Chiffrierschlüssel angeben. Sie können den DatabaseKey-Verbindungsparameter (DBKEY) verwenden, um den Schlüssel im Befehl anzugeben. Wenn Sie zur Eingabe des Chiffrierschlüssels aufgefordert werden möchten, statt ihn offen in die Befehlszeile eingeben zu müssen, können Sie die Serveroption *-ep* folgendermaßen verwenden:

```
dbunload -c "DBF=myenc.db;START=dbeng16 -ep"
```

Wenn Sie die Option -an zum Entladen der Datenbank und Neuladen in eine andere Datenbank verwenden und den Chiffrierschlüssel für die neue Datenbank mit den Optionen -ek oder -ep angeben wollen, beachten Sie Folgendes:

- Wenn die ursprüngliche Datenbank stark verschlüsselt ist, müssen Sie den Schlüssel für die ursprüngliche Datenbank mit dem Verbindungsparameter DatabaseKey (DBKEY) in der Option -c angeben, und nicht mit der Option -ek oder -ep.
- Mit den Optionen -ek und -ep ist es möglich, eine nicht verschlüsselte Datenbank zu entladen und sie wieder in eine neue, stark verschlüsselte Datenbank zu laden. Wenn Sie die Optionen -ep und -an verwenden, müssen Sie den Schlüssel korrekt bestätigen, damit das Entladen nicht fehlschlägt.
- Wenn die ursprüngliche Datenbank stark verschlüsselt ist, aber die Optionen -ek und -ep nicht verwendet werden, wird die neue Datenbank mit einfacher Verschlüsselung verschlüsselt.
- Die Optionen -ek und -ep werden ignoriert, wenn -an nicht angegeben wird. Die dbunload-Optionen -ek und -ep gelten bei einer neuen Datenbank, während die Optionen der Datenbankserver (dbeng16/dbsrv16) und DBKEY= bei bestehenden Datenbanken gelten.
- Wenn Sie an Replikations- oder Synchronisationssystemen beteiligte Datenbanken neu aufbauen, nimmt dbunload an, dass der mit der Option -ek oder -ep angegebene Chiffrierschlüssel der Chiffrierschlüssel der ursprünglichen Datenbank wie auch der Chiffrierschlüssel der neu aufgebauten Datenbank ist.

Weitere Hinweise zur Verschlüsselung finden Sie unter „Datenbankserveroption -ep“ auf Seite 233 und „Verbindungsparameter DatabaseKey (DBKEY)“ auf Seite 353.

### Eine Datenbank neu aufbauen

Führen Sie zum Entladen einer Datenbank dbunload aus, indem Sie einen DBA-Benutzer und ein DBA-Kennwort angeben und die Datenbank mit dem Verbindungsparameter "DBF=" referenzieren.

Um eine Datenbank neu zu laden, erstellen Sie eine neue Datenbank und führen dann die generierte Skriptdatei *reload.sql* über Interactive SQL aus.

Um die Entlade- und Neulade-Schritte zu kombinieren, befolgen Sie die obenstehenden Anleitungen und fügen die Option -an hinzu, um den Namen der neuen Datenbank anzugeben. Siehe die Beschreibung der Optionen -ac und -an.

## Dienstprogramm zum Upgrade (dbupgrad)

### Hinweis

Es ist nicht möglich, mit dem Dienstprogramm zum Upgrade (dbupgrad) Datenbanken der Version SQL Anywhere 9.0.2 und früher auf SQL Anywhere 16 umzustellen. Um Datenbanken der Version SQL Anywhere 9.0.2 und früher auf SQL Anywhere 16 umzustellen, müssen Sie die Datenbank neu aufbauen, indem Sie sie entladen und neu laden. Siehe „SQL Anywhere-Server-Ugrades“ [*SQL Anywhere 16 - Änderungen und Upgrades*].

Aktualisiert die Systemtabellen und -ansichten, fügt neue Datenbankoptionen hinzu, erstellt alle gespeicherten Systemprozeduren neu, installiert die jConnect-Unterstützung, ändert die Java-Unterstützung in der Datenbank, archiviert das Transaktionslog und erstellt ein neues Transaktionslog. Außerdem stoppt dieses Dienstprogramm die Datenbank und startet sie neu.

## Syntax

**dbupgrad** [ *options* ]

Option	Beschreibung
<i>@data</i>	<p>Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.</p>
<b>-c</b> " <i>key-word=value; ...</i> "	<p>Legt Verbindungsparameter fest.</p> <p>Der folgende Befehl führt ein Upgrade einer Datenbank namens "sample16" durch, ohne jConnect-Unterstützung zu installieren, wobei er sich als Benutzer "DBA" mit dem Kennwort "sql" verbindet:</p> <pre>dbupgrad -c "UID=DBA;PWD=sql;DBF=c:\sa16\sample16.db" -i</pre>
<b>-i</b>	<p>Schließt jConnect-Metadaten-Unterstützung aus. Wenn Sie den jConnect-JDBC-Treiber verwenden möchten, um auf Systemkataloginformationen zuzugreifen, dürfen Sie diese Option nicht verwenden. Sie können JDBC weiterhin verwenden, auch wenn diese Option angegeben wird, solange Sie nicht auf Systemkataloginformationen zugreifen. Sie können die jConnect-Metadatenunterstützung zu einem späteren Zeitpunkt mit Sybase Central oder der ALTER DATABASE UPGRADE-Anweisung hinzufügen.</p>
<b>-nrs</b>	<p>Stoppt die Datenbank nach dem Upgrade, startet sie aber nicht neu. Wenn diese Option nicht angegeben ist, wird die Datenbank nach dem Upgrade neu gestartet, es sei denn, der AutoStop-Verbindungsparameter ist auf "Yes" gesetzt.</p>
<b>-o</b> <i>filename</i>	<p>Schreibt Ausgabemeldungen in die angegebene Datei.</p>

Option	Beschreibung
<b>-pd [ Y   N ]</b>	<p>Legt fest, ob Systemprozeduren vor Version 16.0, die mit Privilegien verbundene Vorgänge durchführen, mit den Privilegien des Definierers (Eigentümers) ausgeführt werden oder mit denjenigen des Aufrufers. Eine Liste dieser Prozeduren finden Sie unter „Systemprozeduren vor Version 16.0 als Aufrufer oder Definierer ausführen“ [<a href="#">SQL Anywhere Server - SQL-Benutzerhandbuch</a>].</p> <p>Wenn -pd N angegeben wird, werden die Systemprozeduren mit den Privilegien des Aufrufers ausgeführt (des Benutzers, der die Systemprozedur ausführt).</p> <p>Wenn -pd Y angegeben wird, werden die Systemprozeduren mit den Privilegien des Definierers ausgeführt (des Benutzers oder der Rolle, der bzw. die Eigentümer der Systemprozedur ist).</p> <p>Wenn keine Angabe gemacht wurde, wird die aktuelle Einstellung für die Datenbank beibehalten, für die das Upgrade durchgeführt wird. Beim Upgrade einer Datenbank vor Version 16.0 bedeutet dies, dass diese Systemprozeduren mit den Privilegien des Definierers ausgeführt werden.</p> <p>Diese Einstellung wirkt sich nicht auf Systemprozeduren aus, die in Version 16.0 oder später hinzugefügt wurden, und auch nicht auf das Standardverhalten für benutzerdefinierte Prozeduren, die sich weiterhin nach dem Definierer richten.</p>
<b>-q</b>	Läuft im stillen Modus - es werden keine Meldungen oder Fenster angezeigt.

### Privilegien

Sie müssen das ALTER DATABASE-Systemprivileg haben und als einziger Benutzer mit der Datenbank verbunden sein.

### Bemerkungen

#### Vorsicht

Sichern Sie Ihre Datenbankdateien vor dem Upgrade.

Das Dienstprogramm dbupgrad führt ein Upgrade einer Datenbank durch, die mit früheren Versionen der Software erstellt wurde, damit Funktionen der aktuellen Version der Software aktiviert werden. Die früheste Version, bei der ein Upgrade möglich ist, ist SQL Anywhere 10.0.0. Während spätere Versionen des Datenbankservers zwar mit Datenbanken laufen können, die mit früheren Softwareversionen erstellt wurden, sind einige Funktionen der neueren Version nicht verfügbar, wenn die Datenbank nicht aktualisiert wird.

Eine Fehlermeldung wird zurückgegeben, wenn Sie das Dienstprogramm zum Upgrade verwenden, um ein Upgrade einer Datenbank vorzunehmen, die gespiegelt wird.

#### Hinweis

Aktualisieren Sie die materialisierten Ansichten in der Datenbank, nachdem ein Upgrade der Datenbank durchgeführt wurde.

**Hinweis**

Funktionen, die eine physische Reorganisation der Datenbankdatei erfordern, werden von dbupgrad nicht zur Verfügung gestellt. Solche Funktionen sind Index-Verbesserungen und Änderungen in der Datenspeicherung. Damit Sie diese Verbesserungen nützen können, müssen Sie Ihre Datenbank entladen und neu laden.

Wenn neue Versionen und Software-Updates in SQL Anywhere verfügbar sind, können Sie das Dienstprogramm zum Upgrade verwenden, um die Nutzung der neuen Funktionen zu ermöglichen.

Für das Upgrade ist es nicht erforderlich, die Datenbank zu entladen und neu zu laden.

Während des Upgrades wird das Transaktionslog archiviert. Ein neues Transaktionslog wird erstellt, wenn die Datenbank nach dem Upgrade gestartet wird.

Beendigungscode sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehlslag).

**Siehe auch**

- „Prozeduren und Funktionen zum Ausführen mit Eigentümer- oder Aufruferprivilegien einrichten“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Konfigurationsdateien“ auf Seite 882
- „Verbindungsparameter“ auf Seite 337
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „jConnect-Systemobjekte in einer Datenbank installieren“ [*SQL Anywhere Server - Programmierung*]
- „ALTER DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]
- „Sicherung und Datenwiederherstellung“ auf Seite 1027
- „Materialisierten Ansichten manuell aktualisieren“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „SQL Anywhere-Server-Ugrades“ [*SQL Anywhere 16 - Änderungen und Upgrades*]
- „Upgrade und Neuaufbau in einem Datenbankspiegelungssystem“ [*SQL Anywhere 16 - Änderungen und Upgrades*]

## Validierungs-Dienstprogramm (dbvalid)

Validiert die Indizes und Schlüssel in einigen oder allen Tabellen bzw. materialisierten Ansichten in einer Datenbank.

**Syntax**

**dbvalid** [ *options* ] [ *object-name*, ... ]

Option	Beschreibung
@data	<p>Liest Optionen aus der angegebenen Umgebungsvariable oder Konfigurationsdatei ein.</p> <p>Wenn Sie Kennwörter oder andere Informationen in der Konfigurationsdatei schützen möchten, können Sie das Dienstprogramm zum Verschleiern von Dateien auf die Konfigurationsdatei anwenden.</p>
-c "keyword=value; ..."	<p>Gibt Datenbank-Verbindungsparameter an.</p> <p>Der folgende Befehl validiert die Datenbank einschließlich aller Tabellen und materialisierten Ansichten für c:\salesdata.db, wobei sich ein Benutzer namens DBA mit dem Kennwort sql verbindet:</p> <pre>dbvalid -c "UID=DBA;PWD=sql;DBF=c:\salesdata.db"</pre>
-d	<p>Prüft, ob alle Seiten in der Datenbank dem richtigen Objekt gehören, und führt eine Prüfsummenvalidierung durch. Die Option -d validiert die Korrektheit von Indizes. Die Option -d kann nicht mit den Optionen -i, -s oder -t verwendet werden.</p>
-fx	<p>Deaktiviert die referenzielle Integritätsprüfung von Primärschlüssel/Fremdschlüssel. Die Option -fx kann nicht mit der Option -i verwendet werden.</p>
-i	<p>Definiert <i>object-name</i> als Liste von Indizes.</p>
-o filename	<p>Schreibt Ausgabemeldungen in die benannte Datei.</p>
-q	<p>Ausgabemeldungen werden beim Client nicht angezeigt. Sie können jedoch die Meldungen weiterhin in einer Datei protokollieren, indem Sie die Option -o verwenden.</p>

Option	Beschreibung
<b>-s</b>	Validiert die Datenbank mithilfe von Prüfsummen. Mit Prüfsummen kann festgestellt werden, ob eine Datenbankseite auf der Festplatte geändert wurde. Bei der Prüfsummenvalidierung wird jede einzelne Seite aus der Datenbank von der Festplatte gelesen und ihre Prüfsumme berechnet, falls die Seite über eine Prüfsumme verfügt. Wenn die berechnete Prüfsumme nicht gleich der für die Seite gespeicherten Prüfsumme ist, wurde die Seite auf der Festplatte geändert und es wird eine Fehlermeldung zurückgegeben. Die Seitennummern ungültiger Seiten erscheinen im Meldungsfenster des Datenbankservers. Die Option -s darf nicht zusammen mit der Option -d, -i, -t bzw. -fx verwendet werden.
<b>-t</b>	Definiert <i>object-name</i> als Liste von Tabellen oder materialisierten Ansichten.
<i>object-name</i>	Gibt den Namen der Tabelle oder der materialisierten Ansicht an, die zu validieren ist.  Wenn die Option -i verwendet wird, bezieht sich <i>object-name</i> stattdessen auf einen zu validierenden Index.

### Privilegien

Sie müssen das VALIDATE ANY OBJECT-Systemprivileg haben. Wenn ein bestimmter Index angegeben wird, müssen Sie der Eigentümer der Tabelle sein, für die der Index erstellt wird, oder das VALIDATE ANY OBJECT-Systemprivileg haben.

### Bemerkungen

Mit dem Validierungs-Dienstprogramm können Sie die Indizes und Schlüssel in einigen oder allen Tabellen bzw. materialisierten Ansichten in einer Datenbank validieren. Sie können das Validierungs-Dienstprogramm auch zur Prüfung der Datenbankdateistruktur verwenden, um zu überprüfen, dass alle Seiten in der Datenbank dem korrekten Objekt gehören und die Seitenprüfsummen korrekt sind. Standardmäßig validiert dbvalid alle Tabellen, materialisierten Ansichten und Indizes in der Datenbank sowie die Datenbankdateistruktur selbst.

Bei der Validierung einer Tabelle validiert dbvalid auch alle Tabellenindizes, um zu überprüfen, ob die Menge der Zeilen und Werte in der Tabelle mit der Menge der Zeilen und Werte in jedem Index übereinstimmt. Alle BLOBs in der Tabelle werden auch durchsucht, BLOB-Zuordnungstabellen werden überprüft und verwaiste BLOBs werden erkannt. Das Validierungs-Dienstprogramm prüft auch die physische Struktur aller Indexseiten, die Reihenfolge der Index-Hash-Werte und die Eindeutigkeit des Indexes (falls diese Anforderungen vorgegeben wurden). Wenn die Option -fx nicht angegeben ist, wird

der Wert der einzelnen Fremdschlüssel in der entsprechenden Primärschlüsseltabelle gesucht, um zu überprüfen, ob Integritätsregeln zur Erhaltung der referenziellen Integrität eingehalten wurden.

Wenn die Option -i angegeben wird, validiert dbvalid jeden Index in der Objektliste. Das Validieren eines Index funktioniert genauso wie das Validieren einer Tabelle, außer dass nur der festgelegte Index und die Basistabelle validiert werden. Wenn der Index ein Fremdschlüssel ist, wird jeder Wert in der Primärschlüsseltabelle gesucht, außer wenn die Option -fx angegeben ist.

Wenn Sie die Datenbankvalidierung starten, während der Datenbankaufräumvorgang ausgeführt wird, kann die Validierung erst ausgeführt werden, wenn der Aufräumvorgang abgeschlossen ist.

Sie können das Validierungs-Dienstprogramm auch folgendermaßen starten:

- In Sybase Central verwenden Sie den **Assistenten zum Validieren einer Datenbank**.
- Von Interactive SQL aus verwenden Sie die VALIDATE-Anweisung.

Das Validierungsdienstprogramm kann in Verbindung mit regelmäßigen Sicherungen verwendet werden, um Ihnen Vertrauen in die Integrität der Daten in Ihrer Datenbank zu geben. Wenn Sie eine Sicherungskopie Ihrer Datenbank validieren möchten, wird empfohlen, eine Kopie der Sicherung zu erstellen und die Kopie zu validieren. Damit stellen Sie sicher, dass Sie keine Änderungen an der Datei vornehmen, die zur Wiederherstellung verwendet wird.

#### **Vorsicht**

Sicherungskopien der Datenbank und des Transaktionslogs dürfen auf keinen Fall geändert werden. Wenn während der Sicherung keine Transaktionen aktiv waren oder Sie BACKUP DATABASE WITH CHECKPOINT LOG RECOVER oder WITH CHECKPOINT LOG NO COPY angegeben haben, können Sie die Validität der Sicherungsdatenbank im Schreibschutzmodus prüfen, oder indem Sie eine Kopie der Sicherungsdatenbank validieren.

Wenn jedoch Transaktionen aktiv waren oder Sie BACKUP DATABASE WITH CHECKPOINT LOG COPY angegeben haben, muss der Datenbankserver eine Wiederherstellung der Datenbank bei ihrem Start durchführen. Die Wiederherstellung verändert die Sicherungskopie, womit verhindert wird, dass nachfolgende Transaktionslogdateien aus der Originaldatenbank angewendet werden.

Wenn durch das Validierungs-Dienstprogramm eine Datenbank automatisch gestartet wird, läuft sie im schreibgeschützten Modus. Damit wird verhindert, dass Änderungen an der Datenbank vorgenommen werden, falls die Validierung Teil eines Sicherungs- oder Wiederherstellungsplans ist.

Wenn sich das Validierungs-Dienstprogramm mit einer laufenden Datenbank verbindet, die nicht im schreibgeschützten Modus gestartet wurde, gibt das Dienstprogramm eine Warnmeldung aus. Diese Warnung erinnert daran, dass die validierte Datenbank nicht in einem Wiederherstellungsplan verwendet werden kann. Aufgrund der Methode, nach der Sicherungen erstellt werden, werden die meisten, von dbbackup erstellten Datenbanken als "Wiederherstellung erforderlich" markiert. Wenn die von Ihnen zu validierende Datenbank Wiederherstellung erfordert und Sie erzwingen wollen, dass sie im schreibgeschützten Modus startet, können Sie entweder die Datenbank starten, bevor Sie dbvalid ausführen, oder einen gültigen Wert für den DBS-Verbindungsparameter angeben.

Mit den beiden nachfolgenden Befehlen kann dbvalid ausgeführt werden, wenn die *mycopy.db*-Datenbank wiederhergestellt werden muss:

```
dbvalid -c "UID=DBA;PWD=sql;DBF=mycopy.db;DBS=-n mycopy"
```

```
dbvalid -c "UID=DBA;PWD=sql;DBF=mycopy.db;DBS=-dh"
```

### Vorsicht

Die Validierung einer Tabelle oder einer ganzen Datenbank darf nur durchgeführt werden, wenn keine Verbindungen Änderungen in der Datenbank durchführen, weil sonst möglicherweise Fehler über eine Datenbankbeschädigung gemeldet werden, obwohl eine solche nicht vorliegt.

Das Validierungs-Dienstprogramm kann Warnungen über Prüfsummenverletzungen für Datenbanken ausgeben, bei denen keine globalen Prüfsummen aktiviert sind. Dies liegt daran, dass der Datenbankserver trotzdem automatisch Prüfsummen für kritische Datenbankseiten berechnet, gleichgültig ob Prüfsummen aktiviert sind oder nicht. Eine Datenbank kann auch Prüfsummen für einige Seiten haben, weil sie mit Schreib-Prüfsummen gestartet wurde.

Der Datenbankserver erstellt Prüfsummen auch automatisch für Datenbanken, die auf Windows Mobile und auf Speichermedien laufen, die nicht so zuverlässig sind, z.B. auf Wechseldatenträgern.

Bei der Validierung wird kein exklusiver Zugriff auf die zu validierende Tabelle angefordert und es können Fehler gemeldet werden, wenn die Datenbank während der Validierung geändert wird. Aus diesem Grund wird die Validierung sinnvollerweise dann durchgeführt, wenn keine anderen Aktivitäten in der Datenbank laufen.

Beendigungs-codes sind 0 (Erfolg) oder eine von 0 verschiedene Zahl (Fehl Schlag).

### Siehe auch

- „Konfigurationsdateien“ auf Seite 882
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922
- „sa\_clean\_database-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbanken validieren (Sybase Central)“ auf Seite 1081
- „Sicherung und Datenwiederherstellung“ auf Seite 1027
- „Verbindungsparameter DatabaseSwitches (DBS)“ auf Seite 355
- „Erkennung von Beschädigungen mithilfe von Prüfsummen“ auf Seite 1084
- „Exit-Codes der Softwarekomponenten“ [*SQL Anywhere Server - Programmierung*]
- „VALIDATE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Versionsdiagnose-Dienstprogramm (dbversion)

Gibt Informationen über das angegebene Programm zurück.

### Syntax

```
dbversion executable-name
```

### Bemerkungen

Dieses Dienstprogramm ist nur auf Unix verfügbar und gibt Informationen über SQL Anywhere-Programmdateien zurück.

**Siehe auch**

- „Datenbankserveroption -v “ auf Seite 303

**Beispiel**

Geben Sie den nachstehenden Befehl ein:

```
$ dbversion /opt/sqlanywhere16/bin32/dbversion
```

Dieser Befehl gibt Informationen über das Programm dbversion zurück:

```
SQL Anywhere-Dienstprogramm Versionsdiagnose, Version 16.0.0.1403  
/opt/sqlanywhere16/bin32/dbversion: dbversion GA 16 0 0 1403 linux  
2012/10/10 15:32:50 nothr 32 production
```

Feld	Beschreibung
dbversion	Gibt den Programmnamen zurück.
GA	Gibt einen zweistelligen Code zurück, der einen Installationstyp bezeichnet.
16	Gibt die Hauptversionsnummer zurück.
0	Gibt die Nebenversionsnummer zurück.
0	Gibt die Supportpaketnummer zurück.
1403	Gibt die Build-Nummer zurück.
linux	Gibt den Betriebssystemcode zurück.
2012/10/10 15:32:50	Gibt das Datum bzw. den Zeitstempel für den Build zurück.
nothr	Gibt das Threading-Modell (nothr oder posix) zurück.
32	Gibt den Bitwert des Programms zurück (32 oder 64).
production	Gibt production oder debug zurück.



---

# Datenbankwartung

Dieser Abschnitt beschreibt, wie Sie Datenbankdateien sichern und wie Sie Ereignisse und Zeitpläne verwenden, um die Datenbankadministration zu vereinfachen.

## Sicherung und Datenwiederherstellung

Eine **Sicherung** ist eine vollständige oder teilweise Kopie der Informationen in einer Datenbank, die an einem physisch getrennten Speicherort aufbewahrt wird. Wenn die Datenbank ausfällt, können Sie sie aus der Sicherung **wiederherstellen**. Sie können Ihre Sicherungen verwenden, um alle festgeschriebenen Änderungen bis zu dem Zeitpunkt, an dem die Datenbank ausgefallen ist, wiederherzustellen.

Bei der Sicherung einer aktiven Datenbank wird ein Snapshot der Datenbank angefertigt, wobei die Daten in einem konsistenten Zustand sind, auch wenn andere Benutzer Änderungen in der Datenbank vornehmen.

Wenn das Betriebssystem oder der Datenbankserver ausfällt, oder aber der Datenbankserver nicht sauber herunterfahren wird, muss die Datenbank wiederhergestellt werden. Beim Start der Datenbank prüft der Datenbankserver, ob die Datenbank am Ende der vorhergehenden Sitzung sauber heruntergefahren wurde. Wenn dies nicht der Fall ist, führt der Datenbankserver einen automatischen Wiederherstellungsprozess durch, um alle Änderungen bis zur letzten festgeschriebenen Transaktion wiederherzustellen.

### Siehe auch

- „Arten der Datensicherung“ auf Seite 1029
- „Sichern von Datenbanken“ auf Seite 1027
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Entwerfen von Sicherungs- und Wiederherstellungsplänen“ auf Seite 1061
- „Datenbankwiederherstellung“ auf Seite 1046

## Sichern von Datenbanken

Wenn Sie eine Sicherung anfertigen, müssen Sie entscheiden, wo die Sicherungsdateien gespeichert werden sollen: auf dem Computer des Datenbankservers oder des Clients.

## Serverseitige Sicherungen erstellen

Sichern Sie eine Datenbank und speichern Sie die Sicherungsdateien auf dem Datenbankservercomputer.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

Wenn Sandboxing für die Datenbank aktiviert ist, müssen Sie den Schlüssel für gesicherte Funktionen angeben, damit der Datenbankserver die Sicherung in einem Verzeichnis außerhalb der Sandbox (des

Verzeichnisses, in dem sich die Hauptdatenbankdatei befindet, und der dazugehörigen Unterverzeichnisse) erstellen kann.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Validieren Sie die Datenbank.
3. Führen Sie eine BACKUP DATABASE-Anweisung aus oder führen Sie das Dienstprogramm dbbackup mit der Option -s aus.

### Ergebnisse

Die Datenbanksicherung wird auf dem Datenbankservercomputer gespeichert.

### Beispiel

Führen Sie die folgende Anweisung aus, um eine Sicherungskopie der Datenbankdateien im Verzeichnis *C:\temp\backup* auf dem Servercomputer zu erstellen.

```
BACKUP DATABASE DIRECTORY 'C:\\temp\\backup' ;
```

Führen Sie den folgenden Befehl aus, um eine Sicherungskopie der Datenbankdateien im Verzeichnis *c:\SQLAnybackup* auf dem Servercomputer zu erstellen.

```
dbbackup -s -c "DBN=demo;UID=DBA;PWD=sql" "c:\\temp\\SQLAnybackup"
```

### Siehe auch

- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Clientseitige Sicherungen erstellen“ auf Seite 1028
- „Arten der Datensicherung“ auf Seite 1029
- „Entwerfen von Sicherungs- und Wiederherstellungsplänen“ auf Seite 1061
- „Datenbankwiederherstellung“ auf Seite 1046
- „Sandboxing“ auf Seite 1411

## Clientseitige Sicherungen erstellen

Sichern Sie eine Datenbank und speichern Sie die Sicherungsdateien auf dem Clientcomputer.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.

2. Validieren Sie die Datenbank.
3. Führen Sie auf dem Clientcomputer das Sicherungsdienstprogramm (dbbackup) mit der Option -c aus.

## Ergebnisse

Die Datenbanksicherung wird auf dem Clientcomputer gespeichert.

## Beispiel

Führen Sie den folgenden Befehl aus, um eine Sicherungskopie der Datenbankdateien im Verzeichnis *c:\SQLAnybackup* auf dem Clientcomputer zu erstellen.

```
dbbackup -c "Host=sample_host;SERVER=myserver;DBN=demo;UID=DBA;PWD=sql" "c:\SQLAnybackup"
```

## Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Serverseitige Sicherungen erstellen“ auf Seite 1027
- „Arten der Datensicherung“ auf Seite 1029
- „Entwerfen von Sicherungs- und Wiederherstellungsplänen“ auf Seite 1061
- „Datenbankwiederherstellung“ auf Seite 1046

## Arten der Datensicherung

Eine **Offline**-Sicherung ist eine Kopie der Datenbankdateien. Sie können **Offline**-Sicherungen vornehmen, indem Sie die Datenbankdatei kopieren, wenn die Datenbank nicht läuft. Eine Offline-Sicherung sollte nur vorgenommen werden, wenn die Datenbank nicht läuft und der Datenbankserver ordnungsgemäß heruntergefahren wurde.

Eine **Online**-Sicherung wird bei laufender Datenbank durchgeführt. Bei der Sicherung einer aktiven Datenbank wird ein Snapshot der Datenbank angefertigt, wobei die Daten in einem konsistenten Zustand sind, auch wenn andere Benutzer Änderungen in der Datenbank vornehmen.

In der nachstehenden Tabelle werden die von SQL Anywhere unterstützten Sicherungstypen zusammengefasst:

Sicherungstyp	Beschreibung	Weitere Informationen
Vollständig	Eine vollständige Sicherung ist eine Sicherung der Datenbankdateien und des Transaktionslogs. In der Regel liegen zwischen einer vollständigen Sicherung mehrere inkrementelle Sicherungen.	„Vollständige Sicherungen erstellen“
Inkrementell	Eine Sicherung des Transaktionslogs. Sie müssen eine vollständige Sicherung ausführen, bevor Sie eine inkrementelle Sicherung ausführen können.	„Inkrementelle Sicherungen erstellen“

Sicherungstyp	Beschreibung	Weitere Informationen
Live	Eine kontinuierliche Sicherung ist eine Sicherung der Datenbank, während die Datenbank läuft.	„Live-Sicherungen“
Archiv	Eine Sammlung von Dateien, die alle erforderlichen Informationen für die Sicherung enthalten, also die Hauptdatenbankdatei, das Transaktionslog und etwaige zusätzliche DBSpaces.	„Archivsicherungen“
Image	Eine Kopie der Datenbankdatei bzw. des Transaktionslogs als jeweils getrennte Dateien. Unter Windows Mobile sind nur Sicherungskopien zulässig.	„Sicherungskopien“
Serverseitig	Eine Sicherung, die auf dem Computer des Datenbankservers durchgeführt wird.	„Serverseitige Sicherungen“
Clientseitig	Eine Sicherung, die auf dem Computer des Clients durchgeführt wird.	„Clientseitige Sicherungen“

## Vollständige Sicherungen erstellen

Führen Sie eine vollständige Sicherung aus, um sowohl die Datenbankdatei als auch das Transaktionslog zu sichern.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Kontext und Bemerkungen

Die Sicherungskopien der Datenbankdatei und der Transaktionslogdatei haben dieselben Namen wie die Online-Versionen dieser Dateien. Beispiel: Wenn Sie eine Sicherung der Beispieldatenbank vornehmen, werden die Sicherungen als *demo.db* und *demo.log* bezeichnet. Wenn Sie die Sicherungsanweisung wiederholen, wählen Sie ein neues Sicherungsverzeichnis, um das Überschreiben der Sicherungskopien zu vermeiden.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Validieren Sie die Datenbank, um sicherzustellen, dass sie nicht beschädigt ist. Sie können das Validierungsdienstprogramm, die gespeicherte Prozedur `sa_validate` oder die `VALIDATE DATABASE`-Anweisung verwenden.
3. Sichern Sie die Datenbankdatei und das Transaktionslog. Verwenden Sie beispielsweise die `BACKUP`-Anweisung.

## Ergebnisse

Eine vollständige Sicherung von Datenbankdatei und Transaktionslog wird erstellt.

## Beispiel

Die folgende Anweisung erstellt eine vollständige Sicherung der Datenbank im Verzeichnis *C:\temp\backup*:

```
BACKUP DATABASE
DIRECTORY 'c:\temp\backup';
```

## Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Datenbanken validieren (Sybase Central)“ auf Seite 1081
- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „sa\_validate-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Serverseitige Sicherungen“ auf Seite 1036
- „Clientseitige Sicherungen“ auf Seite 1043
- „Transaktionslogs umbenennen oder kürzen (Sybase Central)“ auf Seite 1070
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031
- „Arten der Datensicherung“ auf Seite 1029

## Inkrementelle Sicherungen erstellen

Eine inkrementelle Sicherung ist eine Art von Online-Sicherung. Eine inkrementelle Sicherung ist eine reine Sicherung des Transaktionslogs und kann nur für die Wiederherstellung verwendet werden, wenn vor der inkrementellen Sicherung eine vollständige Sicherung ausgeführt wurde. Es ist möglich, zwischen vollständigen Sicherungen mehrere inkrementelle Sicherungen auszuführen.

## Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

## Kontext und Bemerkungen

Die Sicherungskopien der Datenbankdatei und der Transaktionslogdatei haben dieselben Namen wie die Online-Versionen dieser Dateien. Beispiel: Wenn Sie eine Sicherung der Beispieldatenbank vornehmen, werden die Sicherungen als *demo.db* und *demo.log* bezeichnet. Wenn Sie die Sicherungsanweisung wiederholen, wählen Sie ein neues Sicherungsverzeichnis, um das Überschreiben der Sicherungskopien zu vermeiden.

Weitere Hinweise zum Einrichten eines wiederholbaren Befehls für die inkrementelle Sicherung durch Umbenennen der Sicherungskopie des Transaktionslogs finden Sie unter „[Sicherungskopien von Transaktionslogs während einer Sicherung umbenennen \(SQL\)](#)“ auf Seite 1073.

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.

2. Validieren Sie die Datenbank, um sicherzustellen, dass sie nicht beschädigt ist. Sie können das Validierungsdienstprogramm, die gespeicherte Prozedur `sa_validate` oder die `VALIDATE DATABASE`-Anweisung verwenden.
3. Sichern Sie nur das Transaktionslog, nicht die Datenbankdatei. Verwenden Sie beispielsweise die `BACKUP`-Anweisung.

### Ergebnisse

Eine inkrementelle Sicherung des Transaktionslogs wird erstellt.

### Beispiel

Die folgende Anweisung erstellt eine inkrementelle Sicherung der Datenbank im Verzeichnis `C:\temp\backup`:

```
BACKUP DATABASE  
  DIRECTORY 'c:\\temp\\backup'  
  TRANSACTION LOG ONLY  
  TRANSACTION LOG TRUNCATE;
```

### Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Datenbanken validieren (Sybase Central)“ auf Seite 1081
- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „sa\_validate-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Serverseitige Sicherungen“ auf Seite 1036
- „Clientseitige Sicherungen“ auf Seite 1043
- „Transaktionslogs umbenennen oder kürzen (Sybase Central)“ auf Seite 1070
- „Vollständige Sicherungen erstellen“ auf Seite 1030
- „Arten der Datensicherung“ auf Seite 1029

## Live-Sicherungen

Eine **Live-Sicherung** ist eine kontinuierliche Sicherung der Datenbank, die sie gegen einen Totalsystemausfall schützt. Sie können die Kopie des Transaktionslogs verwenden, um Ihr System auf einem zweiten Computer neu zu starten.

Wenn Ihr System ausfällt, kann das gesicherte Transaktionslog für einen schnellen Neustart des Systems verwendet werden. Je nach der Auslastung des Datenbankservers kann es aber sein, dass die Live-Sicherung mit einer gewissen Verzögerung gegenüber den festgeschriebenen Transaktionen ausgeführt wird.

Normalerweise müssen Sie das Dienstprogramm `dbbackup` vom Sekundärcomputer aus starten. Wenn der erste Computer unbenutzbar wird, können Sie Ihre Datenbank mit dem zweiten Computer neu starten. Datenbankdatei und Transaktionslog enthalten alle Daten, die für den Neustart der Datenbank erforderlich sind.

Eine Alternative zu einer Live-Sicherung ist die Datenbankspiegelung. Siehe „[Unterschiede zwischen Live-Sicherungen und Transaktionslogspiegeldateien](#)“ auf Seite 1033.

## Live-Sicherungen und regelmäßige Sicherungen

Die Live-Sicherung des Transaktionslogs hat immer maximal dieselbe Länge wie das aktive Transaktionslog. Wenn eine Live-Sicherung läuft und eine andere Sicherung das Transaktionslog neu startet (dbbackup -r oder dbbackup -x), kürzt die Live-Sicherung automatisch das live gesicherte Log und startet die Live-Sicherung neu an dem Punkt, an dem das neue Transaktionslog beginnt.

### Siehe auch

- „Live-Sicherungen erstellen“ auf Seite 1044
- „Datenbanken über Live-Sicherungen neu starten“ auf Seite 1052
- „Arten der Datensicherung“ auf Seite 1029

## Unterschiede zwischen Live-Sicherungen und Transaktionslogspiegeldateien

Live-Sicherungen und Transaktionslogspiegelungen bezwecken jeweils die Bereitstellung einer Kopie des Transaktionslogs. Es gibt aber diverse Unterschiede zwischen der Verwendung von Live-Sicherungen und Transaktionslogspiegeldateien:

- **Im Allgemeinen wird eine Live-Sicherung auf einem anderen Computer ausgeführt** Wenn das Sicherungsdienstprogramm auf einem eigenen Computer ausgeführt wird, übernimmt der Datenbankserver nicht den Schreibvorgang der gesicherten Logdatei. Die Datenübertragung erfolgt durch das Client/Server-Kommunikationssystem von SQL Anywhere. Die Auswirkungen auf die Performance sind daher geringer, die Zuverlässigkeit wird erhöht.

Es wird davon abgeraten, eine Transaktionslog-Spiegeldatei auf einem anderen Computer unterzubringen. Performance-Verschlechterungen und Datenbeschädigung könnten die Folge sein. Außerdem stoppt der Datenbankserver, wenn die Verbindung zwischen den Computern unterbrochen wird.

- **Eine Live-Sicherung bietet Schutz vor dem Totalausfall eines Computers** Auch wenn eine Transaktionslog-Spiegeldatei auf einem eigenen Medium geführt wird, bietet dieses Verfahren keine Möglichkeit zur sofortigen Wiederherstellung, wenn der ganze Computer ausfällt. Sie können Ihr System so konfigurieren, dass zwei Computer auf dieselbe Festplattengruppe zugreifen.
- **Eine Live-Sicherung kann gegenüber dem Datenbankserver zeitlich verzögert sein** Ein Transaktionslogspiegel enthält alle Daten, die für eine vollständige Wiederherstellung der festgeschriebenen Transaktionen erforderlich sind. Je nach der Auslastung des Datenbankservers kann es geschehen, dass die Live-Sicherung gegenüber dem Transaktionslogspiegel verzögert wird und daher nicht alle festgeschriebenen Transaktionen erfasst werden.

### Siehe auch

- „Transaktionslog-Spiegeldateien“ auf Seite 138

## Sicherungsformate

Eine **Archivsicherung** kopiert die Datenbankdatei und das Transaktionslog in eine oder mehrere Dateien, meist auf einem Bandlaufwerk. Archivsicherungen können nur als serverseitige Sicherungen ausgeführt werden.

Die Archivsicherung muss verwendet werden, wenn Sie direkt auf einem Band sichern. Sonst muss eine Sicherungskopie verwendet werden, weil Sicherungskopien einfacher wiederherzustellen sind.

Eine **Sicherungskopie** kopiert die Datenbankdateien bzw. das Transaktionslog als jeweils getrennte Dateien.

## Archivsicherungen

Eine Archivsicherung ist eine Sammlung von Dateien, die alle erforderlichen Informationen für die Sicherung enthalten, also die Hauptdatenbankdatei, das Transaktionslog und etwaige zusätzliche DBSpaces. Archivsicherungen können nur als serverseitige Sicherungen ausgeführt werden. Sie können eine Archivsicherung entweder in einer Datei oder auf einem Bandlaufwerk speichern.

Wenn Sie Archivsicherungen herstellen, wird der Dateiname, den Sie in der BACKUP-Anweisung angegeben haben, bei jeder erstellten Datei mit einer Erweiterung versehen (.1, .2, .3, etc.).

Standardmäßig werden bei Archivsicherungen freie Seiten übersprungen, um das Speichervolumen zu reduzieren und den Vorgang zu beschleunigen. Da Transaktionslogdateien keine freien Seiten enthalten, wirkt sich die Eliminierung freier Seiten nicht auf die Sicherung von Transaktionslogdateien aus. Das bedeutet, die Eliminierung freier Seiten hat möglicherweise geringere Auswirkungen auf Datenbanken mit umfangreichen Transaktionslogdateien als auf Datenbanken mit kleinen Transaktionslogdateien.

### Erstellen mit

Archivsicherungen können unter Verwendung der BACKUP DATABASE-Anweisung oder des **Assistenten zum Sichern einer Datenbank** in Sybase Central erstellt werden.

### Gilt für

Archivsicherungen werden nur auf Windows- (außer Windows Mobile) und Unix-Plattformen unterstützt. Archivsicherungen können nur als serverseitige Sicherungen ausgeführt werden.

### Wiederherstellen mit

Sie führen die Wiederherstellung einer Datenbank anhand einer Archivsicherung mit dem **Assistenten zum Wiederherstellen einer Datenbank** in Sybase Central bzw. der RESTORE DATABASE-Anweisung durch.

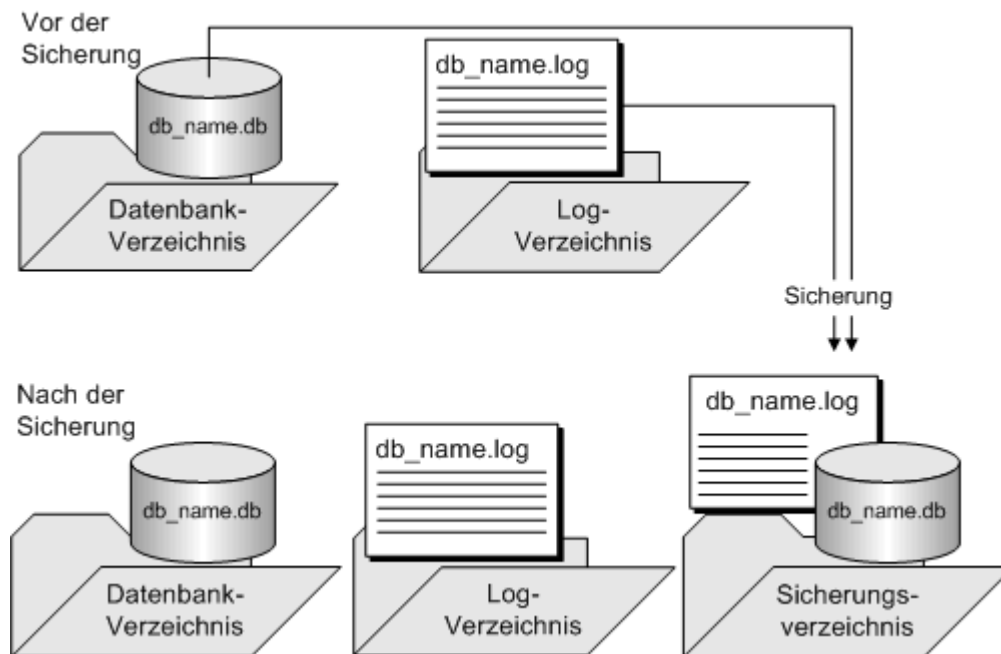
### Siehe auch

- „Sicherungskopien“ auf Seite 1035
- „Archivsicherungen erstellen (Sybase Central)“ auf Seite 1041
- „Archivsicherungen erstellen (SQL)“ auf Seite 1038
- „Archivsicherungen erstellen (Sybase Central)“ auf Seite 1041
- „Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)“ auf Seite 1050
- „Datenbanken aus Archivsicherungen wiederherstellen (Interactive SQL)“ auf Seite 1051
- „Arten der Datensicherung“ auf Seite 1029

## Sicherungskopien

Eine Sicherungskopie ist eine Kopie der Datenbankdatei bzw. des Transaktionslogs als jeweils getrennte Dateien.

Die einfachste Form der Sicherung ist eine Image-Sicherung (also eine Kopie der Datenbankdatei und/oder des Transaktionslogs als getrennte Dateien), bei der eine Kopie der Datenbankdatei und des Transaktionslogs hergestellt wird und das Transaktionslog unverändert bleibt und weder gekürzt noch ersetzt wird. Bei allen Sicherungen bleibt die Datenbankdatei unberührt. Eine vollständige Sicherung dieser Art wird in der nachfolgenden Darstellung gezeigt.



### Erstellen mit

Sie können eine Sicherungskopie mit dem Sicherungsdienstprogramm (dbbackup), dem **Assistenten zur Erstellung von Sicherungskopien** oder der BACKUP DATABASE-Anweisung erstellen.

### Gilt für

Sicherungskopien stehen auf allen unterstützten Plattformen zur Verfügung und sind der einzige unterstützte Sicherungstyp unter Windows Mobile.

Wenn Sie eine Sicherung auf Band erstellen möchten, verwenden Sie eine Archivsicherung.

**Siehe auch**

- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Sicherungskopien erstellen (SQL)“ auf Seite 1039
- „Sicherungskopien erstellen (Sybase Central)“ auf Seite 1041
- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Sicherungskopien erstellen (Sybase Central)“ auf Seite 1041
- „Arten der Datensicherung“ auf Seite 1029
- „Archiv Sicherungen“ auf Seite 1034

## Einschränkungen für die Sicherung und Wiederherstellung von Daten

Der Datenbankserver sperrt folgende Vorgänge, während eine Sicherung läuft:

- Eine weitere Sicherung, ausgenommen eine Live-Sicherung
- Es darf kein Checkpoint gesetzt werden, außer dem, der von der Sicherungsanweisung selbst gesetzt wurde.
- Jegliche Anweisung, die einen Checkpoint setzen würde. Siehe [Anweisungen, die implizite oder explizite Checkpoints auslösen auf Seite 142](#).

Während der Wiederherstellung, auch einer von einer Sicherung durchgeführten Wiederherstellung, dürfen andere Benutzer der Datenbank keine Arbeiten in der Datenbank ausführen.

**Siehe auch**

- [Anweisungen, die implizite oder explizite Checkpoints auslösen auf Seite 142](#)
- „Checkpoint-Logs“ auf Seite 143
- „Sicherungskomponenten“ auf Seite 1076
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077

## Serverseitige Sicherungen

Die Erstellung einer Sicherung auf demselben Computer, auf dem auch der Datenbankserver läuft, ist in der Regel schneller als eine Sicherung auf einem Clientcomputer, weil die Daten nicht über das Client-/Server-Kommunikationssystem transportiert werden müssen. Um eine serverseitige Sicherung in Ihre Anwendung zu integrieren, benutzen Sie eine SQL-Anweisung. Die folgenden Methoden werden für eine serverseitige Sicherung unterstützt:

Tool	Weitere Informationen
BACKUP-Anweisung	Die BACKUP DATABASE-Anweisung nutzt die Parallelität auf Geräteebene, um die Zeit bis zum Abschluss des Sicherungsvorgangs zu verkürzen. Parallele Sicherungen werden unter Windows Mobile nicht unterstützt. Siehe „ <a href="#">Parallele Datenbanksicherungen</a> “ auf Seite 1080.
Sicherungsdienstprogramm (dbbackup)	<p>Das Sicherungsdienstprogramm (dbbackup) nutzt die Parallelität auf Geräteebene, um die Zeit bis zum Abschluss des Sicherungsvorgangs zu verkürzen. Parallele Sicherungen werden unter Windows Mobile nicht unterstützt. Siehe „<a href="#">Parallele Datenbanksicherungen</a>“ auf Seite 1080.</p> <p>Siehe „<a href="#">Serverseitige Sicherungen mit dem Sicherungsdienstprogramm (dbbackup) erstellen</a>“ auf Seite 1040.</p>
<b>Assistent zum Sichern einer Datenbank</b>	Dieser Assistent erstellt eine Archivsicherung. Sie können als Speicherort der Sicherung einen Dateinamen oder ein Bandlaufwerk angeben. Siehe „ <a href="#">Archivsicherungen erstellen (Sybase Central)</a> “ auf Seite 1041.
<b>Assistent zum Erstellen einer Sicherungskopie</b>	Dieser Assistent erstellt Kopien aller Datenbankdateien bei laufender Datenbank. Zur Wiederherstellung kopieren Sie alle Dateien zurück auf den Datenbankservercomputer. Siehe „ <a href="#">Sicherungskopien erstellen (Sybase Central)</a> “ auf Seite 1041.
<b>Assistent zum Erstellen von Wartungsplänen</b>	Mit diesem Assistenten erstellen Sie eine Planung für unterschiedliche Aufgaben, einschließlich für die Sicherung einer Datenbank. Sie können entscheiden, eine Archivsicherung, eine Sicherungskopie oder eine inkrementelle Sicherung zu erstellen. Siehe „ <a href="#">Wartungspläne</a> “ auf Seite 1064.
DBBackup-Funktion	Siehe <a href="#">DBBackup-Methode [Datenbanktools] [SQL Anywhere Server - Programmierung]</a> .
SQL Anywhere Volume-Schattenkopiedienst (dbvss)	Siehe „ <a href="#">SQL Anywhere-Volumeschattenkopiedienst (VSS)</a> “ auf Seite 1042.

Wenn Sandboxing für die Datenbank aktiviert ist, müssen Sie den Schlüssel für gesicherte Funktionen angeben, damit der Datenbankserver die Sicherung in einem Verzeichnis außerhalb der Sandbox (des

Verzeichnisses, in dem sich die Hauptdatenbankdatei befindet, und der dazugehörigen Unterverzeichnisse) erstellen kann.

### Siehe auch

- „Clientseitige Sicherungen“ auf Seite 1043
- „Arten der Datensicherung“ auf Seite 1029
- „Sandboxing“ auf Seite 1411

## Archivsicherungen erstellen (SQL)

Eine Archivsicherung ist eine Sammlung von Dateien, die alle erforderlichen Informationen für die Sicherung enthalten, also die Hauptdatenbankdatei, Transaktionslogs und DBSpaces. Archivsicherungen können nur als serverseitige Sicherungen ausgeführt werden und können entweder in einer Datei oder auf einem Bandlaufwerk gespeichert werden.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Validieren Sie die Datenbank.
3. Führen Sie eine BACKUP-Anweisung aus, um eine Archivsicherung auf Band durchzuführen.

Wenn Sie ATTENDED auf OFF setzen, schlägt die Sicherung fehl, sobald auf dem Band oder der Festplatte kein Platz mehr vorhanden ist. Wenn ATTENDED auf ON gesetzt ist, werden Sie aufgefordert, bei Platzmangel auf dem Sicherungsdatenträger entsprechende Maßnahmen zu treffen.

Bei dieser Sicherung bleibt das Transaktionslog unberührt.

### Ergebnisse

Die BACKUP-Anweisung schreibt einen Eintrag in die Textdatei *backup.syb*. Weitere Hinweise zum Speicherort der Datei *backup.syb* finden Sie unter „SALOGDIR-Umgebungsvariable“ auf Seite 474.

### Beispiel

Mit der folgenden Anweisung erstellen Sie eine Archivsicherung auf dem ersten Bandlaufwerk eines Windows-Computers:

```
BACKUP DATABASE  
TO '\\\\.\\tape0'  
ATTENDED OFF  
WITH COMMENT 'May 6 backup';
```

Das erste Bandlaufwerk unter Windows ist *\\\\.\\tape0*. Da der Backslash in SQL-Zeichenfolgen ein Escapezeichen ist, muss jeder Backslash verdoppelt werden.

**Siehe auch**

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Archivsicherungen“ auf Seite 1034
- „Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)“ auf Seite 1050
- „Sicherungskopien“ auf Seite 1035
- „Datenbankwiederherstellung“ auf Seite 1046

## Sicherungskopien erstellen (SQL)

Erstellen Sie mithilfe der BACKUP-Anweisung eine Sicherungskopie, die aus einer Kopie der Datenbankdatei bzw. des Transaktionslogs als jeweils getrennte Dateien besteht.

**Voraussetzungen**

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

**Aufgabe**

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Validieren Sie die Datenbank.
3. Führen Sie die folgende Anweisung aus, um eine Sicherungskopie zu erstellen:

```
BACKUP DATABASE  
  DIRECTORY directory-name;
```

Bei dieser Sicherung bleibt das Transaktionslog unberührt.

**Ergebnisse**

Die BACKUP-Anweisung schreibt einen Eintrag in die Textdatei *backup.syb*. Weitere Hinweise zum Speicherort der Datei *backup.syb* finden Sie unter „[SALOGDIR-Umgebungsvariable](#)“ auf Seite 474.

**Beispiel**

Mit der nachstehenden Anweisung erstellen Sie eine Sicherungskopie der aktuellen Datenbank und des Transaktionslogs, speichern sie in verschiedenen Dateien und benennen das bestehende Transaktionslog um.

```
BACKUP DATABASE  
  DIRECTORY 'c:\\temp\\backup'  
  TRANSACTION LOG RENAME;
```

**Siehe auch**

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Sicherungskopien“ auf Seite 1035
- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Archivsicherungen“ auf Seite 1034
- „Datenbankwiederherstellung“ auf Seite 1046

## Serverseitige Sicherungen mit dem Sicherungsdienstprogramm (dbbackup) erstellen

Erstellen Sie mithilfe des Dienstprogramms dbbackup eine Sicherungskopie, die aus einer Kopie der Datenbankdatei bzw. des Transaktionslogs als jeweils getrennte Dateien besteht.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Kontext und Bemerkungen

Wenn Sandboxing für die Datenbank aktiviert ist, müssen Sie den Schlüssel für gesicherte Funktionen angeben, damit der Datenbankserver die Sicherung in einem Verzeichnis außerhalb der Sandbox (des Verzeichnisses, in dem sich die Hauptdatenbankdatei befindet, und der dazugehörigen Unterverzeichnisse) erstellen kann.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Validieren Sie die Datenbank.
3. Führen Sie das Dienstprogramm dbbackup aus.

```
dbbackup -s -c "connection-string" [ -t ] backup-directory
```

Die Option -s erstellt eine Sicherungskopie auf dem Datenbankserver.

Geben Sie die Option -t nur an, wenn eine inkrementelle Sicherung durchgeführt werden soll.

Bei dieser Sicherung bleibt das Transaktionslog unberührt.

### Ergebnisse

Die serverseitige Sicherung wird erstellt.

### Beispiel

Im folgenden Beispiel wird eine Sicherungskopie auf dem Datenbankservercomputer im Verzeichnis *c:\SQLAnybackup* erstellt.

```
dbbackup -s -c "HOST=myhost;DBN=demo;UID=DBA;PWD=sql" "c:\SQLAnybackup"
```

**Siehe auch**

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031
- „Sicherungskopien“ auf Seite 1035
- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Datenbankwiederherstellung“ auf Seite 1046
- „Sandboxing“ auf Seite 1411

## Archivsicherungen erstellen (Sybase Central)

Verwenden Sie den **Assistenten zum Sichern einer Datenbank**, um eine Archivsicherung zu erstellen, eine Sammlung von Dateien, die alle erforderlichen Informationen für die Sicherung enthält, also die Hauptdatenbankdatei, Transaktionslogs und DBSpaces. Wenn Sie eine Archivsicherung in Sybase Central durchführen, können Sie die Datenbank direkt auf Band oder Festplatte sichern.

**Voraussetzungen**

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

**Aufgabe**

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Validieren Sie die Datenbank. Sie können das Validierungsdienstprogramm oder die gespeicherte Prozedur sa\_validate verwenden.
3. Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Datenbank sichern**.
4. Befolgen Sie die Anweisungen des Assistenten.

**Ergebnisse**

Eine Archivsicherung wird erstellt.

**Siehe auch**

- „Archivsicherungen“ auf Seite 1034
- „Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)“ auf Seite 1050
- „Datenbankwiederherstellung“ auf Seite 1046

## Sicherungskopien erstellen (Sybase Central)

Mit dem **Assistenten zum Erstellen einer Sicherungskopie** können Sie eine Sicherungskopie erstellen, bei der alle Datenbankdateien kopiert werden, aber das Transaktionslog unberührt bleibt, und so weiterhin mit dem vorhandenen Transaktionslog arbeiten.

## Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Validieren Sie die Datenbank. Sie können das Validierungsdienstprogramm oder die gespeicherte Prozedur sa\_validate verwenden.
3. Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Sicherungskopie erstellen**.
4. Befolgen Sie die Anweisungen im **Assistenten zum Erstellen einer Sicherungskopie**.

Klicken Sie in der Liste **Was wollen Sie mit dem Transaktionslog tun?** auf **Weiterhin dasselbe Transaktionslog verwenden**.

5. Zur Wiederherstellung kopieren Sie alle Dateien zurück auf den Datenbankservercomputer.

## Ergebnisse

Eine Sicherungskopie wird erstellt.

## Siehe auch

- „Sicherungskopien“ auf Seite 1035
- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Datenbankwiederherstellung“ auf Seite 1046

## SQL Anywhere-Volumeschattenkopie-Dienst (VSS)

SQL Anywhere ist mit dem VSS-Dienst (Microsoft Volumeschattenkopie-Dienst) kompatibel. Sie können den VSS-Dienst verwenden, um Point-in-time-Snapshots von gesamten Festplatten-Volumes oder von Volume-Gruppen zu erstellen und Kopien von Dateien zu erstellen, die für die exklusive Verwendung durch Anwendungen wie SQL Anywhere-Datenbankserver geöffnet sind. VSS wird ab den 32-Bit Windows XP-Betriebssystemen und 32-Bit- und 64-Bit Windows Server 2003-Betriebssystemen einschließlich Windows Vista unterstützt.

Standardmäßig können alle SQL Anywhere-Datenbanken den VSS-Dienst für Sicherungen verwenden, wenn das SQL Anywhere-VSS-Schreibprogramm (*dbvss16.exe*) läuft. Sie können VSS ohne das SQL Anywhere-VSS-Schreibprogramm verwenden, um Datenbanken zu sichern. Sie benötigen aber vielleicht die kompletten SQL Anywhere-Wiederherstellungsprozeduren, um die Datenbanken wiederherzustellen. Wenn ein Datenbankserver am Schattenkopiedienst nicht teilnehmen soll, verwenden Sie beim Start des Datenbankservers **-vss-**. Als Alternative können Sie das Dienstprogramm für Dienste (dbsvc) für Windows verwenden, um anzugeben, wann der VSS-Dienst gestartet wird.

So funktioniert VSS mit SQL Anywhere:

- Ihre Sicherungsanwendung sendet einen Befehl an VSS, einen Snapshot zu erstellen.
- VSS gibt den **identify**-Befehl an das SQL Anywhere-VSS-Schreibprogramm (*dbvss16.exe*) aus.
- VSS gibt den **prepare to snapshot**-Befehl aus, um alle Transaktionen zu stoppen und alle geänderten Seiten in allen Datenbanken und allen Datenbankservern auf die Festplatte zu schreiben. Wenn die Transaktionen einer Datenbank nicht binnen 10 Sekunden gestoppt werden, kann der Snapshot nicht festgeschriebene Transaktionen enthalten und eine vollständige Wiederherstellung ist eventuell nicht möglich.
- VSS gibt den **freeze**-Befehl aus, um einen Checkpoint zu setzen, und stoppt dann alle Aktivitäten aller Datenbanken auf allen Datenbankservern. Alle SQL Anywhere-Datenbankserver warten maximal 60 Sekunden, damit alle Datenbanken ihre Aktivitäten einstellen. Dieser Vorgang benötigt normalerweise nur wenige Sekunden.
- VSS gibt den **thaw**-Befehl an das SQL Anywhere-VSS-Schreibprogramm aus, damit alle Transaktionen in allen Datenbanken auf allen Datenbankservern wieder aufgenommen werden.

In seltenen Fällen ist SQL Anywhere möglicherweise nicht in der Lage, die Transaktionen zu stoppen oder einen Checkpoint innerhalb der von VSS erlaubten maximalen Dauer abzuschließen. Wenn dies eintritt, müssen Sie das Transaktionslog verwenden und einen kompletten Wiederherstellungsprozess durchführen, um die gesicherte Datenbank wiederherzustellen.

#### Siehe auch

- „Dienstprogramm für Dienste (dbsvc) für Windows“ auf Seite 974
- „Windows-Dienste erstellen (Sybase Central)“ auf Seite 182

## Clientseitige Sicherungen

Die folgenden Methoden werden für eine clientseitige Sicherung unterstützt:

Tool	Weitere Informationen
Sicherungsdienstprogramm (dbbackup)	Das Sicherungsdienstprogramm (dbbackup) nutzt die Parallelverarbeitung auf der Geräteebe, um die Zeit bis zum Abschluss des Sicherungsvorgangs zu verkürzen. Parallele Sicherungen werden unter Windows Mobile nicht unterstützt.
DBBackup-Funktion	Siehe <a href="#">DBBackup-Methode [Datenbanktools]</a> [ <i>SQL Anywhere Server - Programmierung</i> ].

Das Dienstprogramm dbbackup erstellt eine Sicherungskopie, die aus einer Kopie der Datenbankdatei bzw. des Transaktionslogs als jeweils getrennte Dateien besteht.

### Siehe auch

- „Parallele Datenbanksicherungen“ auf Seite 1080
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Serverseitige Sicherungen“ auf Seite 1036
- „Datenbankwiederherstellung“ auf Seite 1046
- „Arten der Datensicherung“ auf Seite 1029

## Live-Sicherungen erstellen

Erstellen Sie eine Live-Sicherung des Transaktionslogs, indem Sie das Dienstprogramm dbbackup mit der Option -l ausführen. Eine Live-Sicherung liefert eine redundante Kopie des Transaktionslogs und kann verwendet werden, um ein Sekundärsystem neu zu starten, falls das Primärsystem, das den Datenbankserver ausführt, unbrauchbar wird.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Kontext und Bemerkungen

Eine Live-Sicherung läuft permanent mit und wird nur dann beendet, wenn der Server heruntergefahren wird. Wenn ein System ausfällt, kann das gesicherte Transaktionslog für einen schnellen Neustart des Systems verwendet werden. Je nach der Auslastung des Servers kann es aber sein, dass die Live-Sicherung mit einer gewissen Verzögerung gegenüber den festgeschriebenen Transaktionen ausgeführt wird.

### Aufgabe

1. Richten Sie einen Sekundärcomputer ein, von dem aus Sie die Datenbank betreiben können, wenn der Online-Computer ausfällt. Vergewissern Sie sich, dass SQL Anywhere auf dem Sekundärcomputer installiert ist.
2. Stellen Sie vom Sekundärcomputer aus eine Verbindung mit der Datenbank her.
3. Validieren Sie die Datenbank.
4. Führen Sie vom sekundären Computer aus eine vollständige Sicherung auf dem Sekundärcomputer durch:

```
dbbackup -c "connection-string" path-on-secondary-computer\filename
```

5. Führen Sie vom sekundären Computer aus eine Live-Sicherung des Transaktionslogs auf dem Sekundärcomputer durch.

```
dbbackup -l path-on-secondary-computer\filename.log -c "connection-string"
```

6. Führen Sie vom sekundären Computer aus regelmäßig eine vollständige Sicherung der Online-Datenbank durch.

## Ergebnisse

Wenn der Primärcomputer unbrauchbar wird, kann die Datenbank mithilfe der Live-Sicherung auf dem Sekundärcomputer neu gestartet werden. Datenbankdatei und Transaktionslog enthalten alle Daten, die für einen Neustart erforderlich sind.

### Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Live-Sicherungen“ auf Seite 1032
- „Datenbankwiederherstellung“ auf Seite 1046
- „Datenbanken über Live-Sicherungen neu starten“ auf Seite 1052
- „Arten der Datensicherung“ auf Seite 1029

## Sicherungsvalidierung

Die Beschädigung einer Datenbankdatei wird möglicherweise erst erkannt, wenn der Datenbankserver versucht, auf den betroffenen Teil der Datenbank zuzugreifen. Als Teil Ihres Sicherungs- und Wiederherstellungsplans sollten Sie daher regelmäßig die Gültigkeit Ihrer Datenbank prüfen, indem Sie Tools wie den **Assistenten zum Validieren einer Datenbank** in Sybase Central oder das Validierungsdienstprogramm (dbvalid) verwenden. Sie sollten Ihre Datenbank sowohl vor als auch nach einer Sicherung validieren. Sie müssen das VALIDATE ANY OBJECT-Privileg haben, um Validierungsvorgänge durchzuführen.

Wenn Sie eine Sicherungskopie einer zu validierenden Datenbank starten, können Sie die Datenbankoption -ds verwenden, um den Speicherort der DBSpace-Dateien und das Transaktionslog anzugeben. Dadurch können Sie die Sicherungskopie der Datenbank auf dem Computer der ursprünglichen Datenbank starten, während die ursprüngliche Datenbank weiter läuft. Siehe „Datenbankoption -ds“ auf Seite 325.

Abhängig von den von Ihnen angegebenen Optionen kann die Validierung Prüfsummen und die Korrektheit von Indexdaten umfassen, und ob alle Tabellenseiten zu Objekten in der Datenbank gehören. Bei der Expressvalidierung der Datenbank (mit der Option -fx) werden die Daten, die kontinuierliche Zeilenstruktur oder die Fremdschlüsselbeziehungen nicht geprüft.

**Vorsicht**

Sicherungskopien der Datenbank und des Transaktionslogs dürfen auf keinen Fall geändert werden. Wenn während der Sicherung keine Transaktionen aktiv waren oder Sie `BACKUP DATABASE WITH CHECKPOINT LOG RECOVER` oder `WITH CHECKPOINT LOG NO COPY` angegeben haben, können Sie die Validität der Sicherungsdatenbank im Schreibschutzmodus prüfen, oder indem Sie eine Kopie der Sicherungsdatenbank validieren.

Wenn jedoch Transaktionen aktiv waren oder Sie `BACKUP DATABASE WITH CHECKPOINT LOG COPY` angegeben haben, muss der Datenbankserver eine Wiederherstellung der Datenbank bei ihrem Start durchführen. Die Wiederherstellung ändert die Sicherungskopie, und das sollte vermieden werden.

Wenn Sie sicher sein können, dass während der Sicherung keine Transaktionen aktiv waren, braucht der Datenbankserver die Wiederherstellungsschritte nicht auszuführen. In diesem Fall können Sie eine Validitätsprüfung der Sicherung mit der Schreibschutzoption durchführen. Siehe „[Datenbankserveroption -r](#)“ auf Seite 277.

**Tipp**

Die `BACKUP`-Anweisung mit der Klausel `WAIT BEFORE START` sorgt dafür, dass keine Transaktionen laufen, während Sie eine Sicherung starten.

Die Validierung erfordert exklusiven Zugriff auf das Objekt, das validiert wird. Aus diesem Grund wird die Validierung sinnvollerweise dann durchgeführt, wenn keine anderen Aktivitäten in der Datenbank laufen.

Wenn eine Basistabelle in der Datenbankdatei beschädigt ist, behandeln Sie dies wie einen Datenträgerfehler und nehmen Sie eine Wiederherstellung von einer früheren Sicherung vor. Wenn ein Index beschädigt ist, können Sie die Datenbank ohne Indizes entladen und dann wieder einlesen.

**Siehe auch**

- „[Datenbanken validieren \(Sybase Central\)](#)“ auf Seite 1081
- „[Transaktionslog-Validierung](#)“ auf Seite 1075
- „[Validieren einer Tabelle](#)“ auf Seite 1086
- „[VALIDATE-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „[Datenbankwiederherstellung](#)“ auf Seite 1046

## Datenbankwiederherstellung

Bei der **Wiederherstellung** werden die Datenbankdatei, das Transaktionslog und die DBSpaces wiederhergestellt und die Datenbank wird aus den inkrementellen Transaktionslogdateien so weit wie möglich in den aktuellsten Zustand versetzt.

Im Rahmen Ihrer Sicherungs- und Wiederherstellungsplanung müssen Sie Ihre Sicherung validieren. Eine Wiederherstellung sollte nur aus einer validierten Sicherung der Datenbank erfolgen.

Die Vorgehensweise zur Wiederherstellung hängt davon ab, ob bei einer inkrementellen Sicherung das Transaktionslog unberührt geblieben ist oder nicht. Wenn Sie während des Sicherungsvorgangs das Transaktionslog umbenannt oder gelöscht haben, müssen Sie eventuell Änderungen aus mehreren

Transaktionslogs übernehmen. Wenn bei Ihrem Sicherungsvorgang das Transaktionslog erhalten geblieben ist, brauchen Sie nur das Online-Transaktionslog für die Wiederherstellung.

Wenn mehrere Transaktionslogs vorhanden sind, ist es möglich, dass sich Transaktionen über mehrere Logdateien erstrecken. Sie müssen bei der Wiederherstellung die Transaktionslogs in der korrekten Reihenfolge anwenden, weil sonst alle Transaktionen zurückgesetzt werden, die sich über mehrere Transaktionslogs erstrecken. Sie können die Datenbankserveroption `-ad` angeben, damit der Datenbankserver die korrekte Reihenfolge bestimmt, in der die Transaktionslogs angewendet werden.

### Siehe auch

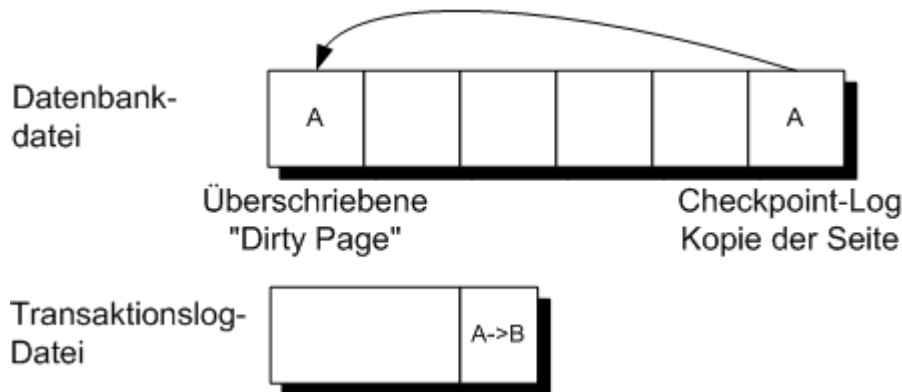
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053

## Der Prozess der automatischen Wiederherstellung

Wenn eine Datenbank während des Normalbetriebs heruntergefahren wird, setzt der Datenbankserver einen Checkpoint, sodass alle Informationen der Datenbank in der Datenbankdatei enthalten sind. Man bezeichnet dies als **sauberes** Herunterfahren.

Wenn Sie eine Datenbank starten, prüft der Datenbankserver, ob das letzte Herunterfahren sauber erfolgt ist oder auf eine Systemstörung zurückzuführen war. Wenn die Datenbank nicht sauber heruntergefahren wurde, trifft der Datenbankserver automatisch folgende Maßnahmen, um die Datenbank nach einem Systemausfall wiederherzustellen:

1. **Er führt eine Wiederherstellung bis zum letzten Checkpoint durch** Um alle Seiten in den Zustand des jüngsten Checkpoints zu versetzen, werden die Checkpoint-Logseiten über die Änderungen kopiert, die seit dem letzten Checkpoint durchgeführt wurden.



2. **Er übernimmt alle Änderungen seit dem Checkpoint** Änderungen zwischen dem Checkpoint und dem Systemausfall, die sich im Transaktionslog befinden, werden übernommen.
3. **Er setzt nicht festgeschriebene Transaktionen zurück** Alle nicht festgeschriebenen Transaktionen werden mit den Rollback-Logs zurückgesetzt.

## Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)

Verwenden Sie Sybase Central, um nicht festgeschriebene Vorgänge wiederherzustellen und alle festgeschriebenen Transaktionen erneut in die Datenbank zu übernehmen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

In einigen Fällen benötigen Sie aber Informationen über Transaktionen, die zum Zeitpunkt des Ausfalls noch nicht abgeschlossen waren. Wenn Sie eine Wiederherstellung nach einem Datenträgerfehler durchführen möchten, der die Datenbankdatei betroffen hat, muss das Transaktionslog unbeschädigt sein.

Der **Assistent zum Übersetzen einer Logdatei** unterstützt Sie bei der Konvertierung einer *.sql*-Datei in Sybase Central.

#### Hinweis

Das Transaktionslog kann Änderungen bis zu dem Punkt enthalten, an dem der Ausfall eingetreten ist, oder auch nicht. Es enthält alle Änderungen, die vor der letzten, festgeschriebenen, die Datenbank ändernden Transaktion eingetreten sind.

### Aufgabe

1. Klicken Sie in Sybase Central auf **Extras » SQL Anywhere 16 » Logdatei übersetzen**.
2. Befolgen Sie die Anweisungen des Assistenten.
3. Bearbeiten Sie das übersetzte Log (SQL-Skriptdatei) in einem Texteditor und ermitteln Sie die benötigten Anweisungen.

### Ergebnisse

Die nicht festgeschriebenen Vorgänge werden wiederhergestellt.

### Siehe auch

- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)“ auf Seite 1050
- „Datenbanken über Live-Sicherungen neu starten“ auf Seite 1052
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Wiederherstellung nach Datenträgerfehlern“ auf Seite 1056

## Nicht festgeschriebene Vorgänge wiederherstellen (Befehlszeile)

Verwenden Sie das Dienstprogramm dbtran, um nicht festgeschriebene Vorgänge wiederherzustellen und alle festgeschriebenen Transaktionen erneut in die Datenbank zu übernehmen.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

In einigen Fällen benötigen Sie aber Informationen über Transaktionen, die zum Zeitpunkt des Ausfalls noch nicht abgeschlossen waren. Wenn Sie eine Wiederherstellung nach einem Datenträgerfehler durchführen möchten, der die Datenbankdatei betroffen hat, muss das Transaktionslog unbeschädigt sein.

### Hinweis

Das Transaktionslog kann Änderungen bis zu dem Punkt enthalten, an dem der Ausfall eingetreten ist, oder auch nicht. Es enthält alle Änderungen, die vor der letzten festgeschriebenen, die Datenbank ändernden Transaktion eingetreten sind.

## Aufgabe

1. Führen Sie `dbtran` aus, um die Transaktionslogdatei in eine SQL-Skriptdatei zu konvertieren, und verwenden Sie dabei die Option `-a`, damit nicht festgeschriebene Transaktionen einbezogen werden.
2. Bearbeiten Sie das übersetzte Log (SQL-Skriptdatei) in einem Texteditor und ermitteln Sie die benötigten Anweisungen.

## Ergebnisse

Die nicht festgeschriebenen Vorgänge werden wiederhergestellt.

## Beispiel

Führen Sie den folgenden Befehl aus, um die Logdatei *sample.log* in die Datei *changes.sql* zu übersetzen:

```
dbtran -a sample.log changes.sql
```

## Siehe auch

- „Dienstprogramm zur Logkonvertierung (dbtran)“ auf Seite 948
- „Wiederherstellen aus einer Sicherungskopie“ auf Seite 1049
- „Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)“ auf Seite 1050
- „Datenbanken über Live-Sicherungen neu starten“ auf Seite 1052
- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Wiederherstellung nach Datenträgerfehlern“ auf Seite 1056

## Wiederherstellen aus einer Sicherungskopie

Stellen Sie eine Datenbank aus einer Sicherungskopie wieder her.

## Voraussetzungen

Es dürfen keine inkrementellen Sicherungen des Transaktionslogs vorliegen, die Sie im Wiederherstellungsprozess anwenden müssen.

### Aufgabe

1. Kopieren Sie die Datenbankdateien zurück an den ursprünglichen Speicherort. Führen Sie zum Beispiel folgenden Befehl aus:

```
copy C:\\temp\\backup\\demo.* C:\\Users\\Public\\Documents\\SQL Anywhere  
16\\Samples
```

2. Starten Sie den Datenbankserver neu.

### Ergebnisse

Die Datenbank wird wiederhergestellt.

### Siehe auch

- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Sicherungskopien“ auf Seite 1035
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048
- „Arten der Datensicherung“ auf Seite 1029

## Datenbanken aus Archivsicherungen wiederherstellen (Sybase Central)

Verwenden Sie Sybase Central, um eine Datenbank aus einer Archivsicherung wiederherzustellen.

### Voraussetzungen

Es dürfen keine inkrementellen Sicherungen des Transaktionslogs vorliegen, die Sie im Wiederherstellungsprozess anwenden müssen.

Wenn Sie eine Sicherung einer stark verschlüsselten Datenbank mit aktivierter Eliminierung freier Seiten erstellt haben, müssen Sie bei der Wiederherstellung den Chiffrierschlüssel für die Datenbank angeben.

### Aufgabe

1. Führen Sie den folgenden Befehl aus, um einen Personal Datenbankserver zu starten:

```
dbeng16 -n server-name
```

2. Starten Sie Sybase Central und stellen Sie eine Verbindung zur Dienstprogrammdatenbank her. Füllen Sie im Fenster **Verbinden** die folgenden Felder aus:
  - a. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - b. Im Feld **Kennwort** geben Sie **sql** ein.
  - c. Im Feld **Datenbankname** geben Sie **utility\_db** ein.
3. Klicken Sie auf **OK**.

4. Klicken Sie auf **Extras » SQL Anywhere 16 » Datenbank wiederherstellen**.
5. Befolgen Sie die Anweisungen des Assistenten.

### Ergebnisse

Die Datenbank wird wiederhergestellt.

### Siehe auch

- „Datenbankwiederherstellung mit mehreren Transaktionslogs“ auf Seite 1053
- „Die Dienstprogrammdatenbank“ auf Seite 145
- „Archivsicherungen“ auf Seite 1034
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048
- „Arten der Datensicherung“ auf Seite 1029

## Datenbanken aus Archivsicherungen wiederherstellen (Interactive SQL)

Verwenden Sie Interactive SQL, um eine Datenbank aus einer Archivsicherung wiederherzustellen.

### Voraussetzungen

Es dürfen keine inkrementellen Sicherungen des Transaktionslogs vorliegen, die Sie im Wiederherstellungsprozess anwenden müssen.

Wenn Sie eine Sicherung einer stark verschlüsselten Datenbank mit aktivierter Eliminierung freier Seiten erstellt haben, müssen Sie bei der Wiederherstellung den Chiffrierschlüssel für die Datenbank angeben.

### Aufgabe

1. Führen Sie den folgenden Befehl aus, um einen Personal Datenbankserver zu starten:

```
dbeng16 -n server-name
```

2. Starten Sie Interactive SQL und stellen Sie eine Verbindung zur Dienstprogrammdatenbank her. Füllen Sie die folgenden Felder aus:
  - a. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - b. Im Feld **Kennwort** geben Sie **sql** ein.
  - c. Im Feld **Datenbankname** geben Sie **utility\_db** ein.
3. Klicken Sie auf **OK**.
4. Führen Sie eine RESTORE DATABASE-Anweisung aus und geben Sie den Archivstamm an.

Jetzt können Sie wählen, ob eine archivierte Datenbank am ursprünglichen Speicherort (Standard) wiederhergestellt werden soll oder auf einem anderen Computer mit anderen Gerätenamen. Verwenden Sie dazu die RENAME-Klausel.

### Ergebnisse

Die Datenbank wird wiederhergestellt.

### Beispiel

Mit der folgenden Anweisung wird eine Datenbank vom Bandarchiv in der Datenbankdatei `c:\newdb\newdb.db` wiederhergestellt.

```
RESTORE DATABASE 'c:\\newdb\\newdb.db'  
FROM '\\\\.\\tape0';
```

Mit der folgenden Anweisung wird eine Datenbank von einer Archivsicherung in der Datei `c:\backup\archive.1` in der Datenbankdatei `c:\newdb\newdb.db` wiederhergestellt. Name und Standort des Transaktionslogs werden in der Datenbank angegeben.

```
RESTORE DATABASE 'c:\\newdb\\newdb.db'  
FROM 'c:\\backup\\archive';
```

Mit der folgenden Anweisung wird eine Datenbank von einer Archivsicherung in der Datei `c:\backup\archive.1` in der Datenbankdatei `c:\newdb\newdb.db` wiederhergestellt. Name und Standort des Transaktionslogs sind in der Datenbank angegeben. Der Chiffrierschlüssel wird für die Datenbank angegeben.

```
RESTORE DATABASE 'c:\\newdb\\newdb.db'  
FROM 'c:\\backup\\archive'  
KEY '3Km57y1z';
```

### Siehe auch

- „RESTORE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -gu“ auf Seite 255
- „Die Dienstprogrammdateiabank“ auf Seite 145
- „Archivsicherungen“ auf Seite 1034
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048
- „Arten der Datensicherung“ auf Seite 1029

## Datenbanken über Live-Sicherungen neu starten

Verwenden Sie zum Neustarten eine Live-Sicherung auf einem separaten Computer von dem Primärcomputer, auf dem Ihre Produktionsdatenbank ausgeführt wird.

### Voraussetzungen

Auf dem Sekundärcomputer muss SQL Anywhere installiert sein.

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

## Aufgabe

1. Kopieren Sie die vollständige Sicherung der Transaktionslogdatei und die Live-Sicherung des Transaktionslogs in ein Verzeichnis, in dem sie an der Sicherungskopie der Datenbankdatei angewendet werden können.
2. Benennen Sie die aktuelle Transaktionslogdatei, deren Name dem erwarteten Transaktionslog-Dateinamen entspricht, um oder löschen Sie sie (falls vorhanden).
3. Starten Sie den Datenbankserver mit der Option -ad, um die Transaktionslogs in dem im Schritt 1 erstellten Verzeichnis anzuwenden, und bringen Sie die Datenbank auf den letzten Stand:

```
dbeng16 "database-name.db" -ad directory-name
```

Der Datenbankserver fährt automatisch herunter, sobald das Transaktionslog übernommen wurde.

4. Starten Sie den Datenbankserver auf normale Weise und geben Sie den Benutzerzugriff frei. Jede neue Aktivität wird in ein neues Transaktionslog geschrieben.
5. Führen Sie eine Live-Sicherung des Transaktionslogs auf dem Sekundärcomputer durch.

```
dbbackup -l path\filename.log -c "connection-string"
```

## Ergebnisse

Die Datenbank wird neu gestartet.

## Siehe auch

- „Live-Sicherungen“ auf Seite 1032
- „Live-Sicherungen erstellen“ auf Seite 1044
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048
- „Arten der Datensicherung“ auf Seite 1029

## Datenbankwiederherstellung mit mehreren Transaktionslogs

Wenn Sie Ihre Datenbank wiederherstellen wollen und mehrere Transaktionslogs vorhanden sind, müssen Sie die Transaktionslogdateien in der richtigen Reihenfolge in der Sicherungskopie der Datenbank anwenden.

Sie können eine der folgenden Methoden verwenden, um Transaktionslogs in der richtigen Reihenfolge anzuwenden:

- Verwenden Sie die Option -a, damit jedes Log einzeln in die Sicherungskopie der Datenbank übernommen wird. Sie können das Dienstprogramm zur Logkonvertierung (dbtran) verwenden, um die Reihenfolge zu bestimmen, in der die Dateien generiert wurden. Das Dienstprogramm generiert und zeigt das früheste Log-Offset im Transaktionslog an. Dies ist eine nützliche Methode, um die richtige Reihenfolge zur Wiederherstellung der Datenbank zu gewährleisten.

- Verwenden Sie die Serveroption -ad, um den Standort der Transaktionslogdateien anzugeben. Der Datenbankserver bestimmt anhand der Log-Offsets die korrekte Reihenfolge der Anwendung der Transaktionslogs in der Sicherungskopie der Datenbank.
- Verwenden Sie die Serveroption -ar, damit der Datenbankserver die der Datenbank zugeordneten Logdateien anwendet, die sich in demselben Verzeichnis wie das Transaktionslog befinden. Der Transaktionslog-Standort wird von der Datenbank bezogen. Der Datenbankserver bestimmt anhand der Log-Offsets die korrekte Reihenfolge der Anwendung der Transaktionslogs in der Sicherungskopie der Datenbank.
- Verwenden Sie das Dienstprogramm zur Logkonvertierung (dbtran), um ein oder mehrere Transaktionslogs in eine .sql-Datei zu konvertieren, die in die Sicherungskopie der Datenbank übernommen werden kann.

### Siehe auch

- „Datenbankoption -a “ auf Seite 321
- „Datenbankoption -ad “ auf Seite 322
- „Datenbankoption -ar “ auf Seite 323
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998

## Datenbanken mit mehreren Transaktionslogs unter Verwendung der Serveroption -ad wiederherstellen

Verwenden Sie die Serveroption -ad, um eine Datenbank durch Anwenden aller Transaktionslogs aus einem angegebenen Verzeichnis auf die Sicherungskopie einer Datenbank wiederherzustellen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Kopieren Sie das Sicherungs-Transaktionslog und das aktuelle Transaktionslog in ein Verzeichnis.
2. Starten Sie den Datenbankserver und wenden Sie die Transaktionslogs auf eine Sicherungskopie einer Datenbank an:

```
dbeng16 backup-copy-of-database -ad directory
```

Der Datenbankserver verwendet die Log-Offsets in den Transaktionslogs, um die korrekte Reihenfolge der Anwendung der Logdateien zu bestimmen.

### Ergebnisse

Der Datenbankserver übernimmt die Transaktionslogs in die Sicherungskopie der Datenbank und wird anschließend heruntergefahren.

**Beispiel**

Starten Sie den Datenbankserver und wenden Sie die Transaktionslogs aus dem Verzeichnis *c:\backuplogs* auf eine Sicherungskopie der Datenbank *backupdemo.db* an:

```
dbeng16 backupdemo.db -ad c:\backuplogs
```

**Siehe auch**

- „Datenbankoption -ad “ auf Seite 322
- „Datenbanken mit mehreren Transaktionslogs unter Verwendung der Serveroption -a wiederherstellen“ auf Seite 1055
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048

## Datenbanken mit mehreren Transaktionslogs unter Verwendung der Serveroption -a wiederherstellen

Verwenden Sie die Serveroption -a, um einer einzelnen Transaktionslogdatei auf die Sicherungskopie einer Datenbank anzuwenden und anschließend den Datenbankserver herunterzufahren. Wenn mehrere Transaktionslogs vorhanden sind, wenden Sie sie einzeln und in der richtigen Reihenfolge an (vom ältesten zum neuesten).

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Aufgabe**

1. Starten Sie den Datenbankserver und übernehmen Sie das Transaktionslog *backupdemo.log* in die Sicherungskopie einer Datenbank mit der Bezeichnung *backupdemo.db*:

```
dbeng16 backupdemo.db -a backupdemo.log
```

Der Datenbankserver übernimmt das Sicherungs-Transaktionslog in die Sicherungskopie der Datenbank und wird anschließend heruntergefahren.

2. Starten Sie den Datenbankserver und übernehmen Sie das aktuelle Transaktionslog *demo.log* in die Sicherungskopie der Datenbank:

```
dbeng16 backupdemo.db -a demo.log
```

**Ergebnisse**

Der Datenbankserver übernimmt das aktuelle Transaktionslog in die Sicherungskopie der Datenbank und wird anschließend heruntergefahren.

**Beispiel**

1. Starten Sie den Datenbankserver und übernehmen Sie das Transaktionslog *backupdemo.log* in die Sicherungskopie einer Datenbank mit der Bezeichnung *backupdemo.db*:

```
dbeng16 backupdemo.db -a backupdemo.log
```

Der Datenbankserver übernimmt das Sicherungs-Transaktionslog in die Sicherungskopie der Datenbank und wird anschließend heruntergefahren.

2. Starten Sie den Datenbankserver und übernehmen Sie das aktuelle Transaktionslog *demo.log* in die Sicherungskopie der Datenbank:

```
dbeng16 backupdemo.db -a demo.log
```

Der Datenbankserver übernimmt das aktuelle Transaktionslog in die Sicherungskopie der Datenbank und wird anschließend heruntergefahren.

### Siehe auch

- „Datenbankoption -a “ auf Seite 321
- „Datenbanken mit mehreren Transaktionslogs unter Verwendung der Serveroption -ad wiederherstellen“ auf Seite 1054
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048

## Wiederherstellung nach Datenträgerfehlern

Wenn Ihre Datenbank nicht mehr benutzt werden kann, liegt eine **Datenbankstörung** vor. SQL Anywhere bietet Schutz gegen folgende Arten von Datenbankstörungen:

Art der Störung	Beschreibung	Beispiele
Datenträger	Die Datenbankdatei bzw. das Transaktionslog können nicht mehr benutzt werden. Diese Art der Störung kann auftreten, weil das System oder das Gerät, auf dem die Datenbankdatei gespeichert ist, instabil wird oder eine Dateibesädigung verursacht. Sicherungen schützen Ihre Daten gegen Datenträgerfehler.	<ul style="list-style-type: none"><li>• Die Festplatte, auf der die Datenbankdatei oder das Transaktionslog gespeichert ist, fällt aus.</li><li>• Die Datenbankdatei oder das Transaktionslog ist beschädigt. Dies kann auf Hardware- oder Softwareprobleme zurückzuführen sein.</li></ul>

Art der Störung	Beschreibung	Beispiele
System	<p>Von einem Systemausfall spricht man dann, wenn der Computer bzw. das Betriebssystem ausfällt und nicht alle Transaktionen abgeschlossen sind. Diese Art der Störung kommt vor, wenn der Computer einfach abgeschaltet oder neu gestartet wird, wenn eine andere Anwendung einen Systemabsturz bewirkt oder der Strom ausfällt.</p> <p>Nach einem Systemausfall wird der Datenbankserver automatisch wiederhergestellt, wenn Sie die Datenbank wieder starten. Die Ergebnisse der einzelnen Transaktionen, die vor dem Systemfehler festgeschrieben wurden, sind intakt. Alle Änderungen durch Transaktionen, die nicht vor dem Systemausfall festgeschrieben wurden, werden storniert.</p>	<ul style="list-style-type: none"> <li>Der Computer oder das Betriebssystem fallen während einer laufenden Transaktion aus. Das kann auf einen Absturz des Betriebssystems, einen Stromausfall oder einen unsachgemäßen Neustart des Computers zurückzuführen sein.</li> </ul>

## Wiederherstellen nach Beschädigung der Datenbankdatei durch einen Datenträgerfehler

Stellen Sie eine Datenbank wieder her, wenn durch den Datenträgerfehler nur die Datenbankdatei verloren gegangen ist.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Aufgabe

1. Stellen Sie eine zusätzliche Sicherungskopie des aktuellen Transaktionslogs her. Da die Datenbankdatei nicht verfügbar ist, enthält nur das Transaktionslog die Änderungen, die seit der letzten Sicherung vorgenommen wurden.
2. Erstellen Sie ein **Wiederherstellungsverzeichnis**, in dem die Dateien für die Wiederherstellung untergebracht werden.
3. Kopieren Sie die Datenbankdatei von der letzten vollständigen Sicherung in das Wiederherstellungsverzeichnis.

4. Übernehmen Sie die Transaktionen, die in gesicherten Transaktionslogs registriert sind, in die Wiederherstellungsdatenbank. Verwenden Sie eine der folgenden Methoden:

Option	Aktion
Manuell jedes Transaktionslog einzeln übernehmen, in chronologischer Reihenfolge	<p>a. Kopieren Sie die Transaktionslogdatei in das Wiederherstellungsverzeichnis.</p> <p>b. Starten Sie den Datenbankserver mit der Option zum Übernehmen des Transaktionslogs (-a):</p> <pre>dbeng16 database-name.db -a log-name.log</pre> <p>Der Datenbankserver fährt automatisch herunter, sobald das Transaktionslog übernommen wurde.</p> <p>c. Wenn Sie alle gesicherten Transaktionslogs angewendet haben, kopieren Sie das Online-Transaktionslog in das Wiederherstellungsverzeichnis.</p> <p>Übernehmen Sie die Transaktionen aus dem Online-Transaktionslog in die Wiederherstellungsdatenbank.</p> <pre>dbeng16 database-name.db -a log-name.log</pre>
Vom Datenbankserver die korrekte Reihenfolge der Transaktionslogs ermitteln und sie automatisch übernehmen lassen	<p>a. Kopieren Sie die Offline- und Online-Transaktionslogdateien in das Wiederherstellungsverzeichnis.</p> <p>b. Starten Sie den Datenbankserver mit der Option -ad, um den Speicherort der Transaktionslogs anzugeben. Der Datenbankserver bestimmt anhand der Log-Offsets die richtige Reihenfolge für die Anwendung der Transaktionslogs:</p> <pre>dbeng16 database-name.db -ad log-directory</pre> <p>Der Datenbankserver fährt automatisch herunter, sobald das Transaktionslog übernommen wurde.</p>

5. Führen Sie Validitätsprüfungen in der Wiederherstellungsdatenbank durch.
6. Führen Sie eine Sicherung durch.
7. Verschieben Sie die Datenbankdatei in das Produktionsverzeichnis.
8. Benachrichtigen Sie die Benutzer, dass sie nun wieder Zugriff auf die Produktionsdatenbank haben.

## Ergebnisse

Die Datenbank wird wiederhergestellt.

**Siehe auch**

- [„Datenbanken validieren \(Sybase Central\)“ auf Seite 1081](#)
- [„Der Prozess der automatischen Wiederherstellung“ auf Seite 1047](#)
- [„Nicht festgeschriebene Vorgänge wiederherstellen \(Sybase Central\)“ auf Seite 1048](#)

**Wiederherstellen nach Beschädigung eines Transaktionslog-Spiegels durch einen Datenträgerfehler**

Verwenden Sie den Transaktionslogspiegel für die Wiederherstellung nach einem Datenträgerfehler.

**Voraussetzungen**

Es gibt keine Voraussetzungen für diese Aufgabe.

**Kontext und Bemerkungen**

Wenn Ihre Datenbank eine konsolidierte Datenbank in einer SQL Remote-Installation ist, sollten Sie einen Transaktionslogspiegel oder eine Hardwarespiegelung verwenden.

**Aufgabe**

1. Erstellen Sie eine Kopie der Sicherung Ihrer Datenbankdatei, die zu dem Zeitpunkt angefertigt wurde, als das Transaktionslog startete.
2. Stellen Sie fest, welche der beiden Dateien beschädigt ist. Führen Sie das Dienstprogramm zur Logkonvertierung (dbtran) für das Transaktionslog und seinen Spiegel aus. Die Datei, die eine Fehlermeldung bewirkt, ist beschädigt.

Der folgende Befehl konvertiert ein Transaktionslog mit dem Namen *demo.log* und speichert die konvertierte Ausgabe in *demo.sql*:

```
dbtran demo.log
```

3. Kopieren Sie die richtige Datei über die beschädigte Datei.
4. Starten Sie den Datenbankserver erneut.

**Ergebnisse**

Die Datenbank wird wiederhergestellt.

**Siehe auch**

- [„Transaktionslog-Spiegeldateien“ auf Seite 138](#)
- [„Der Prozess der automatischen Wiederherstellung“ auf Seite 1047](#)
- [„Nicht festgeschriebene Vorgänge wiederherstellen \(Sybase Central\)“ auf Seite 1048](#)

## Wiederherstellung nach Datenträgerfehler bei einem nicht gespiegelten Transaktionslog

Führen Sie mithilfe eines nicht gespiegelten Transaktionslogs eine teilweise Wiederherstellung Ihrer Datenbank nach einem Datenträgerfehler durch.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Wenn Ihre Datenbank eine konsolidierte Datenbank in einer MobiLink- oder SQL Remote-Installation ist, sollten Sie einen Transaktionslogspiegel oder eine Hardwarespiegelung verwenden.

#### Vorsicht

Der `dbeng16`-Befehl darf nur benutzt werden, wenn die Datenbank nicht in ein MobiLink- oder SQL Remote-System eingebunden ist. Wenn Ihre Datenbank eine konsolidierte Datenbank in einer Replikationsumgebung mit SQL Remote ist, müssen Sie gegebenenfalls die entfernte Datenbank erneut extrahieren.

### Aufgabe

1. Sichern Sie die Datenbankdatei mit einer zusätzlichen Sicherung. Ohne Transaktionslog enthält die Datenbankdatei nur die Aufzeichnungen der Änderungen nach der letzten Sicherung und den jüngsten Checkpoint.
2. Löschen Sie die Transaktionslogdatei oder benennen Sie sie um.
3. Starten Sie die Datenbank von Neuem mit der Option `-f`.

```
dbeng16 "database-name.db" -f
```

Ohne die Option `-f` meldet der Datenbankserver das Fehlen des Transaktionslogs als Fehler. Mit der Option `-f` stellt der Datenbankserver die Datenbank bis zum letzten Checkpoint wieder her und setzt alle Transaktionen zurück, die zum Zeitpunkt dieses Checkpoints nicht festgeschrieben waren. Ein neues Transaktionslog wird erstellt.

### Ergebnisse

Die Datenbank wird teilweise wiederhergestellt. Transaktionen, die zum Zeitpunkt des letzten Checkpoints nicht festgeschrieben waren, werden zurückgesetzt.

### Siehe auch

- „Transaktionslog-Spiegeldateien“ auf Seite 138
- „Das Transaktionslog“ auf Seite 135
- „Der Prozess der automatischen Wiederherstellung“ auf Seite 1047
- „Nicht festgeschriebene Vorgänge wiederherstellen (Sybase Central)“ auf Seite 1048
- „Datenbankserver-Wiederherstellungsoption `-f`“ auf Seite 234

## Entwerfen von Sicherungs- und Wiederherstellungsplänen

Es wird empfohlen, dass Sie eine Sicherungsplanung entwickeln und einführen, um Ihre Daten zu schützen. Ihre Sicherungs- und Wiederherstellungsbefehle sollten außerdem im Rahmen Ihres Sicherungs- und Wiederherstellungsplans getestet werden.

Folgende Faktoren sollten Sie bei der Entwicklung Ihres Sicherungs- und Wiederherstellungsplans in die Überlegungen einbeziehen:

- Wo befinden sich die Datenbankdateien?
- Welche Dateien müssen gesichert werden?
- Wo werden die Sicherungsdateien gespeichert?
- Wie beeinflusst die Sicherung die Performance Ihrer Datenbank oder Ihrer Anwendungen?
- Läuft der Datenbankserver, während Sie die Sicherung durchführen?

Die häufigsten Fälle für die Notwendigkeit der Wiederherstellung aus Datenbanksicherungen sind:

- Datenträgerfehler
- Hardwarefehler
- Dateibeschädigung

In der Regel wird für eine Sicherung eine Kombination aus vollständigen und inkrementellen Sicherungen verwendet. Wie häufig Sie die einzelnen Sicherungsarten verwenden, hängt von den Daten ab, die Sie schützen wollen. Sie sollten Ihre Sicherungen auch validieren, um sicherzustellen, dass sie für die Wiederherstellung verwendet werden können. Siehe [„Sicherungsvalidierung“ auf Seite 1045](#).

Sie können die Funktionen für die Abfolgeplanung in SQL Anywhere verwenden, um die Sicherungen der Datenbank zu automatisieren. Nachdem Sie die Abfolgeplanung erstellt haben, werden die Sicherungen vom Datenbankserver automatisch durchgeführt. Siehe [„Aufgabenautomatisierung mit Abfolgeplanung und Ereignissen“ auf Seite 1087](#) und [„Wartungspläne“ auf Seite 1064](#).

Die maximal zulässige Wiederherstellungszeit richtet sich danach, wie lange Ihr Unternehmen funktionieren kann, ohne Zugang zu den Daten in der Datenbank zu haben.

Sie müssen feststellen, ob die von Ihnen eingerichteten Schutzmaßnahmen Sie gegen Ausfälle der Datenbankdatei und der Transaktionslogdatei ausreichend absichern. Wenn Sie eine Replikationsumgebung aufgebaut haben, ist ein Transaktionslogspiegel zu empfehlen. Siehe [„Datenträgerfehler“ auf Seite 1067](#).

Externe Faktoren wie die verfügbare Hardware, die Größe der Datenbankdateien, die Datenträger für die Wiederherstellung, der Festplattenspeicher und unerwartete Störungen können die Wiederherstellungszeit beeinflussen. Wenn Sie eine Sicherungsstrategie planen, müssen Sie zusätzliche Wiederherstellungszeit für diverse andere Aufgaben einplanen, etwa die Eingabe der Wiederherstellungsbefehle oder das Heraussuchen und Laden von Bändern.

### Siehe auch

- „Sicherungskomponenten“ auf Seite 1076
- „Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung“ auf Seite 1068
- „Einschränkungen für die Sicherung und Wiederherstellung von Daten“ auf Seite 1036
- „Arten der Datensicherung“ auf Seite 1029
- „Sicherungsformate“ auf Seite 1033
- „Vollständige Sicherungen erstellen“ auf Seite 1030
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031

## Sicherungs- und Wiederherstellungsplan entwerfen

Implementieren Sie einen Sicherungs- und Wiederherstellungsplan, um den Verlust von Daten bei einem Ausfall der Datenbank zu minimieren.

### Voraussetzungen

Sie müssen die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT haben.

### Aufgabe

1. Erstellen und prüfen Sie Ihre Sicherungs- und Wiederherstellungsbefehle, einschließlich der Befehle für die Datenbankvalidierung.
2. Messen Sie, wie lange es dauert, die Sicherungs- und Wiederherstellungsbefehle auszuführen.
3. Dokumentieren Sie die Sicherungsbefehle und erstellen Sie schriftliche Verfahrensbeschreibungen, in denen festgehalten wird, wo sich die Sicherungen befinden. Diese Verfahrensbeschreibungen müssen auch Namenskonventionen und die Arten der durchgeführten Sicherungen enthalten.
4. Richten Sie die Sicherungsprozeduren auf dem Produktionsserver ein.
5. Überwachen Sie die Sicherungsprozeduren, um unerwarteten Fehlern vorzubeugen. Achten Sie darauf, dass Änderungen in der Vorgehensweise auch dokumentiert werden.

### Ergebnisse

Der Sicherungs- und Wiederherstellungsplan wird implementiert.

**Siehe auch**

- „Sicherungsvalidierung“ auf Seite 1045
- „Vollständige Sicherungen erstellen“ auf Seite 1030
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031
- „Sicherungskomponenten“ auf Seite 1076
- „Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung“ auf Seite 1068
- „Einschränkungen für die Sicherung und Wiederherstellung von Daten“ auf Seite 1036
- „Arten der Datensicherung“ auf Seite 1029
- „Sicherungsformate“ auf Seite 1033

## Zeitpläne für Sicherungen

In der Regel wird für eine Sicherung eine Kombination aus vollständigen und inkrementellen Sicherungen verwendet. Wie häufig Sie Sicherungen erstellen, hängt von vielen Faktoren ab, etwa von der Wichtigkeit der Daten und der Häufigkeit ihrer Veränderung.

Oft beginnt man den Sicherungsplan, indem man einmal pro Woche eine vollständige Sicherung vornimmt, und täglich eine inkrementelle Sicherung des Transaktionslogs. Vollständige und inkrementelle Sicherungen können online (bei laufender Datenbank) oder offline, serverseitig oder clientseitig durchgeführt werden.

Vor welchen Arten von Ausfällen ein Sicherungszeitplan schützt, hängt nicht nur von der Häufigkeit der geplanten Sicherungen ab, sondern auch davon, wie Ihr Datenbankserver betrieben wird.

Bewahren Sie mehr als eine vollständige Sicherung auf. Sie sollten Ihre vollständigen Sicherungen auch außerhalb der Betriebsräume aufbewahren, damit sie vor Feuer, Hochwasser, Erdbeben, Diebstahl oder Vandalismus geschützt sind.

Sie können die Funktionen von SQL Anywhere für die Ereignisplanung benutzen, um Online-Sicherungen automatisch zu feststehenden Zeiten durchzuführen.

**Vorsicht**

Wenn Sie die letzte Sicherung überschreiben und während der Sicherung ein Datenträgerfehler auftritt, haben Sie überhaupt keine Sicherung mehr.

**Siehe auch**

- „Wartungspläne“ auf Seite 1064

## Wartungspläne

Um die Verwaltung zu vereinfachen, können Sie einen Wartungsplan für Ihre Datenbank einrichten, der vom Datenbankserver automatisch ausgeführt wird. Ein Wartungsplan besteht aus einer Abfolgeplanung zur Durchführung einer der folgenden Aufgaben:

- Die Datenbank validieren
- Die Datenbank sichern
- Wartungsplanberichte verwalten

In Sybase Central erstellen Sie einen Wartungsplan, indem Sie den **Assistenten zum Erstellen von Wartungsplänen** verwenden. Es kann immer nur eine Instanz eines Wartungsplans ausgeführt werden. Nach jedem Ausführen des Wartungsplans wird ein Wartungsplanbericht in der Datenbank gespeichert. Sie können diesen Bericht in Sybase Central anzeigen oder sich den Wartungsplanbericht per E-Mail jedesmal zusenden lassen, wenn der Wartungsplan in der Datenbank ausgeführt wurde.

🔥 **Cloud-Hinweis:** Diese Funktion wird auf Tenant-Datenbanken in der Cloud nicht unterstützt.

### Wartungspläne anpassen

Wartungspläne können benutzerdefinierte Vorgänge enthalten. Im **Assistenten zum Erstellen von Wartungsplänen** können Sie benutzerdefinierte Vorgänge als SQL-Anweisungen hinzufügen, die vor der Validierung oder nach der Sicherung ausgeführt werden.

### Einführung in den Wartungsplanstatus

Wenn ein Wartungsplan ausgeführt wird, wird sein Status im Ordner **Wartungspläne** in Sybase Central angezeigt. Ein laufender Wartungsplan hat einen der folgenden Status:

- **Initialisierung läuft** Neue Verbindungen werden gesperrt und aktuelle Benutzer werden getrennt.
- **Vorvalidierung wird ausgeführt** Benutzerdefinierte Vorgänge (wenn solche bei der Erstellung des Wartungsplans geplant wurden) werden durchgeführt.
- **Seiten werden validiert** Zeigt den Status der Validierung der Datenbankseiten.
- **Objekte werden validiert** Gibt den Status der Validierung von Tabellen materialisierten Ansichten und Indizes an.
- **Sicherung läuft** Zeigt den Fortschritt der Sicherung.
- **Nachverarbeitung nach der Sicherung wird ausgeführt** Benutzerdefinierte Vorgänge (wenn solche bei der Erstellung des Wartungsplans geplant wurden) werden durchgeführt.
- **Vorgang wird beendet** Neue Verbindungen werden zugelassen, Bericht wird gespeichert, entfernt und per E-Mail versendet.

### Wartungspläne erstellen

Erstellen Sie einen Wartungsplan mit Sybase Central.

## Voraussetzungen

Zum Erstellen eines Wartungsplans benötigen Sie entweder das SELECT ANY TABLE-Systemprivileg oder das SELECT-Privileg für die folgenden Tabellen:

- dbo.maint\_plan
- dbo.maint\_plan\_report
- dbo.maint\_plan\_status

Außerdem müssen Sie das MANAGE ANY EVENT-Systemprivileg und entweder das INSERT ANY TABLE-Systemprivileg oder das INSERT-Privileg für die maint\_plan-Tabelle haben.

Wenn Sie diese Aufgabe zum ersten Mal ausführen oder wenn seit dem letzten Zugriff auf die Wartungspläne ein Upgrade der Datenbank durchgeführt wurde, werden Sie mit einer Fehlermeldung darauf hingewiesen, dass die Wartungsplantabellen erstellt bzw. aktualisiert werden müssen. Zum Erstellen oder Aktualisieren dieser Tabellen benötigen Sie das SELECT ANY TABLE-Systemprivileg sowie entweder das CREATE ANY OBJECT-Systemprivileg oder die Systemprivilegien CREATE ANY INDEX und CREATE ANY TABLE. Klicken Sie auf den Ordner **Wartungspläne**, um die Tabellen zu erstellen oder zu aktualisieren.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Wartungspläne** und klicken Sie auf **Neu » Wartungsplan**.
3. Befolgen Sie die Anweisungen des Assistenten.

## Ergebnisse

Ein Wartungsplan wird erstellt.

## Siehe auch

- „Zeitplandefinition“ auf Seite 1090
- „VALIDATE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Arten der Datensicherung“ auf Seite 1029
- „xp\_startsmtp-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Archivsicherungen“ auf Seite 1034
- „Sicherungskopien“ auf Seite 1035
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031
- „Wartungspläne“ auf Seite 1064

## Wartungsplanberichte anzeigen

Wartungsplanberichte in Sybase Central anzeigen

### Voraussetzungen

Zum Anzeigen eines Wartungsplanberichts benötigen Sie entweder das SELECT ANY TABLE-Systemprivileg oder das SELECT-Privileg für die folgenden Tabellen:

- dbo.maint\_plan
- dbo.maint\_plan\_report
- dbo.maint\_plan\_status

Wenn seit dem letzten Zugriff auf die Wartungspläne ein Upgrade der Datenbank durchgeführt wurde, werden Sie mit einer Fehlermeldung darauf hingewiesen, dass die Wartungsplantabellen aktualisiert werden müssen. Zum Aktualisieren dieser Tabellen benötigen Sie das SELECT ANY TABLE-Systemprivileg sowie entweder das CREATE ANY OBJECT-Systemprivileg oder die Systemprivilegien CREATE ANY INDEX und CREATE ANY TABLE. Klicken Sie auf den Ordner **Wartungspläne**, um die Tabellen zu aktualisieren.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Wartungspläne**.
3. Doppelklicken Sie auf Ihren Wartungsplan.
4. Im rechten Fensterausschnitt doppelklicken Sie auf den Report.

### Ergebnisse

Das Fenster **Wartungsplan-Eigenschaften** wird eingeblendet. Der Fensterabschnitt **Details** enthält das Log für den Wartungsplan.

### Siehe auch

- „Archivsicherungen“ auf Seite 1034
- „Sicherungskopien“ auf Seite 1035
- „Inkrementelle Sicherungen erstellen“ auf Seite 1031
- „Wartungspläne“ auf Seite 1064

### Wartungspläne löschen

Löschen Sie einen Wartungsplan mithilfe von Sybase Central.

## Voraussetzungen

Zum Löschen eines Wartungsplans benötigen Sie entweder das SELECT ANY TABLE-Systemprivileg oder das SELECT-Privileg für die folgenden Tabellen:

- dbo.maint\_plan
- dbo.maint\_plan\_report
- dbo.maint\_plan\_status

Außerdem müssen Sie das MANAGE ANY EVENT-Systemprivileg und entweder das DELETE ANY TABLE-Systemprivileg oder das DELETE-Privileg für die maint\_plan-Tabelle haben.

Wenn seit dem letzten Zugriff auf die Wartungspläne ein Upgrade der Datenbank durchgeführt wurde, werden Sie mit einer Fehlermeldung darauf hingewiesen, dass die Wartungsplantabellen aktualisiert werden müssen. Zum Aktualisieren dieser Tabellen benötigen Sie das SELECT ANY TABLE-Systemprivileg sowie entweder das CREATE ANY OBJECT-Systemprivileg oder die Systemprivilegien CREATE ANY INDEX und CREATE ANY TABLE. Klicken Sie auf den Ordner **Wartungspläne**, um die Tabellen zu aktualisieren.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **Wartungspläne**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf den Wartungsplan und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

## Ergebnisse

Der Wartungsplan wird gelöscht.

## Siehe auch

- „Wartungspläne“ auf Seite 1064

## Datenträgerfehler

Sicherungen schützen Ihre Daten gegen Datenträgerfehler.

Wenn Sie eine Datenbank erstellen, wird das Transaktionslog standardmäßig auf demselben Datenträger und in demselben Verzeichnis gespeichert wie die Datenbankdatei. Diese Anordnung schützt nicht gegen Datenträgerfehler und Sie sollten daher überlegen, das Transaktionslog für Ihre Produktionsdatenbank an einem anderen Standort unterzubringen.

**Datenträgerfehler, die die Datenbankdatei betreffen** Wenn Ihre Datenbankdatei nicht mehr benutzbar ist, das Transaktionslog hingegen schon, können Sie alle festgeschriebenen Änderungen der Datenbank wiederherstellen, sofern Sie eine regelmäßige Datenbanksicherung durchgeführt haben. Alle

Daten, die seit der letzten Datenbanksicherung durchgeführt wurden, befinden sich in gesicherten Transaktionslogs oder im gerade aktuellen Transaktionslog.

**Datenträgerfehler, die die Transaktionslogdatei betreffen** Wenn Sie keinen Transaktionslogspegel verwenden, können Sie die geänderten Daten zwischen dem letzten Datenbank-Checkpoint und dem Datenträgerausfall, der das Transaktionslog betrifft, nicht wiederherstellen. Aus diesem Grund wird empfohlen, unter bestimmten Umständen, beispielsweise bei konsolidierten Datenbanken in einer SQL Remote-Umgebung, einen Transaktionslogspegel zu verwenden, damit der Verlust des Transaktionslogs nicht zum Verlust wichtiger Daten oder zum Zusammenbruch eines Replikationssystems führt.

Wie schnell Sie nach einem Datenträgerfehler eine Wiederherstellung vornehmen können, hängt davon ab, ob der Datenträgerfehler die Datenbankdatei oder die Transaktionslogdatei betrifft.

Für eine umfassende Wiederherstellung nach einem Datenträgerfehler sollten Sie das Transaktionslog nicht auf demselben Medium unterbringen wie die Datenbankdatei. Manche Computer mit zwei oder drei Festplatten haben eigentlich nur eine physische Festplatte, die in mehrere logische Laufwerke oder Partitionen aufgeteilt ist: Wenn Sie einen zuverlässigen Schutz gegen einen Datenträgerausfall benötigen, müssen Sie einen Computer verwenden, der mindestens zwei physische Speichermedien hat.

Wenn Sie das Transaktionslog auf einem separaten Speichermedium unterbringen, kann dies die Performance verbessern, weil in diesem Fall die Bewegung des Lesekopfes zwischen Transaktionslog und Haupt-Datenbankdatei vermieden wird.

### **Vorsicht**

Das Transaktionslog sollte nicht in einem Netzwerkverzeichnis untergebracht werden. Das Lesen und Schreiben von Seiten über ein Netzwerk führt zu einer Verschlechterung der Performance und kann Dateibeschädigungen verursachen.

### **Siehe auch**

- „Datenbankerstellung“ auf Seite 121
- „Speicherorte von Transaktionslogs ändern (Sybase Central)“ auf Seite 136
- „Speicherorte von Transaktionslogs ändern (Befehlszeile)“ auf Seite 137

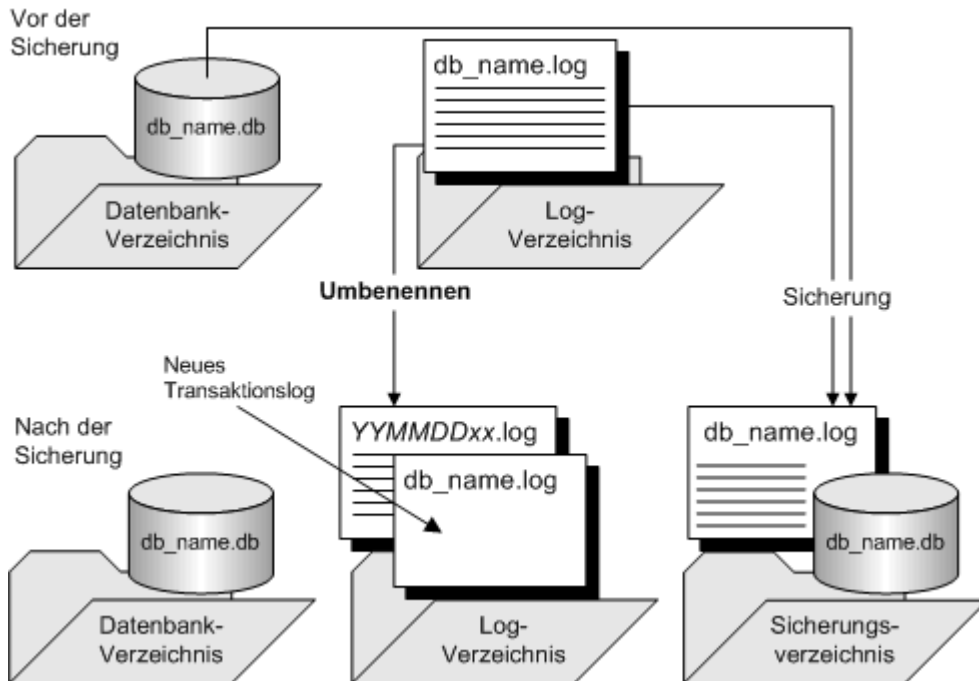
## **Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung**

Wenn Ihre Datenbank Teil einer SQL Remote-Installation ist, muss der Nachrichtenagent Zugriff auf alte Transaktionen haben. Wenn es sich um eine konsolidierte Datenbank handelt, enthält sie die Masterkopie der kompletten SQL Remote-Installation, und daher sind sorgfältige Sicherungsprozeduren von besonderer Bedeutung, damit garantiert keine Daten verlorengehen.

Wenn Ihre Datenbank Teil eines MobiLink-Systems ist, in dem dbmlsync verwendet wird, gelten dieselben Hinweise. Wenn allerdings Ihre Datenbank eine konsolidierte MobiLink-Datenbank ist, sind alte Transaktionslogs nicht nötig.

Für Synchronisations- und Replikationsumgebungen können Sie Sicherungsoptionen wählen, um das Transaktionslog umzubenennen und neu zu starten. Diese Art der Sicherung schützt vor einem grenzenlosen Wachsen des Transaktionslogs, während Informationen über alte Transaktionen bewahrt bleiben.

Diese Art der Sicherung wird in der nachfolgenden Darstellung gezeigt.



Weitere Hinweise finden Sie unter [„Transaktionslogs umbenennen oder kürzen \(Sybase Central\)“](#) auf Seite 1070.

Sicherungsprozeduren sind in den entfernten Datenbanken weniger wichtig als in der konsolidierten Datenbank. Sie könnten sich auf die Replikation in die konsolidierte Datenbank als Methode zur Datensicherung verlassen. Im Fall eines Datenträgerfehlers würde die entfernte Datenbank aus der konsolidierten Datenbank extrahiert, und dabei würden nur alle jene Vorgänge, die nicht repliziert wurden, verloren gehen. Sie könnten das Dienstprogramm zur Logkonvertierung verwenden, um zu versuchen, die verloren gegangenen Vorgänge wieder herzustellen. Siehe [„Dienstprogramm zur Logkonvertierung \(dbtran\)“](#) auf Seite 948.

Auch wenn Sie sich auf die Replikation verlassen, um entfernte Datenbankdaten zu schützen, müssen trotzdem Sicherungen an entfernten Datenbanken regelmäßig durchgeführt werden, um zu verhindern, dass das Transaktionslog zu groß wird. Sie sollten dieselbe Option (das Log umbenennen und neu starten) wie in der konsolidierten Datenbank verwenden, indem Sie den Nachrichtenagenten so ausführen, dass er Zugriff auf die umbenannten Logdateien hat. Wenn Sie in der entfernten Datenbank die Option `delete_old_logs` auf `On` setzen, werden die alten Logdateien automatisch vom Nachrichtenagenten gelöscht, wenn sie nicht mehr benötigt werden. Siehe [„delete\\_old\\_logs-Option \[SQL Remote\]“](#) auf Seite 607.

### Automatisches Umbenennen des Transaktionslogs in SQL Remote

Verwenden Sie die Option -x des Nachrichtenagenten, damit das Transaktionslog auf dem entfernten Computer nicht umbenannt werden muss, wenn der Datenbankserver heruntergefahren wird. Mit der Option -x wird das Transaktionslog umbenannt, nachdem es nach zu versendenden Nachrichten durchsucht wurde. Siehe „[SQL Remote-Nachrichtenagent-Dienstprogramm \(dbremote\)](#)“ [[SQL Remote](#)].

## Transaktionslog-Verwaltung

### Transaktionslogs umbenennen oder kürzen (Sybase Central)

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, benennen Sie das Transaktionslog um, um ein neues Transaktionslog für die Datenbank zu erstellen. Wenn Ihre Datenbank nicht in eine Replikationsumgebung eingebunden ist und nur begrenzt Festplattenspeicher auf dem Computer zur Verfügung steht, kürzen Sie das Transaktionslog.

#### Voraussetzungen

Sie müssen das BACKUP DATABASE-Privileg haben.

#### Kontext und Bemerkungen

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, empfiehlt es sich, Kopien der alten Transaktionslogs aufzubewahren, bis Sie sicher sind, dass sie nicht mehr benötigt werden. Als Alternative zum Umbenennen des Transaktionslogs können Sie auch weiterhin mit dem vorhandenen Transaktionslog arbeiten, wenn Sie Ihre Datenbank sichern.

Wenn Sie das Transaktionslog während der Sicherung kürzen, um den Inhalt des Online-Transaktionslogs zu löschen, müssen Sie für die Wiederherstellung Ihrer Datenbank nach einem Datenträgerfehler, der die Datenbankdatei betroffen hat, alle Sicherungskopien verwenden, die seit der letzten vollständigen Sicherung erstellt wurden.

#### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Sicherungskopie erstellen**.
3. Befolgen Sie die Anweisungen im **Assistenten zum Erstellen einer Sicherungskopie**.

Option	Aktion
Transaktionslog umbenennen	Klicken Sie in der Liste <b>Was wollen Sie mit dem Transaktionslog tun?</b> auf <b>Transaktionslog umbenennen</b> .
Transaktionslog kürzen	Klicken Sie in der Liste <b>Was wollen Sie mit dem Transaktionslog tun?</b> auf <b>Transaktionslog kürzen</b> .

## Ergebnisse

Eine Sicherung wird erstellt und das Transaktionslog wird umbenannt bzw. gekürzt.

### Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Das Transaktionslog“ auf Seite 135
- „Datenbankwiederherstellung“ auf Seite 1046

## Transaktionslogs umbenennen oder kürzen (SQL)

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, benennen Sie das Transaktionslog um, um ein neues Transaktionslog für die Datenbank zu erstellen. Wenn Ihre Datenbank nicht in eine Replikationsumgebung eingebunden ist und nur begrenzt Festplattenspeicher auf dem Computer zur Verfügung steht, kürzen Sie das Transaktionslog.

### Voraussetzungen

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

### Kontext und Bemerkungen

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, empfiehlt es sich, Kopien der alten Transaktionslogs aufzubewahren, bis Sie sicher sind, dass sie nicht mehr benötigt werden. Als Alternative zum Umbenennen des Transaktionslogs können Sie auch weiterhin mit dem vorhandenen Transaktionslog arbeiten, wenn Sie Ihre Datenbank sichern.

Wenn Sie das Transaktionslog während der Sicherung kürzen, um den Inhalt des Online-Transaktionslogs zu löschen, müssen Sie für die Wiederherstellung Ihrer Datenbank nach einem Datenträgerfehler, der die Datenbankdatei betroffen hat, alle Sicherungskopien verwenden, die seit der letzten vollständigen Sicherung erstellt wurden.

### Aufgabe

- Verwenden Sie die BACKUP-Anweisung mit den folgenden Klauseln:

Option	Aktion
Transaktionslog umbenennen	<code>BACKUP DATABASE DIRECTORY backup-directory [ TRANSACTION LOG ONLY ] TRANSACTION LOG RENAME;</code>
Transaktionslog kürzen	<code>BACKUP DATABASE DIRECTORY backup-directory [ TRANSACTION LOG ONLY ] TRANSACTION LOG TRUNCATE;</code>

Fügen Sie die Klausel TRANSACTION LOG ONLY nur dann ein, wenn Sie eine inkrementelle Sicherung durchführen.

Die Sicherungskopien des Transaktionslogs und der Datenbankdatei werden in das *backup-directory* geschrieben. Wenn Sie einen Verzeichnispfad angeben, bezieht er sich auf das Arbeitsverzeichnis des Datenbankservers, nicht der Clientanwendung.

### Ergebnisse

Eine Sicherung wird erstellt und das Transaktionslog wird umbenannt bzw. gekürzt.

### Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Das Transaktionslog“ auf Seite 135
- „Datenbankwiederherstellung“ auf Seite 1046

## Transaktionslogs umbenennen oder kürzen (Befehlszeile)

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, benennen Sie das Transaktionslog um, um ein neues Transaktionslog für die Datenbank zu erstellen. Wenn Ihre Datenbank nicht in eine Replikationsumgebung eingebunden ist und nur begrenzt Festplattenspeicher auf dem Computer zur Verfügung steht, kürzen Sie das Transaktionslog.

### Voraussetzungen

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

### Kontext und Bemerkungen

Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, empfiehlt es sich, Kopien der alten Transaktionslogs aufzubewahren, bis Sie sicher sind, dass sie nicht mehr benötigt werden. Als Alternative zum Umbenennen des Transaktionslogs können Sie auch weiterhin mit dem vorhandenen Transaktionslog arbeiten, wenn Sie Ihre Datenbank sichern.

Wenn Sie das Transaktionslog während der Sicherung kürzen, um den Inhalt des Online-Transaktionslogs zu löschen, müssen Sie für die Wiederherstellung Ihrer Datenbank nach einem Datenträgerfehler, der die Datenbankdatei betroffen hat, alle Sicherungskopien verwenden, die seit der letzten vollständigen Sicherung erstellt wurden.

### Aufgabe

- Führen Sie den folgenden Befehl aus:

Option	Aktion
Transaktionslog umbenennen	<code>dbbackup -c "connection-string" -r [ -t ] backup-directory</code>
Transaktionslog kürzen	<code>dbbackup -c "connection-string" -x [ -t ] backup-directory</code>

Geben Sie die Option -t nur an, wenn eine inkrementelle Sicherung durchgeführt werden soll.

Die Sicherungskopien des Transaktionslogs und der Datenbankdatei werden in das *backup-directory* geschrieben. Wenn Sie einen Verzeichnispfad angeben, bezieht er sich auf das Verzeichnis, aus dem der Befehl ausgeführt wird.

## Ergebnisse

Eine Sicherung wird erstellt und das Transaktionslog wird umbenannt bzw. gekürzt.

## Siehe auch

- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Das Transaktionslog“ auf Seite 135
- „Datenbankwiederherstellung“ auf Seite 1046

## Sicherungskopien von Transaktionslogs während einer Sicherung umbenennen (SQL)

Verwenden Sie die BACKUP-Anweisung, um die Sicherungskopie des Transaktionslogs umzubenennen, die standardmäßig denselben Namen hat wie die Online-Datei. Sie können einen wiederholbaren Befehl für eine inkrementelle Sicherung erstellen, indem Sie die Sicherungskopie des Transaktionslogs umbenennen.

### Voraussetzungen

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

### Kontext und Bemerkungen

Alternativ können Sie die Sicherungskopie des Transaktionslogs verschieben, statt sie umzubenennen.

Die Sicherungskopie des Transaktionslogs wird wie folgt benannt: *JJMMTTxx.log*. Dabei gilt: *JJ* ist das Jahr, *MM* der Monat, *TT* der Tag des Monats und *xx* eine Buchstabenfolge von AA bis ZZ, die inkrementiert wird, wenn mehr als eine Sicherung pro Tag erfolgt. Die Dateinamen *JJMMTTxx.log* werden verwendet, um die Dateien unterscheiden zu können, nicht zur Sortierung.

Diese Sicherungsoptionen werden in der Regel bei Datenbanken verwendet, die in eine Replikationsumgebung eingebunden sind. In diesem Fall werden nicht nur Sicherungskopien der Datenbankdatei und des Transaktionslogs hergestellt, sondern das Transaktionslog wird zum Sicherungszeitpunkt in ein Offline-Transaktionslog umbenannt und ein neues Transaktionslog wird gestartet, das den Namen des bisher aktiven Transaktionslogs übernimmt.

### Aufgabe

- Benutzen Sie das Schlüsselwort MATCH in der BACKUP-Anweisung. Beispiel: Mit der folgenden Anweisung wird das Transaktionslog inkrementell im Verzeichnis *c:\backup* gesichert. Die Sicherungskopie des Transaktionslogs wird wie folgt benannt: *JJMMTTxx.log*. Dabei gilt: *JJMMTT* ist das Datum und *xx* eine fortlaufende Buchstabenfolge, beginnend mit AA.

```
BACKUP DATABASE
DIRECTORY 'c:\backup'
```

```
TRANSACTION LOG ONLY  
TRANSACTION LOG RENAME MATCH;
```

### Ergebnisse

Die Sicherungskopie des Transaktionslogs wird umbenannt.

### Siehe auch

- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Transaktionslogs umbenennen oder kürzen (Befehlszeile)“ auf Seite 1072
- „Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung“ auf Seite 1068
- „Das Transaktionslog“ auf Seite 135
- „Datenbankwiederherstellung“ auf Seite 1046

## Sicherungskopien von Transaktionslogs während einer Sicherung umbenennen (Befehlszeile)

Verwenden Sie das Dienstprogramm dbbackup, um die Sicherungskopie des Transaktionslogs umzubenennen, die standardmäßig denselben Namen hat wie die Online-Datei. Sie können einen wiederholbaren Befehl für eine inkrementelle Sicherung erstellen, indem Sie die Sicherungskopie des Transaktionslogs umbenennen.

### Voraussetzungen

Sie müssen das BACKUP DATABASE-Systemprivileg haben.

### Kontext und Bemerkungen

Alternativ können Sie die Sicherungskopie des Transaktionslogs verschieben, statt sie umzubenennen.

Die Sicherungskopie des Transaktionslogs wird wie folgt benannt: *JJMMTTxx.log*. Dabei gilt: *JJ* ist das Jahr, *MM* der Monat, *TT* der Tag des Monats und *xx* eine Buchstabenfolge von AA bis ZZ, die inkrementiert wird, wenn mehr als eine Sicherung pro Tag erfolgt. Die Dateinamen *JJMMTTxx.log* werden verwendet, um die Dateien unterscheiden zu können, nicht zur Sortierung.

Diese Serie von Sicherungsoptionen wird in der Regel bei Datenbanken verwendet, die in ein Replikationssystem eingebunden sind. In diesem Fall werden nicht nur Sicherungskopien der Datenbankdatei und des Transaktionslogs hergestellt, sondern das Transaktionslog wird zum Sicherungszeitpunkt in ein Offline-Log umbenannt und ein neues Transaktionslog wird gestartet, das den Namen des bisher aktiven Transaktionslogs übernimmt.

### Aufgabe

- Geben Sie die Option -n für dbbackup an. Beispiel: Der folgende Befehl führt eine inkrementelle Sicherung der Beispieldatenbank durch und benennt die Sicherungskopie des Transaktionslogs um.

```
dbbackup -c "connection-string" -r -t -n c:\backup-name
```

## Ergebnisse

Die Sicherungskopie des Transaktionslogs wird umbenannt.

### Siehe auch

- [„Sicherungsdienstprogramm \(dbbackup\)“ auf Seite 886](#)
- [„Sicherungskopien von Transaktionslogs während einer Sicherung umbenennen \(SQL\)“ auf Seite 1073](#)
- [„Sicherungen von Datenbanken in einer Synchronisations- und Replikationsumgebung“ auf Seite 1068](#)
- [„Das Transaktionslog“ auf Seite 135](#)
- [„Datenbankwiederherstellung“ auf Seite 1046](#)

## Transaktionslog-Validierung

Wenn eine Datenbank mit Transaktionslogspiegelung gestartet wird, führt der Datenbankserver eine Reihe von Prüfungen und automatischen Vorgängen für die Wiederherstellung durch, um zu bestätigen, dass das Transaktionslog und dessen Spiegelung nicht beschädigt sind, sowie um bestimmte Probleme zu beheben, falls eine Beschädigung festgestellt wird.

Beim Starten prüft der Server, ob das Transaktionslog und dessen Spiegelung identisch sind, indem er beide Dateien vollständig vergleicht. Wenn sie identisch sind, starten die Datenbanken wie üblich. Der Vergleich von Log und Spiegelung verlängert die Startzeit der Datenbank.

Wenn die Datenbank wegen eines Systemausfalls gestoppt wird, ist es möglich, dass einige Vorgänge in das Transaktionslog geschrieben wurden, jedoch nicht in die Spiegelung. Wenn der Server feststellt, dass das Transaktionslog und die Spiegelung bis zum Ende der kürzeren Datei identisch sind, wird der Rest der längeren Datei in die kürzere Datei kopiert. Dadurch sind Log und Spiegelung wieder identisch. Nach diesem automatischen Wiederherstellungsschritt startet der Server wie üblich.

Wenn sich bei der Prüfung herausstellt, dass das Transaktionslog und der Transaktionslogspiegel im Hauptteil Unterschiede aufweisen, ist eine der Dateien beschädigt. In diesem Fall wird die Datenbank nicht gestartet und eine Fehlermeldung mit dem Hinweis ausgegeben, dass das Transaktionslog oder dessen Spiegelung ungültig ist.

Sie können auch das Dienstprogramm zur Logkonvertierung (dbtran) verwenden, um Transaktionslogs zu validieren, unabhängig davon, ob Sie ein Online- oder Offline-Transaktionslog verwenden. Wenn das Dienstprogramm zur Logkonvertierung die Logdatei lesen kann, ist sie gültig.

### Siehe auch

- [„Dienstprogramm zur Logkonvertierung \(dbtran\)“ auf Seite 948](#)

## Der interne Sicherungsvorgang

Wenn Sie eine Sicherung durchführen, arbeiten vielleicht noch andere Benutzer in der Datenbank. Wenn Sie Ihre Datenbank von einer Sicherung wiederherstellen wollen, müssen Sie wissen, welche Daten gesichert wurden und welche nicht.

Folgende Schritte führt ein Datenbankserver während der Sicherung aus:

1. Er setzt einen Checkpoint. Bis zum Abschluss der Sicherung können keine weiteren Checkpoints gesetzt werden.
2. Er führt eine Sicherung der Datenbankdateien durch, wenn eine vollständige Sicherung erstellt wird.
3. Er führt eine Sicherung des Transaktionslogs durch.

Die Sicherung enthält alle Vorgänge, die im Transaktionslog vor dem Lesen der letzten Seite des Logs verzeichnet wurden. Dies kann Anweisungen einbeziehen, die nach dem Start der Sicherung eingeleitet wurden.

Die Sicherungskopie des Transaktionslogs ist in der Regel kleiner als das Online-Transaktionslog. Der Datenbankserver weist den Online-Transaktionslogs Speicherblöcke von jeweils 64 kB zu, sodass die Transaktionslogdatei in der Regel leere Seiten enthält. Allerdings werden nur die nicht leeren Seiten gesichert.

4. Der Datenbankserver markiert das Sicherungsabbild der Datenbank, um anzuzeigen, dass eine Wiederherstellung erforderlich ist. Bei diesem Schritt werden alle Vorgänge, die seit dem Start der Sicherungen ausgeführt wurden, angewendet, sobald die Sicherungskopie der Datenbank gestartet wurde. Außerdem sorgt dies dafür, dass Vorgänge, die zum Zeitpunkt des Checkpoints nicht abgeschlossen waren, zurückgesetzt werden, wenn sie nicht festgeschrieben wurden.

## Sicherungskomponenten

Wenn eine Datenbank ordnungsgemäß heruntergefahren wird, enthält die Datenbankdatei den kompletten und aktuellen Stand aller Daten, die darin gespeichert wurden. Bei laufender Datenbank ist die Datenbankdatei hingegen nicht immer aktuell bzw. unvollständig.

Der einzige Zeitpunkt, zu dem eine Datenbankdatei garantiert eine komplette und aktuelle Version aller Daten enthält, ist unmittelbar nach dem Ausführen eines Checkpoints. Nachdem ein Checkpoint gesetzt wurde, befindet sich der Inhalt des Datenbankcaches auf der Festplatte.

Der Datenbankserver setzt in einer Datenbank unter folgenden Bedingungen einen Checkpoint:

- Als Teil des Verfahrens zum Herunterfahren einer Datenbank
- Wenn das Zeitintervall seit dem letzten Checkpoint die Einstellung der Serveroption `-gc` überschreitet.
- Wenn die geschätzte Zeit zur Wiederherstellung die Einstellung der Serveroption `-gr` überschreitet.
- Wenn der Server lange genug inaktiv ist, um alle nicht festgeschriebenen Seiten (Dirty Pages) zu schreiben
- Wenn bestimmte DDL-Anweisungen (wie `ALTER TABLE`, `DROP TABLE`, `DROP INDEX`, `LOAD TABLE` oder `BACKUP`) ausgeführt werden.
- Wenn eine Verbindung eine `CHECKPOINT`-Anweisung veranlasst

- Wenn der Server ohne Transaktionslog läuft und eine Transaktion festgeschrieben wird

Um sicherzustellen, dass Sie eine vollständige Kopie aller festgeschriebenen Transaktionen zwischen Checkpoints haben, benötigen Sie die Datenbankdatei und das Transaktionslog.

#### Siehe auch

- „Checkpoint-Logs“ auf Seite 143
- „Einschränkungen für die Sicherung und Wiederherstellung von Daten“ auf Seite 1036
- „So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist“ auf Seite 1077
- „Datenbankserveroption -gc “ auf Seite 239
- „Datenbankserveroption -gr “ auf Seite 249

## So entscheidet die Datenbank, wann ein Checkpoint auszuführen ist

Die Priorität, nicht festgeschriebene Seiten (Dirty Pages) auf die Festplatte zu schreiben, steigt mit der abgelaufenen Zeit und der Arbeitsmenge seit dem letzten Checkpoint. Die Priorität wird von folgenden Faktoren bestimmt:

- **Checkpoint-Dringlichkeit** Die Zeit, die seit dem letzten Checkpoint verstrichen ist, als Prozentsatz der Datenbankeinstellung für die Checkpoint-Zeit. Sie können in Minuten das maximale Zeitintervall zwischen Checkpoints angeben, indem Sie die Serveroption -gc oder die Datenbankoption checkpoint\_time verwenden. Wenn -gc angegeben ist, wird die Einstellung der Option checkpoint\_time in der Datenbank ignoriert.
- **Wiederherstellungs-Dringlichkeit** Ein heuristischer Wert zur Schätzung der Zeitdauer, die für das Wiederherstellen der Datenbank erforderlich ist, wenn sie genau jetzt ausfällt. Sie können in Minuten das maximale Zeitintervall für die Wiederherstellung bei einem Systemausfall eingeben, indem Sie die Serveroption -gr oder die Datenbankoption recovery\_time verwenden. Wenn -gr angegeben ist, wird die Einstellung der Option reconvery\_time in der Datenbank ignoriert.

Checkpoint- und Wiederherstellungs-Dringlichkeit sind nur dann wichtig, wenn der Datenbankserver nicht über genügend Leerlaufzeit verfügt, um nicht festgeschriebene Seiten (Dirty Pages) auf die Festplatte zu schreiben. Die untere Grenze für das Intervall zwischen Checkpoints basiert auf einer Kombination der Optionen recovery\_time und checkpoint\_time. Die recovery\_time-Optionseinstellung wird nicht berücksichtigt, wenn dadurch ein Checkpoint zu früh erzwungen würde.

Häufige Checkpoints führen dazu, dass die Wiederherstellung schneller vonstatten geht, sorgen aber auch für mehr Arbeit für den Server, der die nicht festgeschriebenen Seiten auf die Festplatte schreiben muss.

Wenn die Anzahl der nicht festgeschriebenen Seiten wegen einer anderen Aktivität in der Datenbank auf Null fällt und die Checkpoint-Dringlichkeit 33% oder mehr beträgt, wird automatisch ein Checkpoint ausgeführt, da es sich um einen günstigen Zeitpunkt handelt.

Die Werte für Checkpoint-Dringlichkeit und Wiederherstellungs-Dringlichkeit steigen an, bis ein Checkpoint eintritt, wonach sie auf Null fallen.

## Siehe auch

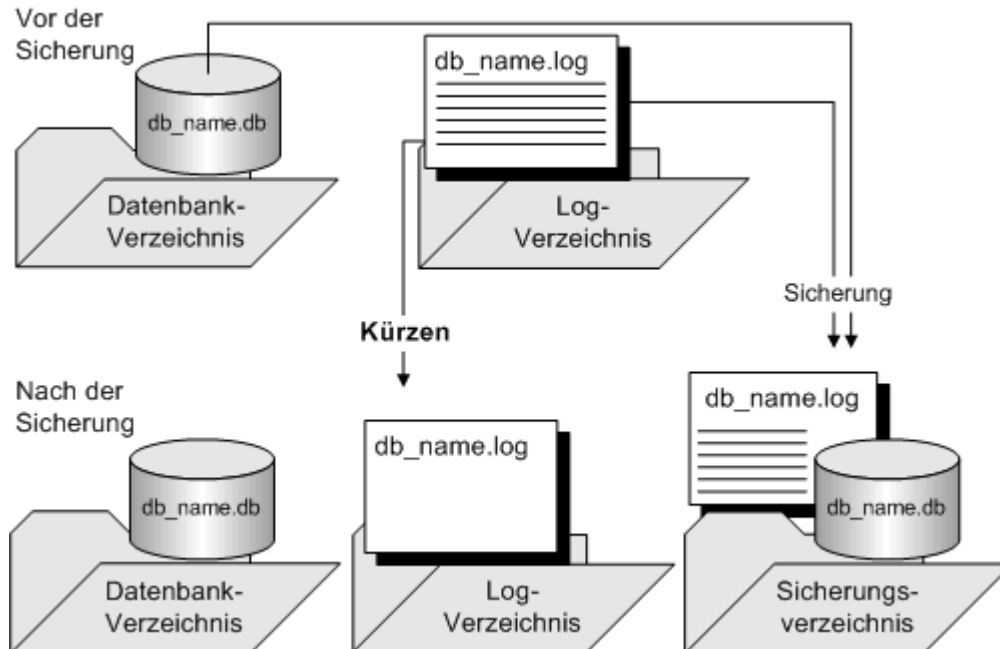
- „Checkpoint-Logs“ auf Seite 143
- „Datenbankserveroption -gc “ auf Seite 239
- „checkpoint\_time-Option“ auf Seite 588
- „Datenbankserveroption -gr “ auf Seite 249
- „recovery\_time-Option“ auf Seite 661

## Transaktionslog-Verwaltung

Wenn Sie eine Sicherung erstellen, stellt der Sicherungsvorgang standardmäßig eine Kopie des aktuellen Zustands des Transaktionslogs her und lässt das Transaktionslog unverändert. Wenn Ihre Datenbank in eine Synchronisations- oder Replikationsumgebung eingebunden ist, müssen Sie eventuell auf alte Kopien des Transaktionslogs nach der Wiederherstellung Ihrer Datenbank zugreifen.

Häufig kann aufgrund des begrenzten Festplattencaches das Transaktionslogs nicht unbegrenzt wachsen. Um Festplattenspeicher freizugeben, können Sie in diesem Fall den Inhalt des Transaktionslogs nach abgeschlossener Sicherung löschen, damit Speicherplatz freigegeben wird. Diese Option sollte nicht gewählt werden, wenn die Datenbank in einem Replikationssystem läuft, da für die Replikation der Zugriff auf das Transaktionslog erforderlich ist.

Eine vollständige Sicherung mit Kürzung der Logdatei wird in der nachfolgenden Darstellung gezeigt. Bei einer inkrementellen Sicherung wird nur das Transaktionslog gesichert.



Wenn das Transaktionslog nach jeder inkrementellen Sicherung gelöscht wird, ist die Wiederherstellung der Datenbankdatei nach einem Datenträgerausfall komplizierter. Jedes Transaktionslog muss in der

ursprünglichen Reihenfolge angewendet werden, um die Datenbank zu aktualisieren, und es kann mehrere unterschiedliche Transaktionslogs seit der letzten Sicherung geben.

Sie können diese Art der Sicherung bei einer Datenbank verwenden, die als konsolidierte MobiLink-Datenbank benutzt wird, da sich MobiLink nicht auf das Transaktionslog stützt. Wenn Sie SQL Remote oder die MobiLink-Anwendung *dbmlsync.exe* verwenden, muss Ihr Sicherungsschema die Archivierung alter Transaktionslogs beinhalten.

#### Siehe auch

- „Transaktionslogs umbenennen oder kürzen (Sybase Central)“ auf Seite 1070
- „Sicherungskopien von Transaktionslogs während einer Sicherung umbenennen (SQL)“ auf Seite 1073

## Offline-Transaktionslogs

Zusätzlich zur Sicherung des Transaktionslogs kann der Sicherungsvorgang das Online-Transaktionslog umbenennen und ihm einen Namen des Formats *JJMMTTxx.log* geben. Diese Datei wird vom Datenbankserver nicht mehr benutzt, steht aber dem Nachrichtenagenten noch zur Verfügung. Dieses Log wird als **Offline-Transaktionslog** bezeichnet. Ein neues Online-Transaktionslog wird mit demselben Namen wie das alte Transaktionslog gestartet.

Die Dateinamen *JJMMTTxx.log* werden benutzt, um die Dateien auseinander halten zu können, nicht zur Sortierung. Die umbenannte Logdatei von der ersten Sicherung am 10. Dezember 2000 heißt *001210AA.log*. Die ersten beiden Stellen zeigen das Jahr, die zweiten den Monat, die dritten den Tag, und die zwei letzten Buchstaben unterscheiden die aufeinanderfolgenden Sicherungen eines Tages.

Der Nachrichtenagent kann die Offline-Kopien benutzen, um erforderlichenfalls alte Transaktionen abzurufen. Wenn Sie die `delete_old_logs`-Datenbankoption auf "On" setzen, löscht der Nachrichtenagent die Offline-Dateien, wenn sie nicht mehr benötigt werden. Damit wird Speicherplatz auf dem Datenträger gespart.

## Das Rollback-Log

Parallel zu den Änderungen am Inhalt von Tabellen wird ein **Rollback-Log** geführt, damit Änderungen widerrufen werden können, wenn eine Transaktion zurückgesetzt wird oder bei einem Systemausfall nicht festgeschriebene Transaktionen vorhanden sind. Für jede Verbindung wird ein eigenes Rollback-Log eingerichtet. Wenn eine Transaktion festgeschrieben oder zurückgesetzt wird, werden die Einträge im Rollback-Log für diese Verbindung gelöscht. Die Rollback-Logs werden in der Datenbank gespeichert, und Rollback-Logseiten werden gemeinsam mit anderen geänderten Seiten in das Checkpoint-Log kopiert.

Das Rollback-Log wird auch als **Undo-Log** bezeichnet.

#### Siehe auch

- „Transaktionen und Isolationsstufen“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Parallele Datenbanksicherungen

Wenn Sie eine serverseitige Sicherungskopie mit dem Sicherungsdienstprogramm (dbbackup) unter Angabe der Option -s oder der BACKUP DATABASE-Anweisung erstellen, wird eine parallele Datenbanksicherung durchgeführt. Parallele Sicherungen verwenden Parallelität auf der physischen Device-Ebene, um die für einen Sicherungsvorgang erforderliche Gesamtzeit zu verringern. Parallele Sicherungen werden unter Windows Mobile nicht unterstützt.

Der Datenbankserver erstellt einen Reader-Thread für jedes Laufwerk, auf dem Datenbankdateien gespeichert sind. Ein Writer-Thread wird für das Ziellaufwerk erstellt, auf dem sich das Sicherungsverzeichnis befindet. Die Verwendung von separaten Reader- und Writer-Threads ermöglicht es, I/O-Vorgänge parallel statt sequenziell durchzuführen.

Die Performance einer parallelen Sicherung hängt von der langsamsten Komponente im System ab. Normalerweise handelt es sich um eine physische Festplatte, aber auch andere Komponenten wie ein I/O-Controller oder der Systembus können Auswirkungen auf die Performance haben. Jeder dieser Komponenten hat eine Maximalrate für die Datenübertragung.

Die BACKUP DATABASE-Anweisung und das Sicherungsdienstprogramm (dbbackup) enthalten Optionen, mit denen Sie das Verhalten einer parallelen Sicherung konfigurieren können, einschließlich folgender:

- Wann und wie das Checkpoint-Log kopiert wird
- Die maximale Anzahl von Seiten, die gleichzeitig bei der Übertragung von Daten vom Datenbankserver zu "dbbackup" verwendet werden (nur bei Verwendung von "dbbackup" verfügbar)
- Weitere Writer-Threads hinzufügen (nur BACKUP-Anweisung)

Sicherungen sollten stets auf einem separaten physischen Device durchgeführt werden. Dies führt zu einer Performancesteigerung dank der I/O-Parallelität und erhöht auch die Datensicherheit bei einem Hardwareausfall.

### Siehe auch

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886

## Datenbankvalidierung

Die Beschädigung einer Datenbankdatei wird möglicherweise erst erkannt, wenn der Datenbankserver versucht, auf den betroffenen Teil der Datenbank zuzugreifen. Sie sollten daher regelmäßig die Gültigkeit Ihrer Datenbank überprüfen, indem Sie Tools wie den **Assistenten zum Validieren einer Datenbank** in Sybase Central oder das Dienstprogramm zur Validierung (dbvalid) bzw. die VALIDATE-Anweisung ausführen.

Abhängig von den von Ihnen angegebenen Optionen kann die Validierung Prüfsummen und die Korrektheit von Indexdaten umfassen, und ob alle Tabellenseiten zu Objekten in der Datenbank gehören. Bei der Expressvalidierung der Datenbank (mit der Option dbvalid -fx) werden die Daten, die

kontinuierliche Zeilenstruktur oder die Fremdschlüsselbeziehungen nicht geprüft. Sie können auch die WITH EXPRESS CHECK-Klausel in der VALIDATE-Anweisung festlegen, um die Prüfung der referenziellen Integrität zu deaktivieren.

Bei der Validierung wird kein exklusiver Zugriff auf die zu validierende Tabelle angefordert und es können Fehler gemeldet werden, wenn die Tabelle während der Validierung geändert wird. Aus diesem Grund wird die Validierung sinnvollerweise dann durchgeführt, wenn keine anderen Aktivitäten in der Datenbank laufen. Wenn eine Basistabelle in der Datenbankdatei beschädigt ist, müssen Sie dies wie einen Datenträgerfehler behandeln und eine Wiederherstellung von einer früheren Sicherung aus vornehmen. Wenn ein Index beschädigt ist, können Sie die Datenbank ohne Indizes entladen und dann wieder einlesen. Sie können auch die REBUILD-Klausel der ALTER INDEX-Anweisung verwenden, um Indexbeschädigungen zu beheben.

#### **Tipp**

Die BACKUP-Anweisung mit der Klausel WAIT BEFORE START sorgt dafür, dass keine Transaktionen laufen, während Sie eine Sicherung starten. Wenn während der Sicherung keine Transaktionen aktiv waren oder Sie BACKUP DATABASE WITH CHECKPOINT LOG RECOVER oder WITH CHECKPOINT LOG NO COPY angegeben haben, können Sie die Validität der Sicherungsdatenbank im Schreibschutzmodus prüfen, oder indem Sie eine Kopie der Sicherungsdatenbank validieren.

#### **Siehe auch**

- „Datenbanken validieren (Sybase Central)“ auf Seite 1081
- „Transaktionslog-Validierung“ auf Seite 1075
- „Validieren einer Tabelle“ auf Seite 1086
- „VALIDATE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_validate-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „Konzepte und Referenz zu Textindizes“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „ALTER INDEX-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -r“ auf Seite 277

## **Datenbanken validieren (Sybase Central)**

Die Beschädigung einer Datenbankdatei wird möglicherweise erst erkannt, wenn der Datenbankserver versucht, auf den betroffenen Teil der Datenbank zuzugreifen. Sie können die Gültigkeit Ihrer Datenbank mit Sybase Central überprüfen.

#### **Voraussetzungen**

Sie müssen das VALIDATE ANY OBJECT-Systemprivileg haben. Führen Sie die Validierung nach Möglichkeit dann durch, wenn keine anderen Aktivitäten in der Datenbank laufen.

### Vorsicht

Die Validierung einer Tabelle oder einer ganzen Datenbank darf nur durchgeführt werden, wenn keine Verbindungen Änderungen in der Datenbank durchführen, weil sonst möglicherweise Fehler über eine Datenbankbeschädigung gemeldet werden, obwohl eine solche nicht vorliegt.

### Kontext und Bemerkungen

Wenn Sie die Gültigkeit einer Sicherungskopie prüfen, muss die Datenbank schreibgeschützt ausgeführt werden, damit sie während der Prüfung nicht verändert werden kann. Dies können Sie allerdings nur tun, wenn während der Sicherung keine Transaktionen aktiv waren.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Wählen Sie im linken Fensterausschnitt die Datenbank aus.
3. Klicken Sie im Menü **Datei** auf **Datenbank validieren**.
4. Befolgen Sie die Anweisungen im **Assistenten zum Validieren einer Datenbank**.

### Tipp

Sie können den **Assistenten zum Validieren einer Datenbank** auch aus Sybase Central auf eine der folgenden Weisen aufrufen:

- Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Datenbank validieren**.
- Wählen Sie die Datenbank aus und klicken Sie auf **Extras » SQL Anywhere 16 » Datenbank validieren**.

### Ergebnisse

Die Datenbank wird validiert.

### Siehe auch

- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „VALIDATE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -r“ auf Seite 277

## Datenbanken validieren (SQL)

Die Beschädigung einer Datenbankdatei wird möglicherweise erst erkannt, wenn der Datenbankserver versucht, auf den betroffenen Teil der Datenbank zuzugreifen. Sie können die Gültigkeit Ihrer Datenbank überprüfen, indem Sie in SQL die gespeicherte Prozedur `sa_validate` oder die `VALIDATE DATABASE`-Anweisung ausführen.

## Voraussetzungen

Sie müssen das `VALIDATE ANY OBJECT`-Systemprivileg haben. Führen Sie die Validierung nach Möglichkeit dann durch, wenn keine anderen Aktivitäten in der Datenbank laufen.

### Vorsicht

Die Validierung einer Tabelle oder einer ganzen Datenbank darf nur durchgeführt werden, wenn keine Verbindungen Änderungen in der Datenbank durchführen, weil sonst möglicherweise Fehler über eine Datenbankbeschädigung gemeldet werden, obwohl eine solche nicht vorliegt.

## Kontext und Bemerkungen

Wenn Sie die Gültigkeit einer Sicherungskopie prüfen, muss die Datenbank schreibgeschützt ausgeführt werden, damit sie während der Prüfung nicht verändert werden kann. Dies können Sie allerdings nur tun, wenn während der Sicherung keine Transaktionen aktiv waren.

## Aufgabe

- Stellen Sie eine Verbindung mit der Datenbank her.

Option	Aktion
Gespeicherte Prozedur <code>sa_validate</code>	<p>Führen Sie die gespeicherte Prozedur <code>sa_validate</code> aus:</p> <pre>CALL sa_validate;</pre> <p>Die Prozedur gibt eine einzelne Spalte zurück, die die Bezeichnung "Messages" trägt. Wenn alle Tabellen gültig sind, enthält die Spalte die Meldung Keine Fehler gefunden.</p>
<code>VALIDATE DATABASE</code> -Anweisung	Führen Sie die <code>VALIDATE DATABASE</code> -Anweisung aus.

## Ergebnisse

Die Datenbank wird validiert.

## Siehe auch

- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „`VALIDATE`-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption `-r`“ auf Seite 277
- „`sa_validate`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbanken validieren (Befehlszeile)

Sie können eine Datenbank über die Befehlszeile validieren.

## Voraussetzungen

Sie müssen das VALIDATE ANY OBJECT-Systemprivileg haben. Führen Sie die Validierung nach Möglichkeit dann durch, wenn keine anderen Aktivitäten in der Datenbank laufen.

### Vorsicht

Die Validierung einer Tabelle oder einer ganzen Datenbank darf nur durchgeführt werden, wenn keine Verbindungen Änderungen in der Datenbank durchführen, weil sonst möglicherweise Fehler über eine Datenbankbeschädigung gemeldet werden, obwohl eine solche nicht vorliegt.

## Kontext und Bemerkungen

Wenn Sie die Gültigkeit einer Sicherungskopie prüfen, muss die Datenbank schreibgeschützt ausgeführt werden, damit sie während der Prüfung nicht verändert werden kann. Dies können Sie allerdings nur tun, wenn während der Sicherung keine Transaktionen aktiv waren.

## Aufgabe

- Starten Sie das Dienstprogramm dbvalid:

```
dbvalid -c "connection-string"
```

## Ergebnisse

Die Datenbank wird validiert.

## Siehe auch

- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „VALIDATE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -r“ auf Seite 277

# Erkennung von Beschädigungen mithilfe von Prüfsummen

**Mit Prüfsummen kann festgestellt werden, ob eine Datenbankseite auf der Festplatte geändert wurde.** SQL Anywhere unterstützt zwei Typen von Prüfsummen: globale Prüfsummen und Schreib-Prüfsummen.

## Globale Prüfsummen

Globale Prüfsummen sind aktiviert, wenn die Datenbank erstellt wird. Wenn Sie eine Datenbank mit aktivierten globalen Prüfsummen erstellen, berechnet das System eine Prüfsumme, direkt bevor eine Datenbankseite auf die Festplatte geschrieben wird. Wenn die Seite von der Festplatte gelesen wird, ermittelt das System die Prüfsumme erneut und vergleicht sie mit dem auf der Seite gespeicherten Wert. Wenn die Prüfsummen unterschiedlich sind, wurde die Seite auf der Festplatte geändert und ein Fehler tritt auf.

Sie können überprüfen, ob eine Datenbank mit aktivierten globalen Prüfsummen erstellt wurde, indem Sie die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'Checksum' );
```

Diese Abfrage gibt ON zurück, wenn Prüfsummen aktiviert sind, sonst wird OFF zurückgegeben.

Mit der CHECKSUM-Klausel der ALTER DATABASE-Anweisung können Sie globale Prüfsummen für eine vorhandene Datenbank deaktivieren. Die Deaktivierung von Prüfsummen wird nicht empfohlen. Nachdem globale Prüfsummen deaktiviert wurden, können sie nicht mehr aktiviert werden. Sie können entweder die Option -wc+ verwenden, um das Schreiben von Prüfsummen für die Datenbank zu aktivieren, oder Sie können die Datenbank mit aktivierten Prüfsummen neu erstellen.

## Schreib-Prüfsummen

Standardmäßig sind für Datenbanken, die mit Version 10 und 11 von SQL Anywhere erstellt wurden, keine globalen Prüfsummen aktiviert. Wenn Sie eine Datenbank, die mit SQL Anywhere 11 erstellt wurde, auf einem Datenbankserver der Version 12 oder später starten, erstellt der Datenbankserver standardmäßig Schreib-Prüfsummen, bei denen es sich um Prüfsummen handelt, die den Seiten nur hinzugefügt werden, wenn sie auf die Festplatte geschrieben werden.

Für Datenbanken der Version 12 und höher sind globale Prüfsummen standardmäßig aktiviert. Wenn Sie eine neue Datenbank erstellen und globale Prüfsummen für die Datenbank deaktivieren, können Sie Schreib-Prüfsummen mit der Option -wc+ oder der START DATABASE-Anweisung aktivieren.

Sie können überprüfen, ob eine Datenbank mit Schreib-Prüfsummen gestartet wurde, indem Sie die folgende Anweisung ausführen:

```
SELECT DB_PROPERTY ( 'WriteChecksum' );
```

Diese Abfrage gibt ON zurück, wenn Prüfsummen nur aktiviert sind, wenn Seiten auf die Festplatte geschrieben werden (weil globale Prüfsummen oder Schreib-Prüfsummen aktiviert sind). Andernfalls wird OFF zurückgegeben.

Siehe:

- „Datenbankserveroption -wc“ auf Seite 304
- „Datenbankoption -wc“ auf Seite 334
- „START DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- WriteChecksum-Datenbankeigenschaft auf Seite 789

## Automatische Schreib-Prüfsummenerstellung

In den folgenden Situationen sind Schreib-Prüfsummen für die Datenbank aktiviert, unabhängig von der bei der Erstellung der Datenbank angegebenen Einstellung für globale Prüfsummen.

- **Kritische Seiten** Der Datenbankserver berechnet Prüfsummen bei kritischen Datenbankseiten in allen Datenbanken, unabhängig davon, ob Prüfsummen aktiviert sind. Diese Prüfsummen werden verwendet, um Offline-Beschädigungen zu ermitteln, was die Wahrscheinlichkeit verringert, dass andere Daten aufgrund einer beschädigten kritischen Seite in Mitleidenschaft gezogen werden. Da der Datenbankserver diese Prüfsummen berechnet, fährt er mit einem schwerwiegenden Fehler auch dann herunter, wenn eine Datenbank beschädigt wird, bei der Prüfsummen nicht aktiviert sind.

Wenn Sie eine Datenbank validieren, bei der globale Prüfsummen nicht aktiviert sind, die aber eine beschädigte kritische Seite hat, kann dbvalid weiterhin Warnungen über Prüfsummen-Verstöße zurückgeben.

- **Windows Mobile-Datenbanken** Der Datenbankserver aktiviert automatisch Schreib-Prüfsummen für Datenbanken, die unter Windows Mobile laufen, um frühzeitig zu erkennen, ob eine Datenbankdatei beschädigt ist.
- **Datenbanken, die auf bestimmten Datenträgern laufen** Wenn Datenbanken auf Datenträgern laufen, die möglicherweise nicht sehr verlässlich sind, wie z.B. Netzwerk- oder Wechseldatenträger, aktiviert der Datenbankserver automatisch Schreib-Prüfsummen für die Datenbank. Schreib-Prüfsummen bleiben aktiviert, solange die Datenbank auf einem derartigen Gerät gespeichert ist, und für die Seiten werden Prüfsummen ermittelt, während sie geschrieben werden. Wenn die Datenbank auf ein verlässlicheres Speichermedium verschoben wird, überprüft der Datenbankserver die Prüfsumme für Seiten, bei denen Prüfsummen ermittelt wurden, wenn sie im Datenbankserver-Cache abgelegt werden.

Siehe:

- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- Checksum-Datenbankeigenschaft auf Seite 770

### Prüfsummen validieren

Sie können Plattenspeicherseiten für Datenbanken validieren, die globale oder Schreib-Prüfsummen verwenden. Wenn für eine Datenbank globale Prüfsummen aktiviert sind, werden alle Datenbankseiten validiert. Wenn eine Datenbank nur Schreib-Prüfsummen verwendet hat, werden nur Seiten mit Prüfsummen validiert.

Bei Datenbanken mit aktivierten Prüfsummen wird für jede Datenbankseite eine Prüfsumme berechnet und dieser Wert wird gespeichert, wenn die Seite auf die Festplatte geschrieben wird. Sie können das Validierungsdienstprogramm (dbvalid), die VALIDATE-Anweisung, die sa\_validate-Systemprozedur oder den **Assistenten zum Validieren einer Datenbank** in Sybase Central zur Prüfsummenvalidierung einsetzen, bei der die Datenbankseiten von der Festplatte gelesen werden und eine Prüfsumme für jede Seite ermittelt wird. Wenn die berechnete Prüfsumme nicht mit der für eine Seite gespeicherten Prüfsumme übereinstimmt, wurde die Seite entweder geändert oder auf der Festplatte bzw. während des Schreibens auf die Seite beschädigt. Sind eine oder mehrere Seiten beschädigt, dann erscheint im Meldungsfenster des Datenbankservers eine Fehlermeldung mit einem Hinweis auf die ungültigen Seiten.

Siehe:

- „VALIDATE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Validierungs-Dienstprogramm (dbvalid)“ auf Seite 1020
- „sa\_validate-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Validieren einer Tabelle

Sie können eine Tabelle mit Sybase Central validieren.

### Voraussetzungen

Sie müssen das `VALIDATE ANY OBJECT`-Systemprivileg haben. Führen Sie die Validierung nach Möglichkeit dann durch, wenn keine anderen Aktivitäten in der Tabelle laufen.

### Kontext und Bemerkungen

- Wenn Fehlermeldungen erscheinen, können Sie alle Indizes und Schlüssel für eine Tabelle löschen und sie wieder neu erstellen. Jeder Fremdschlüssel für die Tabelle muss ebenfalls neu erstellt werden.
- Wenn Sie eine Beschädigung in einen bestimmten Index vermuten, können Sie eine `ALTER INDEX ... REBUILD`-Anweisung ausführen, um den beschädigten Index neu zu erstellen.
- Eine weitere Lösung für Fehler, die durch die `VALIDATE TABLE`-Anweisung gemeldet werden, besteht darin, die gesamte Datenbank zu entladen und neu zu laden. Geben Sie die `dbunload`-Option `-u` an, damit beim Entladeprozess kein möglicherweise beschädigter Index zum Ordnen der Daten verwendet wird.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Tabellen**.
3. Rechtsklicken Sie auf die Tabelle und klicken Sie auf **Validieren**.
4. Klicken Sie auf **OK**.

### Ergebnisse

Die Tabelle wird validiert.

### Siehe auch

- „`VALIDATE`-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`ALTER INDEX`-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Validierungs-Dienstprogramm (`dbvalid`)“ auf Seite 1020

## Aufgabenautomatisierung mit Abfolgeplanung und Ereignissen

Viele Datenbank-Verwaltungsaufgaben werden am besten systematisch durchgeführt. So ist beispielsweise eine regelmäßige Sicherung ein wichtiger Teil einer ordentlichen Datenbankverwaltung.

Sie können Routineaufgaben in SQL Anywhere automatisieren, indem Sie einer Datenbank ein **Ereignis** (Event) hinzufügen und einen Abfolgeplan für dieses Ereignis festlegen. Wenn einer der im Abfolgeplan festgelegten Zeitpunkte verstreicht, führt der Datenbankserver eine Sequenz von Aktionen aus, die als **Event-Handler** bezeichnet wird.

Zur Datenbankverwaltung gehört auch, dass bestimmte Maßnahmen getroffen werden, wenn bestimmte Bedingungen eintreten. Beispiel: Es kann sinnvoll sein, einen Systemadministrator per E-Mail zu verständigen, wenn eine Festplatte voll wird, auf der sich das Transaktionslog befindet, damit der Administrator auf diesen Zustand reagieren kann. Auch diese Aufgaben können automatisiert werden, indem Event-Handler für eines der **Systemereignisse** festgelegt werden.

## Fragen und Antworten

Frage	Empfohlene Lektüre
Was ist eine Abfolgeplanung?	„Zeitpläne“
Was ist ein Ereignis?	„Ereignisse“
Was ist ein Systemereignis?	„Systemereignisse“
Was ist ein Event-Handler?	„Event-Handler (Fehlerverarbeitungsroutinen)“
Wie erfolgt die Fehlersuche von Event-Handlern?	„Debugging von Event-Handlern“ auf Seite 1099
Wie benutzt der Datenbankserver die Abfolgeplanung, um Event-Handler auszulösen?	„Prüfung von geplanten Ereignissen durch den Datenbankserver“
Wie kann ich regelmäßige Sicherungen planen?	„Zeitpläne“
Welche Art von Systemereignissen kann der Datenbankserver benutzen, um Event-Handler auszulösen?	„Systemereignisse“ „CREATE EVENT-Anweisung“ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ]
Unter welchen Verbindungen werden Event-Handler ausgeführt?	„Ausführungsweise von Event-Handlern“
Wie beziehen Event-Handler Informationen über die Ereignisse, die sie ausgelöst haben?	„Triggerbedingungen für Ereignisse“ auf Seite 1093 „EVENT_PARAMETER-Funktion [System]“ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ]

## Ereignisse

Sie können Routineaufgaben in SQL Anywhere automatisieren, indem Sie einer Datenbank ein Ereignis (Event) hinzufügen und einen Abfolgeplan für dieses Ereignis festlegen. SQL Anywhere unterstützt die folgenden Ereignistypen:

- **Geplante Ereignisse** haben eine zugeordnete Abfolgeplanung und werden zu bestimmten Zeiten ausgeführt. Siehe „Zeitpläne“ auf Seite 1089.

- **Systemereignisse** sind einem bestimmten Typ von Bedingung zugeordnet, die der Datenbankserver protokolliert. Siehe „[Systemereignisse](#)“ auf Seite 1091.
- **Manuelle Ereignisse** werden explizit mit der TRIGGER EVENT-Anweisung ausgelöst. Siehe „[Auslösen eines Event-Handlers](#)“ auf Seite 1099.
- **Benutzer-Trace-Ereignisse** werden verwendet, um Informationen zu einer Anwendung in einer Ereignisprotokollierungssitzung zu protokollieren. Diese Ereignisse sind für alle Verbindungen mit einer Datenbank sichtbar. Siehe „[Ereignisprotokollierung](#)“ auf Seite 1101 und „[CREATE TEMPORARY TRACE EVENT-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

Nach jeder Ausführung eines Event-Handlers wird ein COMMIT ausgeführt, falls kein Fehler aufgetreten ist. Wenn es einen Fehler gegeben hat, wird ein ROLLBACK ausgeführt.

## Zeitpläne

Durch die Abfolgeplanung von Aktivitäten können Sie dafür Sorge tragen, dass zu festgelegten Zeiten eine Serie von Maßnahmen durchgeführt wird. Die Informationen für die Abfolgeplanung und der Event-Handler werden in der Datenbank selbst gespeichert.

Obwohl dies in der Regel nicht notwendig sein wird, können Sie komplexe Abfolgepläne festlegen, indem Sie mehr als einen Abfolgeplan mit einem bestimmten Ereignis verknüpfen. Ein Einzelhandelsgeschäft könnte beispielsweise planen, dass während der Betriebsstunden ein Ereignis einmal pro Stunde eintritt, wobei die Betriebsstunden aber je nach Wochentag variieren. Sie können dieselbe Wirkung durch die Definition mehrerer Ereignisse erreichen, die jeweils ihren eigenen Ablaufplan haben, und indem Sie eine gespeicherte Prozedur aufrufen.

Bei der Planung von Ereignissen können Sie entweder die englischen Namen der Wochentage in ganzer Form angeben (Monday, Tuesday usw.), oder die Namen in Kurzform (Mon, Tue usw.). Nur die ausgeschriebenen englischen Namen der Wochentage werden von Servern erkannt, die eine andere Sprache als Englisch benutzen.

Im folgenden Beispiel werden einige Aktionen aufgeführt, für die ein Zeitplan sinnvoll wäre.

## Beispiele

Eine inkrementelle Sicherung täglich um 1:00 morgens durchführen:

```
CREATE EVENT IncrementalBackup
SCHEDULE
  START TIME '1:00 AM' EVERY 24 HOURS
HANDLER
BEGIN
  BACKUP DATABASE DIRECTORY 'c:\\backup'
  TRANSACTION LOG ONLY
  TRANSACTION LOG RENAME MATCH
END;
```

Alle Aufträge am Ende eines Arbeitstages zusammenfassen.

```
CREATE EVENT Summarize
SCHEDULE
```

```
START TIME '6:00 pm'
ON ( 'Monday', 'Tuesday', 'Wednesday', 'Thursday',
    'Friday' )
HANDLER
BEGIN
INSERT INTO OrderSummary
  SELECT CURRENT DATE,
    COUNT( * ),
    SUM( amount )
  FROM Orders
  WHERE date_ordered = current date
END;
```

### Siehe auch

- „CREATE EVENT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Zeitplandefinition

Um sie flexibel gestalten zu können, besteht die Definition der Zeitplanung aus mehreren Komponenten:

- **Name** Jeder Zeitplan hat einen Namen. Sie können einem Ereignis mehr als einen Zeitplan zuordnen und damit komplexe Abläufe gestalten.
- **Startzeit** Sie können eine Startzeit für das Ereignis festlegen (der Zeitpunkt, an dem die Ausführung beginnt).
- **Bereich** Als Alternative zur Startzeit können Sie eine Zeitspanne festlegen, in der das Ereignis aktiv sein soll. Das Ereignis tritt zwischen den definierten Beginn- und Endzeiten ein. Die Häufigkeit wird durch die festgelegte Einstellung der Wiederholung bestimmt.
- **Wiederholung** Jede Zeitplanung kann sich wiederholen. Das Ereignis wird wiederholt ausgeführt. Die Zeitangabe kann dabei in Stunden, Minuten, Sekunden und Tagesgruppen (Wochentage oder Monatstage) definiert werden. Sich wiederholende Ereignisse enthalten eine **EVERY**- oder **ON**-Klausel.

## Zeitpläne für Ereignisse erstellen

Definieren Sie einen Zeitplan für ein Ereignis, um sicherzustellen, dass eine Aktion zu einer voreingestellten Zeit ausgeführt wird.

### Voraussetzungen

Sie müssen entweder das ALTER ANY OBJECT-Systemprivileg oder das MANAGE ANY EVENT-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Ereignisse**.

3. Doppelklicken Sie im rechten Fensterausschnitt auf das Ereignis, für das Sie einen Zeitplan erstellen möchten.
4. Klicken Sie auf die Registerkarte **Zeitpläne**.
5. Klicken Sie auf **Datei » Neu » Zeitplan**.
6. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen von Zeitplänen**.

### Ergebnisse

Ein Zeitplan für das Ereignis wird erstellt.

### Siehe auch

- „ALTER EVENT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Systemereignisse

SQL Anywhere registriert mehrere Systemereignisse. Jedes Systemereignis stellt einen Startpunkt dar, der mit einer Serie von Maßnahmen verknüpft werden kann. Der Datenbankserver registriert die Ereignisse und führt die Maßnahmen aus (die für den Event-Handler vorher definiert wurden), wenn das Systemereignis eine gegebene **Triggerbedingung** erfüllt.

Indem Sie Event-Handler definieren, die ausgeführt werden, wenn ein bestimmtes Systemereignis eintritt und einer von Ihnen definierten Triggerbedingung entspricht, können Sie die Sicherheit und den Schutz Ihrer Daten verbessern sowie die Administration vereinfachen. Die Aktionen eines Event-Handlers werden festgeschrieben, wenn während der Ausführung kein Fehler festgestellt wurde, und zurückgesetzt, falls Fehler festgestellt wurden.

### Siehe auch

- „Triggerbedingungen für Ereignisse“ auf Seite 1093

## Systemereignistypen

- **BackupEnd** Sie können den Ereignistyp BackupEnd benutzen, um Maßnahmen am Ende einer Sicherung zu ergreifen.
- **Connect-Ereignisse** Wenn eine Verbindung eingerichtet wird (Connect) oder fehlschlägt (ConnectFailed). Sie können diese Ereignisse für die Sicherheitsverwaltung benutzen. Als Alternative zu einem Connect-Event-Handler können Sie eine Login-Prozedur in Betracht ziehen. Siehe „[login\\_procedure-Option](#)“ auf Seite 625.
- **DatabaseStart** Sie können den Ereignistyp DatabaseStart benutzen, um Aktionen für den Datenbankstart festzulegen.
- **Deadlock** Sie können das Deadlock-Ereignis verwenden, um Aktionen durchzuführen, wenn ein Deadlock eintritt. Der Event-Handler kann mit der Prozedur sa\_report\_deadlock Informationen über die Bedingungen erhalten, die zum Deadlock geführt haben. Wenn Sie das Deadlock-Ereignis

verwenden, sollten Sie den Datenbankserver dahingehend konfigurieren, dass er die Deadlock-Daten aufzeichnet, indem Sie die Option "log\_deadlocks" auf ON setzen und indem Sie die Funktion RememberLastStatement mit sa\_server\_option oder der Serveroption -zl aktivieren.

Deadlock-Ereignisse werden bei Verbindungs-Deadlocks und Thread-Deadlocks ausgelöst. Ein Deadlock-Ereignis liefert nur die Informationen, die über die Systemprozedur sa\_report\_deadlocks verfügbar gemacht werden. Die Verwendung dieses Ereignisses ermöglicht es Ihnen allerdings, auf ein Deadlock rechtzeitig zu reagieren. Eine schnelle Reaktion kann wichtig sein, da die Menge an Deadlocks betreffender Informationen, die der Datenbankserver aufrecht erhält, beschränkt ist. Siehe:

- „sa\_report\_deadlocks-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „log\_deadlocks-Option“ auf Seite 623
- „Deadlocks“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

- **Disconnect** Sie können das Ereignis Disconnect benutzen, um eine Aktion einzuleiten, wenn ein Benutzer oder eine Anwendung eine Verbindung trennt.
- **Freier Festplattenspeicher** Damit wird der freie Speicherplatz auf dem Speichermedium registriert, auf dem sich die Datenbankdatei (DBDiskSpace), die Logdatei (LogDiskSpace) oder die Temporärdatei (TempDiskSpace) befinden. Dieses Systemereignis steht unter Windows Mobile nicht zur Verfügung.

Sie können Festplattenereignisse benutzen, um den Systemadministrator zu verständigen, wenn der Speicherplatz knapp wird.

Sie können die Option -fc beim Starten des Datenbankservers angeben, um eine Callback-Funktion zu implementieren, wenn der Datenbankserver Speichermangel im Dateisystem feststellt. Siehe [„Datenbankserveroption -fc“ auf Seite 235](#).

- **Dateigröße** Die Datei erreicht eine vorher festgelegte Größe. Dies kann für die Datenbankdatei (GrowDB), das Transaktionslog (GrowLog) oder die Temporärdatei (GrowTemp) benutzt werden.

Sie können Dateigrößenereignisse benutzen, um ungewöhnliche Aktionen in der Datenbank zu registrieren oder Massenvorgänge zu überwachen.

- **GlobalAutoincrement** Wenn die Anzahl der verbleibenden Werte für eine mit GLOBAL AUTOINCREMENT definierte Spalte niedriger ist als ein Prozent des festgelegten Bereiches, wird das Ereignis GlobalAutoIncrement ausgelöst. Eine typische Aktion für den Handler könnte darin bestehen, einen neuen Wert für die Option global\_database\_id auf der Grundlage der Tabelle und der Anzahl der restlichen Werte anzufordern, die als Parameter für dieses Ereignis übergeben wurden. Um die restlichen Werte für die Tabelle im Ereignis zu beziehen, verwenden Sie die Funktion EVENT\_PARAMETER mit den Parametern RemainingValues und TableName. RemainingValues gibt die Anzahl der restlichen Werte zurück, die bei der Spalte generiert werden können, und TableName gibt die Tabelle zurück, die die Spalte GLOBAL AUTOINCREMENT enthält, bei der der Bereich beinahe ausgeschöpft ist. Siehe [„EVENT\\_PARAMETER-Funktion \[System\]“ \[\[SQL Anywhere Server - SQL-Referenzhandbuch\]\(#\)\]](#).
- **RAISERROR-Fehler** Wenn eine RAISERROR-Anweisung ausgeführt wird, können Sie den Ereignistyp RAISERROR benutzen, um Maßnahmen einzuleiten. Die in der RAISERROR-Anweisung verwendete Fehlernummer kann innerhalb des Event-Handlers ermittelt werden, indem

Sie die Funktion `EVENT_CONDITION` verwenden (z.B. `EVENT_CONDITION( 'ErrorNumber' )`).

- **Leerlaufzeit** Der Datenbankserver wurde eine Zeit lang nicht benutzt (`ServerIdle`). Sie können diesen Ereignistyp verwenden, um Routine-Wartungsvorgänge in Ruhezeiten auszuführen.
- **Systemereignistypen für Datenbankspiegelungen** Die folgenden Systemereignisse werden bei der Datenbankspiegelung unterstützt:
  - **MirrorFailover** Dieses Ereignis wird jedesmal ausgelöst, wenn ein Datenbankserver Eigentümer der gespiegelten Datenbank wird. Es wird z.B. ausgelöst, wenn ein Server erstmals startet und bestimmt, dass er der Eigentümer der Datenbank sein soll. Es wird auch ausgelöst, wenn ein Server, der bisher als Spiegelserver gedient hat, feststellt, dass der Primärserver ausgefallen ist, und nach Beratungen mit dem Arbiterserver bestimmt, dass er Eigentümer werden soll.
  - **MirrorServerDisconnect** Wenn die Verbindung zwischen dem Primärserver und dem Spiegel- oder Arbiterserver unterbrochen wurde, wird das `MirrorServerDisconnect`-Ereignis ausgelöst. Im Handler für dieses Ereignis ist der Wert von `EVENT_PARAMETER( "MirrorServerName" )` der Name des Servers, dessen Verbindung unterbrochen wurde. Dieses Ereignis wird nur auf dem Primärserver ausgelöst.

## Triggerbedingungen für Ereignisse

Mit jeder Ereignisdefinition ist ein Systemereignis verknüpft. Außerdem sind ihr eine oder zwei Triggerbedingungen zugeordnet. Der Event-Handler wird ausgelöst, wenn die Triggerbedingungen für das Systemereignis eintreten.

Die Triggerbedingungen werden in die `WHERE`-Klausel der `CREATE EVENT`-Anweisung eingebaut und können mit dem Schlüsselwort `AND` kombiniert werden. Die Triggerbedingungen haben folgendes Format:

**event\_condition**( *condition-name* ) *comparison-operator* *value*

Das Argument *condition-name* ist eine von mehreren vordefinierten Zeichenfolgen, die für unterschiedliche Ereignistypen geeignet sind. Beispiel: Sie können **DBSize** (Größe der Datenbankdatei in MB) benutzen, um eine Triggerbedingung für das Systemereignis **GrowDB** einzustellen. Der Datenbankserver prüft nicht, ob der Bedingungsname zum Ereignistyp passt: Sie müssen dafür Sorge tragen, dass die Bedingung im Zusammenhang mit dem Ereignistyp einen Sinn ergibt.

### Beispiele

- Das Transaktionslog soll auf 10 MB begrenzt werden:

```
CREATE EVENT LogLimit
TYPE GrowLog
WHERE event_condition( 'LogSize' ) > 10
HANDLER
BEGIN
    IF EVENT_PARAMETER( 'NumActive' ) = 1 THEN
        BACKUP DATABASE
```

```
DIRECTORY 'c:\\logs'
TRANSACTION LOG ONLY
TRANSACTION LOG RENAME MATCH;
END IF;
END;
```

- Ein Administrator soll benachrichtigt werden, wenn der freie Speicher auf dem Medium mit der Datenbankdatei unter 10% fällt, wobei aber die Verarbeitungsroutine maximal alle 5 Minuten (300 Sekunden) ausgeführt werden darf:

```
CREATE EVENT LowDBSpace
TYPE DBDiskSpace
WHERE event_condition( 'DBFreePercent' ) < 10
AND event_condition( 'Interval' ) >= 300
HANDLER
BEGIN
CALL xp_sendmail( recipient='DBAdmin',
subject='Low disk space',
"message"='Database free disk space '
|| EVENT_PARAMETER( 'DBFreeSpace' ) );
END;
```

- Ein Administrator soll über einen versuchten Einbruch in die Datenbank in Kenntnis gesetzt werden:

```
CREATE EVENT SecurityCheck
TYPE ConnectFailed
HANDLER
BEGIN
DECLARE num_failures INT;
DECLARE mins INT;
INSERT INTO FailedConnections( log_time )
VALUES ( CURRENT_TIMESTAMP );

SELECT COUNT( * ) INTO num_failures
FROM FailedConnections
WHERE log_time >= DATEADD( minute, -5,
current_timestamp );
IF( num_failures >= 3 ) THEN
SELECT DATEDIFF( minute, last_notification,
current_timestamp ) INTO mins
FROM Notification;
IF( mins > 30 ) THEN
UPDATE Notification
SET last_notification = current_timestamp;
CALL xp_sendmail( recipient='DBAdmin',
subject='Security Check', "message"=
'over 3 failed connections in last 5 minutes' )
END IF
END IF
END;
```

- Ein Prozess wird ausgeführt, wenn sich der Server mehr als 10 Minuten im Leerlauf befindet. Der Prozess darf aber nicht öfter als einmal pro Stunde ausgeführt werden:

```
CREATE EVENT Soak
TYPE ServerIdle
WHERE event_condition( 'IdleTime' ) >= 600
AND event_condition( 'Interval' ) >= 3600
HANDLER
```

```
BEGIN  
MESSAGE ' Insert your code here ... '  
END;
```

## Event-Handler (Fehlerverarbeitungsroutinen)

Event-Handler werden über eine Verbindung ausgeführt, die von der sie auslösenden Aktion getrennt ist, und stören daher Clientanwendungen nicht. Sie werden mit den Privilegien des Ereigniserstellers ausgeführt.

Event-Handler für geplante Ereignisse oder Systemereignisse enthalten zusammengesetzte Anweisungen und ähneln in vielerlei Hinsicht gespeicherten Prozeduren. Sie können Schleifen, bedingte Ausführung usw. hinzufügen sowie den SQL Anywhere-Debugger für das Debugging von Event-Handlern verwenden.

Nach jeder Ausführung eines Event-Handlers wird ein COMMIT ausgeführt, falls kein Fehler aufgetreten ist. Wenn es einen Fehler gegeben hat, wird ein ROLLBACK ausgeführt.

### Kontext für Event-Handler

Im Unterschied zu gespeicherten Prozeduren übernehmen Event-Handler keine Argumente. Sie können die EVENT\_PARAMETER-Funktion verwenden, um Informationen über den Kontext abzurufen, in dem ein Ereignis ausgelöst wurde. Die zurückgegebenen Informationen umfassen die Verbindungs-ID und die Benutzer-ID, die das Auslösen eines Ereignisses veranlasst haben, sowie den Ereignisnamen und die Häufigkeit der Ausführung.

### Event-Handler testen

Während der Entwicklung sollen Event-Handler zum gewünschten Zeitpunkt ausgelöst werden. Sie können die Anweisung TRIGGER EVENT verwenden, um die Ausführung eines Ereignisses zu bewirken, auch wenn die Triggerbedingung oder die für die Abfolgeplanung festgelegte Zeit nicht eingetreten sind. TRIGGER EVENT führt allerdings deaktivierte Event-Handler nicht aus.

Es empfiehlt sich zwar nicht, Event-Handler in einer Produktionsdatenbank zu entwickeln, aber Sie können Event-Handler mit der ALTER EVENT-Anweisung explizit deaktivieren.

### Code gemeinsam nutzen

Es kann sinnvoll sein, eine einzelne Aktionsgruppe einzurichten, um mehrfache Ereignisse zu verarbeiten. Beispiel: Sie können eine Benachrichtigungsaktion durchführen, wenn der Festplattenspeicher auf einem der Devices zur Neige geht, auf dem die Datenbank- oder Logdateien untergebracht sind. Dazu erstellen Sie eine gespeicherte Prozedur und rufen sie im Hauptteil jedes Event-Handlers auf, wobei Sie ggf. benötigte Kontextinformationen als Parameter an die Prozedur übergeben.

### Debugging für Event-Handler durchführen

Die Fehlersuche in Event-Handlern ähnelt sehr der Fehlersuche in gespeicherten Prozeduren. Die Event-Handler erscheinen in der Liste der Ereignisse.

## Event-Handler ausblenden

Sie können die ALTER EVENT-Anweisung mit der SET HIDDEN-Klausel verwenden, um die Definition eines Event-Handlers auszublenden. Das Angeben der SET HIDDEN-Klausel führt zur permanenten Verschleierung der Event-Handler-Definition, die in der Aktionsspalte der ISYSEVENT-Systemtabelle gespeichert ist.

## Aktive Ereignisse begrenzen

Sie können ermitteln, wie viele Instanzen eines bestimmten Event-Handlers derzeit aktiv sind, indem Sie die EVENT\_PARAMETER-Funktion mit dem NumActive-Kontextnamen verwenden. Diese Funktion ist nützlich, wenn Sie einen Event-Handler auf jeweils eine Instanz begrenzen möchten.

## Siehe auch

- „Ausführungsweise von Event-Handlern“ auf Seite 1097
- „ALTER EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „EVENT\_PARAMETER-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „TRIGGER EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Debugging von Event-Handlern“ auf Seite 1099
- „Ausblenden eines Event-Handlers“ auf Seite 1100
- „Auslösen eines Event-Handlers“ auf Seite 1099

## Prüfung von Systemereignissen durch den Datenbankserver

Systemereignisse werden nach ihrem **Ereignistyp** gemäß der Angabe in der CREATE EVENT-Anweisung klassifiziert. Es gibt zwei Gattungen von Ereignistypen:

- **Aktive Ereignistypen** Einige Ereignistypen sind das Ergebnis einer Aktion des Datenbankservers. Diese aktiven Ereignistypen schließen beispielsweise wachsende Datenbankdateien oder den Start und das Ende diverser Datenbankaktionen (BackupEnd etc.) oder RAISERROR ein.

Wenn der Datenbankserver selbst für die Aktion verantwortlich ist, prüft er, ob die in der WHERE-Klausel definierten Triggerbedingungen eingetreten sind. Wenn ja, wird das für diesen Ereignistyp definierte Ereignis ausgelöst.

- **Abgefragte Ereignistypen** Einige Ereignistypen, etwa jene, die sich auf den freien Speicherplatz beziehen (DBDiskSpace etc.), oder IdleTime, werden nicht nur durch Datenbankaktionen ausgelöst.

Für diese Ereignistypen fragt der Datenbankserver alle dreißig Sekunden den Zustand ab, zum ersten Mal ca. 30 Sekunden nach dem Start des Datenbankservers.

Für den IdleTime-Ereignistyp prüft der Datenbankserver, ob der Server während der gesamten 30 Sekunden im Leerlauf war. Wenn keine Abfragen gestartet wurden und keine Abfragen derzeit aktiv sind, fügt er das Leerlaufzeitprüfintervall (in Sekunden) der Gesamt-Leerlaufzeitsumme hinzu. Wenn nicht, wird die Gesamt-Leerlaufzeit auf 0 zurückgesetzt. Der Wert für IdleTime ist daher immer ein Vielfaches von 30 Sekunden. Wenn IdleTime größer als das Intervall ist, das in der Triggerbedingung definiert wurde, werden die IdleTime zugeordneten Event-Handler ausgelöst.

## Prüfung von geplanten Ereignissen durch den Datenbankserver

Die Berechnung der in der Abfolgeplanung festgelegten Zeiten erfolgt, wenn der Datenbankserver startet und jedes Mal, wenn ein Event-Handler für ein in der Abfolgeplanung festgelegtes Ereignis abgelaufen ist.

Die Berechnung des nächsten Zeitpunkts basiert auf dem Intervall, das in der Definition der Abfolgeplanung festgelegt wurde, wobei dieses Intervall dem vorherigen Startzeitpunkt hinzugefügt wird. Wenn der Event-Handler für seinen Abschluss länger braucht als das vorgesehene Intervall, also der Zeitpunkt überschritten wird, zählt der Datenbankserver bis zum darauf folgenden geplanten Zeitpunkt weiter.

Beispiel: Ein Event-Handler, der 65 Minuten für seinen Abschluss braucht und jede Stunde zwischen 9:00 und 17:00 laufen soll, wird daher alle zwei Stunden ausgeführt: 9:00, 11:00, 13:00, etc.

Um einen Prozess so auszuführen, dass er zwischen 9:00 und 17:00 läuft und vor dem nächsten Ausführen eine gewisse Zeit verzögert wird, können Sie einen Event-Handler in eine Schleife einbauen, die zum Abschlusszeitpunkt andauert, wobei zwischen jeder Wiederholung eine WAITFOR-Anweisung verwendet wird.

Wenn Sie einen Datenbankserver intermittierend betreiben und er nicht zu festgelegten Zeiten läuft, wird der Event-Handler beim Start nicht ausgeführt. Der nächste geplante Zeitpunkt wird daher beim Start neu berechnet. Beispiel: Wenn Sie eine Sicherung für jede Nacht um ein Uhr früh festlegen, den Datenbankserver aber am Ende eines Arbeitstages herunterfahren, wird die Sicherung nie durchgeführt.

Wenn die nächste geplante Ausführung eines Ereignisses mehr als eine Stunde entfernt ist, berechnet der Datenbankserver den nächsten geplanten Zeitpunkt auf Stundenbasis neu. Das ermöglicht es, Ereignisse wie erwartet auszulösen, wenn die Systemuhr aufgrund der Sommerzeitumstellung neu eingestellt wird.

## Ausführungsweise von Event-Handlern

Wenn ein Event-Handler ausgelöst wird, richtet das System eine temporäre interne Verbindung ein, auf der der Event-Handler ausgeführt wird. Der Handler wird nicht über die Verbindung ausgeführt, über die er ausgelöst wurde. Daher sind Anweisungen wie MESSAGE ... TO CLIENT, die mit der Clientanwendung interagieren, in Event-Handlern nicht sinnvoll. Außerdem sind Anweisungen nicht zulässig, die Ergebnismengen zurückgeben.

Die temporäre Verbindung, auf der die Verarbeitungsroutine läuft, wird in die Zählung der Verbindungen für die Lizenzierung nicht einbezogen, und die durch die Option login\_procedure angegebene Prozedur wird bei Ereignisverbindungen nicht ausgeführt.

Event-Handler werden über eine separate Verbindung mit den Privilegien des Ereigniseigentümers ausgeführt. Sie können auch eine Prozedur aus dem Event-Handler heraus aufrufen. In diesem Fall wird die Prozedur mit den Privilegien des Prozedureigentümers ausgeführt. Die separate Verbindung für den Event-Handler zählt nicht zu den zehn Verbindungen, auf die der Personal Datenbankserver beschränkt ist.

Etwaige Ereignisfehler werden im Meldungslog des Datenbankservers protokolliert.

**Hinweis**

Die Transaktion in einem Event-Handler wird festgeschrieben, wenn keine Fehler während der Ausführung erkannt werden, und sie wird zurückgesetzt, wenn Fehler erkannt werden. Siehe [Routine bei Ausnahmefehlern und atomare zusammengesetzte Anweisungen \[SQL Anywhere Server - SQL-Benutzerhandbuch\]](#).

**Siehe auch**

- [„Event-Handler \(Fehlerverarbeitungsroutinen\)“ auf Seite 1095](#)

## Datenbankereignisse erstellen

Mithilfe von Ereignissen können Sie Routineaufgaben automatisieren. Sie können geplante Ereignisse, Systemereignisse und manuelle Ereignisse erstellen.

**Voraussetzungen**

Sie müssen entweder das `MANAGE ANY EVENT`-Systemprivileg oder das `CREATE ANY OBJECT`-Systemprivileg haben.

**Kontext und Bemerkungen**

Wenn Sie Event-Handler entwickeln, können Sie später über Sybase Central oder die `ALTER EVENT`-Anweisung Zeitpläne oder Systemereignisse hinzufügen, um das Auslösen eines Ereignisses zu steuern.

Wenn Sie einen Event-Handler ohne Zeitplan oder Systemereignis zum Auslösen erstellen, wird er nur nach manueller Auslösung ausgeführt.

**Aufgabe**

1. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Ereignisse** und klicken Sie auf **Neu » Ereignis**.
3. Befolgen Sie die Anweisungen des **Assistenten zum Erstellen von Ereignissen**.

**Ergebnisse**

Das Ereignis wird zur Datenbank hinzugefügt.

**Siehe auch**

- [„CREATE EVENT-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„Aufgabenautomatisierung mit Abfolgeplanung und Ereignissen“ auf Seite 1087](#)
- [„Auslösen eines Event-Handlers“ auf Seite 1099](#)
- [„ALTER EVENT-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Auslösen eines Event-Handlers

Jeder Event-Handler kann nicht nur im Rahmen eines Zeitplans oder durch ein Systemereignis ausgelöst werden, sondern auch manuell.

### Voraussetzungen

Sie müssen das `MANAGE ANY EVENT`-Systemprivileg haben.

### Kontext und Bemerkungen

Das manuelle Auslösen von Ereignissen kann bei der Entwicklung von Event-Handlern nützlich sein und für bestimmte Ereignisse auch in Produktionsumgebungen. Beispiel: Wenn Sie einen Zeitplan für einen monatlichen Umsatzbericht erstellt haben, können Sie unabhängig vom Monatsende Umsatzberichte abrufen.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Ereignisse**.
3. Rechtsklicken Sie auf das Ereignis und klicken Sie auf **Trigger**.

Das Ereignis muss aktiviert sein, bevor Sie es auslösen können. Um ein Ereignis zu aktivieren, rechtsklicken Sie darauf und klicken Sie auf **Aktiviert**.

4. Im Feld **Parameter** geben Sie eine von Kommas unterteilte Liste von Parametern für das Ereignis ein. Zum Beispiel:

```
parameter=value,parameter=value
```

5. Klicken Sie auf **OK**.

### Ergebnisse

Der Event-Handler wird ausgelöst.

### Siehe auch

- „Event-Handler (Fehlerverarbeitungsroutinen)“ auf Seite 1095
- „`TRIGGER EVENT`-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Debugging von Event-Handlern

Sie können das Debugging eines Event-Handlers mit Sybase Central durchführen.

### Voraussetzungen

Sie müssen das `DEBUG ANY PROCEDURE`-Systemprivileg haben.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie auf **Modus » Debug**.
3. Doppelklicken Sie im linken Fensterausschnitt auf **Ereignisse**.
4. Doppelklicken Sie im rechten Fensterausschnitt auf das Ereignis, für das Sie das Debugging durchführen möchten.
5. Auf der Registerkarte **SQL** im rechten Fensterausschnitt drücken Sie F9, um einen Breakpoint zu setzen.

### Ergebnisse

Lösen Sie den Event-Handler mit der TRIGGER EVENT-Anweisung aus. Die Ausführung stoppt an dem Breakpoint, den Sie gesetzt haben.

### Siehe auch

- „Event-Handler (Fehlerverarbeitungsroutinen)“ auf Seite 1095
- „SQL Anywhere-Debugger“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „TRIGGER EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Ausblenden eines Event-Handlers

Um die Sicherheit zu erhöhen, können Sie die Definition für einen Event-Handler mit der ALTER EVENT-Anweisung ausblenden.

### Voraussetzungen

Sie müssen entweder das MANAGE ANY EVENT-Systemprivileg oder das ALTER ANY OBJECT-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine ALTER EVENT-Anweisung mit der SET HIDDEN-Klausel aus:

```
ALTER EVENT event-name SET HIDDEN
```

### Ergebnisse

Der Event-Handler wird in der Event-Handler-Definition, die in der Aktionsspalte der ISYSEVENT-Systemtabelle gespeichert ist, permanent verschleiert.

## Beispiel

Mit der folgenden Anweisung wird die Definition des Event-Handlers secret\_event ausgeblendet:

```
ALTER EVENT secret_event SET HIDDEN
```

## Siehe auch

- „Event-Handler (Fehlerverarbeitungsroutinen)“ auf Seite 1095
- „ALTER EVENT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SYSEVENT-Systemansicht“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

# Ereignisprotokollierung

Bei der Ereignisprotokollierung werden Informationen zu systemdefinierten und benutzerdefinierten Trace-Ereignissen in einem Ereignisprotokollierungsziel erfasst. Eine Trace-Sitzung besteht aus Trace-Ereignissen (bestimmten Punkten in der Datenbankserver-Software oder Ihrer SQL-Anwendung), deren Informationen gesammelt und in einem Ziel protokolliert werden. Ziele sind der Speicherort (z.B. eine Datei), an dem der Datenbankserver Trace-Ereignisse protokolliert.

Zu den während einer Ereignisprotokollierungssitzung protokollierten Informationen gehören die Informationen aus den angegebenen system- und benutzerdefinierten Trace-Ereignissen. Die Ereignisprotokollierung kann für die Diagnose von Datenbankserver- und Anwendungsproblemen, einschließlich Performanceproblemen, bei Produktionsdatenbanken verwendet werden.

- **System-Trace-Ereignisse** Dies sind Trace-Ereignisse, die der Datenbankserver generiert. Trace-Ereignisse werden generiert für Vorgänge wie das Starten oder Beenden eines Checkpoints sowie das Starten oder Stoppen einer Datenbank. Zum Abfragen der verfügbaren Systemereignisse und Systemereignisfelder können Sie die Systemprozedur sp\_trace\_events bzw. sp\_trace\_event\_fields verwenden. Ereignisfelder enthalten erforderliche Informationen zu dem Ereignis. Systemereignisse werden nicht beibehalten, wenn Sie eine Datenbank neu aufbauen, und welche Systemereignisse verfügbar sind, hängt von der Version des Datenbankservers ab. System-Trace-Ereignisse können sich beim Wechseln der Hauptversion ändern.
- **Benutzer-Trace-Ereignisse** Mit diesen Trace-Ereignissen werden Informationen aus einer Anwendung in einer Ereignisprotokollierungssitzung protokolliert. Benutzer-Trace-Ereignisse sind für alle Verbindungen mit der Datenbank sichtbar. Sie können ein Benutzer-Trace-Ereignis mithilfe der CREATE TEMPORARY TRACE EVENT-Anweisung erstellen.

## Ereignisprotokollierungsziele

Als Ereignisprotokollierungsziele werden nur ETD-Dateien unterstützt. ETD-Dateien sind plattformunabhängig und können mit dem Dienstprogramm dbmanageetd verarbeitet werden.

## Trace-Sitzungen

Eine Trace-Sitzung ist eine Sammlung von Trace-Ereignissen und Zielen für eine Datenbank. Trace-Sitzungen sind für alle Verbindungen mit der Datenbank sichtbar und bleiben erhalten, bis die Datenbank heruntergefahren wird.

## Schweregrade für Ereignisse

Die folgenden SQL-Schweregrade sind für alle Trace-Ereignistypen definiert:

Ebene	Schweregrad des Wertebereichs
ALWAYS	0
CRITICAL	1-50
ERROR	51-100
WARNING	101-150
INFORMATION	151-200
DEBUG	201-255

## Ereignisprotokollierung für Datenbanken einrichten

Führen Sie die folgenden Schritte aus, um die Ereignisprotokollierung für eine Datenbank einzurichten:

1. Erstellen Sie in Ihrer Anwendung Benutzer-Trace-Ereignisse für die Informationen, die Sie in das Diagnoselog einbeziehen möchten.
2. Erstellen Sie eine Prozedur, die die NOTIFY TRACE EVENT-Anweisung abruft.
3. Erstellen Sie eine Trace-Sitzung und fügen Sie ihr Trace-Ereignisse hinzu.
4. Starten Sie die Ereignisprotokollierungssitzung.

### Siehe auch

- „Tools für Performanceüberwachung und Diagnose“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „sp\_trace\_events-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „sp\_trace\_event\_fields-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE TEMPORARY TRACE EVENT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE TEMPORARY TRACE EVENT SESSION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Benutzer-Trace-Ereignisse erstellen

Erstellen Sie Benutzer-Trace-Ereignisse, um Informationen in Ihrer Anwendung zu protokollieren.

### Voraussetzungen

Sie müssen die Systemprivilegien `MANAGE ANY TRACE SESSION` und `NOTIFY TRACE EVENT` haben.

## Aufgabe

1. Erstellen Sie das erforderliche Benutzer-Trace-Ereignis für Ihre Datenbank.

Zum Beispiel:

```
CREATE TEMPORARY TRACE EVENT my_event( id INTEGER, information LONG
VARCHAR );
```

Sie können eine gespeicherte Prozedur erstellen, die beim Starten der Datenbank ausgeführt wird, um alle erforderlichen Benutzer-Trace-Ereignisse zu erstellen.

2. Führen Sie eine NOTIFY TRACE EVENT-Anweisung für jedes benutzerdefinierte Ereignis aus, das für die Datenbank protokolliert wird.

Zum Beispiel:

```
NOTIFY TRACE EVENT my_event( 1, 'Hello world' );
```

Die NOTIFY TRACE EVENT-Anweisung protokolliert Informationen zu Trace-Ereignissen in allen Trace-Sitzungen, für die das Ereignis relevant ist. Wenn ein Ereignis zum Zeitpunkt des Ausführens von NOTIFY TRACE EVENT nicht definiert ist, generiert der Datenbankserver einen Fehler. Wenn ein Ereignis nicht vorhanden ist, können Sie die NOTIFY TRACE EVENT-Anweisung in einem TRY-Block platzieren, um das Verhalten zu definieren.

## Ergebnisse

Das Trace-Ereignis bleibt bestehen, bis die Datenbank heruntergefahren wird.

## Nächste Schritte

Erstellen Sie eine Trace-Sitzung für die Datenbank. Siehe [„Trace-Sitzungen erstellen“ auf Seite 1103](#).

## Siehe auch

- [„CREATE TEMPORARY TRACE EVENT-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„NOTIFY TRACE EVENT-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„TRY-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Trace-Sitzungen erstellen

Erstellen Sie eine Trace-Sitzung, mit der Informationen zu Trace-Ereignissen im Diagnoselog erfasst werden können.

## Voraussetzungen

Sie müssen das MANAGE ANY TRACE SESSION-Systemprivileg haben.

Alle Benutzer-Trace-Ereignisse, die in NOTIFY TRACE EVENT-Anweisungen für die Datenbank referenziert werden, müssen vorhanden sein, es sei denn, die NOTIFY TRACE EVENT-Anweisung ist in

einem TRY-Block enthalten, der Fehler verarbeitet, wenn Benutzer-Trace-Ereignisse nicht vorhanden sind. Siehe [„Benutzer-Trace-Ereignisse erstellen“ auf Seite 1102](#).

### Aufgabe

- Führen Sie eine CREATE TEMPORARY TRACE EVENT SESSION-Anweisung aus.

Zum Beispiel:

```
CREATE TEMPORARY TRACE EVENT SESSION my_session
  ADD TRACE EVENT my_event, -- user event
  ADD TRACE EVENT SYS_ConsoleLog_Information -- system event
  ADD TARGET FILE ( SET filename_prefix='my_trace_file' );
```

Die ADD TRACE EVENT-Klauseln geben Benutzer- und System-Trace-Ereignisse an, die Teil der Sitzung sind. Die ADD TARGET FILE-Klausel gibt den Namen des Protokollierungsziels und optional diesem Ziel zugeordnete Parameter an.

### Ergebnisse

Die Trace-Sitzung wird für die Datenbank erstellt, muss aber manuell gestartet werden.

### Nächste Schritte

Starten Sie die Trace-Sitzung für die Datenbank.

### Siehe auch

- [„CREATE TEMPORARY TRACE EVENT SESSION-Anweisung“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

## Trace-Sitzungen starten oder stoppen

Starten Sie eine Trace-Sitzung, damit Informationen zu Trace-Ereignissen in den Ereignisprotokollierungszielen erfasst werden, und stoppen Sie die Trace-Ereignis-Sitzung, wenn Sie mit dem Erfassen der Informationen fertig sind.

### Voraussetzungen

Sie müssen das MANAGE ANY TRACE SESSION-Systemprivileg haben.

### Aufgabe

- Führen Sie eine ALTER TRACE EVENT SESSION-Anweisung aus, die den erforderlichen Zustand der Trace-Sitzung angibt: START oder STOP.

Die folgende Anweisung startet beispielsweise die Trace-Sitzung my\_session:

```
ALTER TRACE EVENT SESSION my_session
  STATE = START;
```

Die folgende Anweisung stoppt die Trace-Sitzung my\_session:

```
ALTER TRACE EVENT SESSION my_session
STATE = STOP;
```

## Ergebnisse

Nach dem Starten läuft die Sitzung, bis sie explizit gestoppt oder die Datenbank heruntergefahren wird.

## Nächste Schritte

Zeigen Sie den Inhalt der Diagnoselogdatei mithilfe des Dienstprogramms dbmanagetd an.

## Siehe auch

- „ALTER TRACE EVENT SESSION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Dienstprogramm für die Verwaltung von ETD-Dateien (dbmanagetd)“ auf Seite 918

# Inhalt der Diagnoselogdatei anzeigen

Zeigen Sie den Inhalt der Diagnoselogdatei mithilfe des Dienstprogramms für die Verwaltung von ETD-Dateien (dbmanagetd) an.

## Voraussetzungen

Ereignisprotokollierungsdaten aus einer Protokollierungssitzung müssen in einer ETD-Datei protokolliert sein.

## Aufgabe

1. Führen Sie das Dienstprogramm dbmanagetd aus, um den Inhalt der Diagnoselogdatei im Textformat anzuzeigen. Zum Beispiel:

```
dbmanagetd diagnostic-log.etd -o diagnostic-log.txt
```

2. Öffnen Sie die Datei in einem Texteditor.

Die folgende Tabelle enthält die möglichen Schweregrade für die Ereignisprotokollierung.

Ebene	Schweregrad des Wertebereichs
ALWAYS	0
CRITICAL	1-50
ERROR	51-100
WARNING	101-150
INFORMATION	151-200
DEBUG	201-255

## Ergebnisse

Das Diagnoselog wird generiert und kann in einem Texteditor angezeigt werden.

### Siehe auch

- [„Dienstprogramm für die Verwaltung von ETD-Dateien \(dbmanageetd\)“ auf Seite 918](#)

## Verfügbare Trace-Ereignisse auflisten

Zeigen Sie die benutzerdefinierten und systemdefinierten Trace-Ereignisse sowie deren Felder an, die im Diagnoselog erfasst werden können.

### Voraussetzungen

Das `MANAGE ANY TRACE SESSION`-Systemprivileg ist erforderlich.

### Aufgabe

1. Wenn Sie eine Liste aller Trace-Ereignisse anzeigen möchten, führen Sie die `sp_trace_events`-Systemprozedur aus.
2. Wenn Sie eine Liste der Felder für die Trace-Ereignisse anzeigen möchten, führen Sie die `sp_trace_event_fields`-Systemprozedur aus.

Die folgende Tabelle enthält die möglichen Schweregrade für die Ereignisprotokollierung.

Ebene	Schweregrad des Wertebereichs
<b>ALWAYS</b>	0
<b>CRITICAL</b>	1-50
<b>ERROR</b>	51-100
<b>WARNING</b>	101-150
<b>INFORMATION</b>	151-200
<b>DEBUG</b>	201-255

## Ergebnisse

Der Datenbankserver gibt eine Ergebnismenge zurück, in der die unterstützten Trace-Ereignisse aufgelistet werden.

### Siehe auch

- [„sp\\_trace\\_events-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„sp\\_trace\\_event\\_fields-Systemprozedur“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

# Fehlerbehandlung im Zusammenhang mit SQL Anywhere-Problemen

## Siehe auch

- „Häufig gestellte Fragen - SQL Anywhere“ [[SQL Anywhere 16 - Einführung](#)]
- „Tipps zum Verbessern der Performance“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Anwendungsprofilerstellung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SQL Anywhere-Monitor“ auf Seite 1115
- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 877
- „Performanceverbesserungen, Diagnosen und Monitoring“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Unerwartete Änderungen der Datenbankgröße

Datenbankseiten werden freigegeben, wenn alle Datensätze auf der Seite gelöscht werden. Wenn eine Datenbankseite freigegeben wird, wird sie für die Wiederbenutzung verfügbar, aber sie kann nicht aus der Datei entfernt werden. Spätere INSERT- und UPDATE-Anweisungen können die freigegeben Seiten verwenden.

Wenn die gewünschten Änderungen, wie Einfügungen, Aktualisierungen oder Löschungen, in der Datenbank vorgenommen werden, werden dem Rollback-Log, das im System-DBSpace gespeichert wird, Einträge hinzugefügt. Wenn viele dieser Vorgänge ausgeführt werden, bevor eine Festschreibung vorgenommen wird, kann das Rollback-Log sehr groß und die Größe der Datenbank erhöht werden.

Das Checkpoint-Log wird am Ende des System-DBSpace gespeichert. Wenn der Datenbankserver heruntergefahren wird, wird das Checkpoint-Log gekürzt und der System DBSpace nimmt ab. Seiten, die durch DELETE- oder TRUNCATE-Vorgänge freigegeben wurden, bleiben in der Datenbankdatei für die zukünftige Wiederverwendung und können nicht aus der Datei entfernt werden.

Wenn die Größe der Datenbankdatei zunimmt oder nicht in der erwarteten Form abnimmt, können Sie wie folgt vorgehen:

- Führen Sie häufig COMMIT-Anweisungen aus, wenn Sie INSERT-, UPDATE- oder DELETE-Anweisungen verwenden. Seiten, die dem Rollback-Log zugewiesen sind, werden bei der Ausführung einer COMMIT-Anweisung für die Wiederverwendung im System-DBSpace freigegeben.
- Führen Sie gelegentlich CHECKPOINT-Anweisungen aus, wenn Sie UPDATE- oder DELETE-Anweisungen verwenden oder wenn Sie bei großen Indizes INSERT-Anweisungen verwenden. Seiten im Checkpoint-Log werden nach jedem Checkpoint für die Wiederbenutzung durch das Checkpoint-Log verfügbar.
- Führen Sie eine TRUNCATE TABLE-Anweisung aus, die zu Löschungen auf Seitenebene führen kann. In diesen Fällen müssen dem Checkpoint-Log keine Kopien der Seiten hinzugefügt werden und die einzelnen Vorgänge auf Zeilenebene müssen nicht dem Rollback-Log hinzugefügt werden. Seiten, die durch TRUNCATE TABLE freigegeben wurden, sind erst nach dem nächsten Checkpoint

wiederverwendbar. TRUNCATE TABLE führt zu Löschungen auf Seitenebene, wenn folgende Bedingungen zutreffen:

- Es gibt keine Fremdschlüssel für bzw. von der gekürzten Tabelle.
- Die TRUNCATE TABLE-Anweisung wird nicht innerhalb eines Triggers ausgeführt.
- TRUNCATE TABLE wird nicht in Verbindung mit einem atomaren Vorgang ausgeführt.
- Die Checkpoint-Log-Seiten werden an das Ende der System-DBSpace-Datei geschrieben. Diese Seiten werden entfernt, wenn der Datenbankserver heruntergefahren wird.

Der Neuaufbau der Datenbank kann die Größe der Datenbank verringern, weil die neu aufgebaute Datenbank weniger freien Seiten hat.

## Fehlerbehandlung: Fehler in SQL Anywhere melden

Durch Einsenden von Performancedaten, z.B. Crash-Berichten und Diagnoseinformationen, können Sie zur Verbesserung des Produkts beitragen. Fehlerberichte werden unbegrenzt im Dateisystem Ihres Computers gespeichert.

### Voraussetzungen

Konfigurieren Sie ggf. Ihre Proxy-Host- und Port-Einstellungen.

### Kontext und Bemerkungen

Es werden alle Anstrengungen unternommen, um sicherzustellen, dass der Bericht keine vertraulichen Daten enthält, z.B. Ihren Netzwerk-Benutzernamen oder Ihr Kennwort.

### Aufgabe

- Führen Sie den folgenden Befehl aus:

```
dbsupport -sa
```

### Ergebnisse

Alle im Diagnoseverzeichnis gespeicherten Crash-Berichte und Diagnoseinformationen werden an das Softwareentwicklungsteam gesendet.

### Siehe auch

- [„Dienstprogramm für Supportanfragen \(dbsupport\)“ auf Seite 987](#)
- [Details zur Performancedatensammlung](#)

## Regelmäßig Performancedaten senden

Als Beitrag zur Verbesserung des Produkts bietet die Software die Möglichkeit, Performancedaten automatisch dem Software-Entwicklungsteam zu melden. Während der Installation wird diese Funktion standardmäßig aktiviert. Sie können diese Funktion ebenfalls aktivieren:

- In Interactive SQL durch Klicken auf **Extras » Optionen » Support**
- In Sybase Central durch Klicken auf **Hilfe » SQL Anywhere 16 » Suchfunktion für Updates konfigurieren**
- Mit dem Dienstprogramm für Supportanfragen (dbsupport) durch Angeben der Option -cc autosubmit  
Siehe „Dienstprogramm für Supportanfragen (dbsupport)“ auf Seite 987.

### OEM-Benutzer

Standardmäßig ist die Funktion, die automatisch Performancedaten an das Software-Entwicklungsteam sendet, beim Deployment der Administrationstools deaktiviert. Ihre Benutzer können diese Funktion jedoch in den Administrationstools aktivieren bzw. deaktivieren. Um zu verhindern, dass Ihre Benutzer die Einstellung ändern, ob ihre Daten eingesendet werden oder nicht, setzen Sie in der Datei *OEM.ini* die showPerformanceDataUI-Option auf FALSE.

Damit Ihre Benutzer Performancedaten an SAP senden können, müssen Sie das Dienstprogramm für Supportanfragen (dbsupport) mit der Option -cc autosubmit verwenden.

### Siehe auch

- „Dienstprogramm für Supportanfragen (dbsupport)“ auf Seite 987
- „Konfiguration der Administrationstools“ [*SQL Anywhere Server - Programmierung*]

## Fehlerbehandlung: Datenbanken für den technischen Support verschlüsseln

Wenn Sie eine Datenbank, die wiederhergestellt werden muss, verschlüsseln möchten, um sie an den technischen Support zu senden, müssen Sie die CREATE ENCRYPTED FILE-Anweisung verwenden. Alle zu der Datenbank gehörenden Dateien, z.B. Transaktionslogs und Transaktionslogspiegel sowie DBSpace-Dateien, müssen ebenfalls mit dieser Anweisung verschlüsselt werden. Siehe „CREATE ENCRYPTED FILE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

## Fehlerbehandlung beim Datenbankserverstart Sicherstellen der Gültigkeit der Transaktionslogdatei

Der Datenbankserver startet nicht, wenn das vorhandene Transaktionslog ungültig ist. Es kann z.B. während der Entwicklung vorkommen, dass Sie eine Datenbankdatei durch eine neue Version ersetzen, ohne gleichzeitig die Transaktionslogdatei zu löschen. Dies führt allerdings dazu, dass sich die Transaktionslogdatei von der Datenbank unterscheidet und dass die Transaktionslogdatei ungültig wird.

## Sicherstellen von genügend Festplattenspeicher für die temporäre Datei

SQL Anywhere verwendet eine temporäre Datei, um während der Ausführung Daten zu speichern. Diese Datei befindet sich normalerweise in dem Verzeichnis, auf das die SATMP-Umgebungsvariable zeigt, in der Regel `c:\temp`.

Wenn nicht genügend Festplattenspeicher für die temporäre Datei zur Verfügung steht, kommt es beim Start des Servers zu Problemen.

### Siehe auch

- „SATMP-Umgebungsvariable“ auf Seite 475

## Fehlersuche bei Startproblemen mit der Netzwerkkommunikation

Wenn der Server nicht startet und ein TCP/IP- oder Kommunikation-bezogener Fehler gemeldet wird, können Sie die Serveroption `-z` für die Fehlersuche verwenden. Die Startinformationen werden im Meldungsfenster des Datenbankservers angezeigt. Sie können die Option `-o` verwenden, wenn die Ergebnisse in einer Datei protokolliert werden sollen.

### Siehe auch

- „Datenbankserveroption `-z`“ auf Seite 312
- „Datenbankserveroption `-o`“ auf Seite 268

## Fehlerbehandlung bei Performancewarnungen des Datenbankservers

Die Performancewarnungen des Datenbankservers erscheinen in der Meldungslogdatei des Datenbankservers. Diese Warnungen werden gemeldet, wenn eine Datenbank oder ein Datenbankserver einen Zustand erreicht, der möglicherweise Auswirkungen auf seine Performance hat.

## Performancewarnung: Server-Cachegröße für die Datenbank %1 ist zu klein

Diese Warnung wird ausgegeben, wenn die maximale Cachegröße des Datenbankservers (die Obergrenze der Pufferpoolgröße des Datenbankservers, die vom Server berechnet oder explizit mit der Option `-ch` festgelegt wurde) weniger als 10 % der Gesamtgröße aller offenen DBSpaces für eine Datenbank beträgt.

Beispiel: Ein Datenbankserver, der eine Datenbank einer Größe von 21 GByte hostet, würde diese Warnung ausgeben, wenn die maximale Cachegröße des Servers weniger als 2,1 GByte beträgt. Diese Warnung wird pro Datenbank berechnet und möglicherweise nicht ausgegeben, wenn mehrere Datenbanken auf demselben Datenbankserver gestartet werden.

**Siehe auch**

- „Datenbankserveroption -ch “ auf Seite 221
- „Tipp: Performance durch den Einsatz des Cachespeichers steigern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Dynamische Cachedimensionierung“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Statistiken zum Überwachen der Cachegröße“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## **Performancewarnung: Seitengröße %1 der Datenbank %3 passt nicht zum Höchstwert von %2, der für den Server gesetzt wurde, was zu einer nicht effizienten Nutzung des Caches führt**

Die Seitengröße des Pufferpools des Datenbankservers muss mindestens so groß sein wie die Seitengröße einer Datenbank, die auf diesem Datenbankserver gestartet wurde. Ein Datenbankserver kann einen höheren Wert für die Seitengröße des Caches verwenden. Dies kann mit der Option -gp angegeben werden. Auf einem SQL Anywhere-Datenbankserver muss jedoch eine 1:1-Zuordnung zwischen Datenbankseiten und Seiten-Frames im Pufferpool bestehen. Jeder Seiten-Frame im Speicher kann nur eine Datenbankseite enthalten und eine Seite kann nur in einem Seiten-Frame enthalten sein. Wenn der Cache 8-KByte-Seiten verwendet, aber die Datenbank 4-KByte-Seiten verwendet, enthält jeder Cacheseiten-Frame im Speicher nur 4 KByte Daten und die anderen 4 KByte dieses Seiten-Frames werden nicht genutzt. Diese Situation führt zu einem Cache der Hälfte der gewünschten Größe.

**Siehe auch**

- „Datenbankserveroption -gp “ auf Seite 249
- „Hinweise zur maximalen Seitengröße“ auf Seite 160

## **Performancewarnung: Kein eindeutiger Index oder Primärschlüssel für die Tabelle %1 in der Datenbank %2**

Diese Warnung wird gemeldet, wenn eine Tabelle aktualisiert wird, die mehr als 10 Zeilen enthält und nicht über einen Primärschlüssel bzw. einen eindeutigen Index verfügt.

In SQL Anywhere enthält das Transaktionslog logische Zeilenvorgänge (UPDATE, INSERT und DELETE) und nicht die Änderungen von physischen Seiten. Zeilenvorgänge im Transaktionslog werden vom Wert des Primärschlüssels oder des eindeutigen Indexes identifiziert, sodass beim Wiederherstellen einer Datenbank die aktualisierten Werte für den Vorgang im Transaktionslog auf die richtige Zeile angewendet werden können. Wenn kein Primärschlüssel bzw. kein eindeutiger Index vorhanden ist, werden alle Werte in der Zeile als Primärschlüssel der Zeile verwendet. Dieses Verhalten kann zu einem erheblichen Anwachsen des Transaktionslogs führen. Eine Tabelle, die keinen Index enthält, kann zu langsamen Wiederherstellungszeiten der Datenbank führen.

**Siehe auch**

- „Hinweise zur Transaktionsloggröße“ auf Seite 138
- „Indizes“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Das Transaktionslog“ auf Seite 135

## Performancewarnung: Seitengröße für die Datenbank %1 ist zu klein

Diese Performancewarnung wird gemeldet, wenn eine Datenbank alle folgenden Bedingungen erfüllt:

1. Die Datenbankseitengröße beträgt 2 KByte.
2. Die Anzahl der Seiten in der gesamten Datenbank ist größer als 100000, entsprechend einer Datenbankgröße von etwa 200 MByte.

Es wird empfohlen, die Datenbank zu entladen und sie dann in eine neue Datenbank mit einer Seitengröße von 4 KByte oder größer neu zu laden, um erhöhte Speichereffizienz und eine bessere Performance zu erreichen.

### Siehe auch

- „Neuaufbau von Datenbanken“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Tipp: Angemessene Seitengröße verwenden“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Performancewarnung: Datenbankdatei %1 besteht aus %2 Festplattenfragmenten

Wenn eine Datenbank auf einem Datenbankserver gestartet wird, meldet SQL Anywhere die Anzahl der Dateifragmente für die Hauptdatenbankdatei, wie vom Betriebssystem gemeldet. Übermäßige Plattenfragmentierung des Datenträgers, auf dem sich die Datenbank befindet, kann zu Performanceproblemen führen, da Fragmentierung zu zusätzlicher Verarbeitungszeit des Datenträgers während der I/O-Vorgänge führen kann.

Das Problem der Dateisystemfragmentierung ist unabhängig von der Tabellenseitenfragmentierung innerhalb der Datenbank. Die Analyse und Lösung dieser separaten Probleme erfolgt mit anderen Methoden und Tools. Die Anzahl der Dateifragmente wird nur für Windows-basierte SQL Anywhere-Datenbankserver gemeldet. Unix-Dateisysteme, einschließlich Linux-Dateisysteme, verursachen deutlich weniger Fragmentierungsprobleme als Windows-basierte Systeme.

Auf Windows-Plattformen bestehen Datenbankdateien im Allgemeinen aus mehr als einem Fragment. Wenn Sie folgende Meldung für eine Datenbank erhalten, hilft Ihnen die Anzahl der Fragmente relativ zur Größe der Datenbankdatei dabei festzulegen, ob der Systemadministrator bestimmte Aktionen durchführen muss. Beispiel: Eine 100-GB-Datei, die aus 25 Fragmenten besteht, sollte kein besonderes Problem darstellen. Eine 50-MB-Datei, die aus 300 Speicherfragmenten besteht, kann dagegen möglicherweise Performanceprobleme aufweisen. Um Probleme mit der Dateifragmentierung auszuschalten, sollten Sie die Datenbank in einer eigenen Plattenpartition speichern und dann regelmäßig eines der Windows-Dienstprogramme zur Platten-Defragmentierung ausführen.

### Siehe auch

- „Tipp: Fragmentierung reduzieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Tabellenfragmentierung reduzieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Tabellenfragmentierung reduzieren“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- DBFileFragments-Datenbankeigenschaft auf Seite 772

## Performancewarnung: In der Datenbank %3, Tabelle %1 ist die AUTOINCREMENT-Spalte %2 nicht indiziert

Diese Warnung wird gemeldet, wenn eine permanente Basistabelle eine AUTOINCREMENT-Spalte enthält und es keinen Index für die Spalte gibt. Die Warnung wird nur in Fällen generiert, in denen der maximale Identity-Wert für die betreffende Spalte, der in der MAX\_IDENTITY-Spalte in der ISYSTABCOL-Katalogtabelle gespeichert ist, unbekannt ist oder ungültig wird. Diese Situation kann auftreten, wenn eine vorhandene Spalte in eine AUTOINCREMENT-Spalte geändert wurde oder die globalen Autoinkrement-Einstellungen für die Datenbank geändert wurden.

### Siehe auch

- „ISYSTABCOL-Systemtabelle“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Der Standardwert "Autoincrement"“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Der Standardwert GLOBAL AUTOINCREMENT“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Performancewarnung: Ansicht %1 in Datenbank %2 wurde aufgrund von DDL-Vorgängen auf einem ihrer referenzierten Objekte außer Kraft gesetzt

Diese Warnung wird gemeldet, wenn ein DDL-Vorgang eine vorhandene Ansicht ungültig macht. Wenn eine Ansicht von einem Schema-Objekt, das geändert wurde, abhängig ist und die Ansicht anschließend nicht neu kompiliert werden kann, bleibt der Status für diese Ansicht "UNGÜLTIG". Bei jeder folgenden Referenz von einer Abfrage, versucht der Datenbankserver die Ansicht neu zu kompilieren.

### Siehe auch

- „Abhängigkeiten und Vorgänge, die ein Schema ändern“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Ansichten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Status für reguläre Ansichten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Fehlerbehandlung für Netzwerkverbindungen

Für die Netzwerksoftware sind mehrere Komponenten erforderlich, und das erhöht die Wahrscheinlichkeit, dass Probleme auftreten. Obwohl hier einige Hinweise zur Fehlerbehandlung enthalten sind, ist die wichtigste Quelle der Unterstützung bei der Fehlerbehandlung Ihre IT-Abteilung oder der Netzwerkadministrator.

## Verwenden Sie die Protokollierung

Wenn Sie die Datenbankserveroptionen -z und -o angeben, werden Diagnosemeldungen und andere Meldungen für Fehlerbehandlungszwecke im Meldungsfenster des Datenbankservers protokolliert. Wenn Sie auf dem Client den Verbindungsparameter LogFile in Ihre Verbindungszeichenfolge einfügen, werden Diagnosemeldungen zur Kommunikation in einer Datei gespeichert. Diese Meldungen geben Hinweise

zur Diagnose der fehlgeschlagenen Verbindung und enthalten Informationen darüber, welche Verbindungsparameter beim Verbindungsversuch verwendet werden und welche Kommunikationsverbindungen verwendet wurden.

### Siehe auch

- [„Datenbankserveroption -z “ auf Seite 312](#)
- [„Verbindungsparameter LogFile \(LOG\)“ auf Seite 371](#)

## Timeoutwerte anpassen

Wenn es zu Problemen mit abrupt abbrechenden Verbindungen kommt, sollten Sie das Verfügbarkeits- oder Inaktivitäts-Timeout anpassen.

### Siehe auch

- [„LivenessTimeout-Verbindungsparameter \(LTO\)“ auf Seite 370](#)
- [„Datenbankserveroption -tl “ auf Seite 292](#)
- [„Verbindungsparameter Idle“ auf Seite 365](#)
- [„Datenbankserveroption -ti “ auf Seite 291](#)

---

# Datenbank-Monitoring

Dieser Abschnitt beschreibt, wie Sie den SQL Anywhere-Monitor verwenden, um Ihre SQL Anywhere-Datenbanken und MobiLink-Server zu überwachen. Er beschreibt auch, wie Sie den SQL Anywhere SNMP Extension Agent einrichten und konfigurieren.

## SQL Anywhere-Monitor

Der SQL Anywhere-Monitor, auch als Monitor bezeichnet, ist ein browserbasiertes Administrationstool, das Informationen über Zustand und Verfügbarkeit von SQL Anywhere-Datenbanken (einschließlich Datenbanken in Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen), MobiLink-Servern, MobiLink-Serverfarmen und Relay Server-Farmen bereitstellt.

Der Monitor stellt folgende Funktionen bereit:

- **Fortlaufende Datensammlung** Im Gegensatz zu vielen anderen Administrationstools sammelt der Monitor ständig Metriken, auch wenn Sie nicht beim Browser angemeldet sind. Der Monitor sammelt Metriken, bis Sie ihn herunterfahren.
- **E-Mail-Alarm** Während die Metriken gesammelt werden, überprüft sie der Monitor und kann E-Mail-Benachrichtigungen versenden, wenn anzunehmen ist, dass in einer Ressource eine Störung vorliegt.
- **Browserbasierte Benutzeroberfläche** Sie können sich jederzeit über einen Webbrowser am Monitor anmelden, um Alarmer und gesammelte Metriken zu prüfen.
- **Überwachen mehrerer Datenbanken, MobiLink-Server, MobiLink-Serverfarmen und Relay Server-Farmen** Mit einem einzigen Tool können Sie gleichzeitig mehrere Ressourcen überwachen, die auf demselben oder verschiedenen Computern laufen.
- **Minimale Auswirkungen auf die Performance** Der Monitor kann routinemäßig in Entwicklungs- und Produktionsumgebungen eingesetzt werden, weil die Überwachungsfunktionen die Performance nicht beeinträchtigen.

Der Monitor ist so ausgelegt, dass ihn alle Benutzer (unabhängig davon, ob sie Datenbankadministratoren sind) verwenden können, die für Aufgaben wie die folgenden verantwortlich sind:

- Sicherstellen, dass eine Datenbank, ein MobiLink-Server oder eine Relay Server-Farm mit dem Netzwerk verbunden ist.
- Sicherstellen, dass genügend Plattenspeicher oder Speicher für eine Datenbank, einen MobiLink-Server oder eine Relay Server-Farm verfügbar ist.
- Sicherstellen, dass Benutzer nicht blockiert werden oder Abfragen zu lange dauern.
- Prüfung der Anzahl von Synchronisationen, die ein MobiLink-Server in einem bestimmten Zeitraum durchführt.

- Sicherstellen, dass ein Relay Server bereit ist, das Verkehrsaufkommen weiterzuleiten.
- Prüfen von Verkehrsaufkommen, Durchsatz und Ausfallquote einer Relay Server-Farm.

### Siehe auch

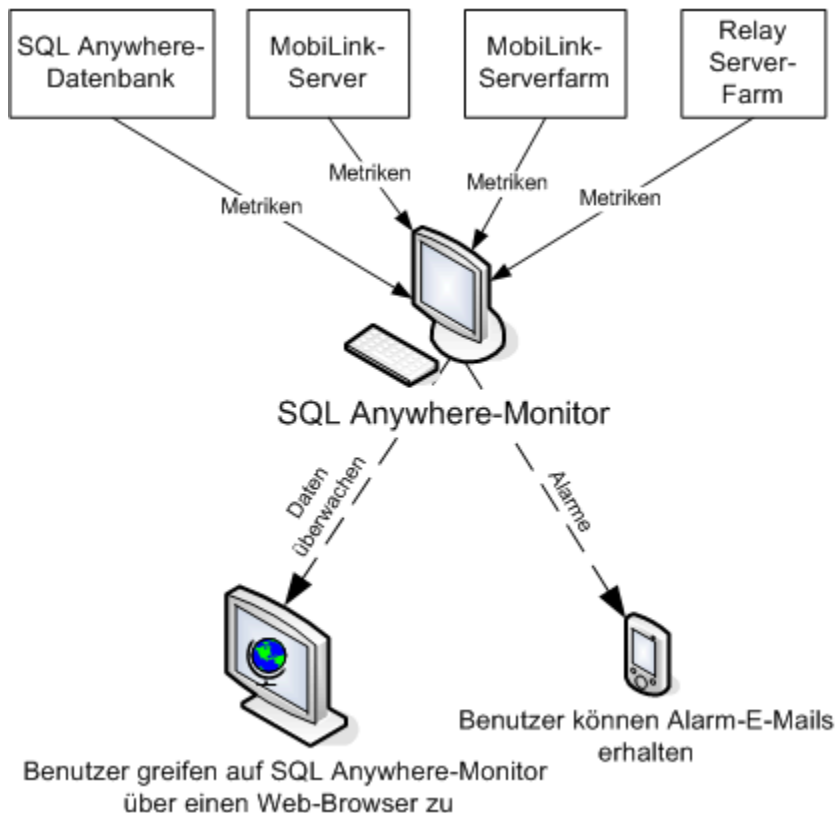
Hinweise zu anderen Administrations- und Performance-Tools, die für Datenbanken verfügbar sind, finden Sie hier:

- „Anwendungsprofilerstellung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „SQL Anywhere-Konsolendienstprogramm (dbconsole)“ auf Seite 981
- „Funktionen des Sybase Central-Systemmonitors zum Überwachen von Statistiken“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Optionen des Windows-Systemmonitors“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Dienstprogramm für Performancestatistik (dbstats) (Unix)“ auf Seite 953

Hinweise zu anderen Administrations- und Performance-Tools, die für MobiLink-Server eingesetzt werden können, finden Sie an folgenden Stellen „[MobiLink-Profiler](#)“ [[MobiLink - Serveradministration](#)].

## Architektur des Monitors

Der Monitor sammelt Metriken und Performancedaten von Datenbanken (einschließlich Datenbanken in Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen), MobiLink-Servern, MobiLink-Serverfarmen und Relay Server-Farmen, die auf anderen Computern laufen, wobei der Zugriff auf den Monitor von einem separaten Computer aus über einen Browser erfolgt.



Der Monitor ist eine Flash-basierte Anwendung, die über den in SQL Anywhere integrierten HTTP-Server in einem Webbrowser bereitgestellt wird. Die Interaktion mit dem Monitor erfolgt über dessen Browserschnittstelle.

Es gibt zwei Versionen des Monitors:

- **SQL Anywhere-Monitor Developer Edition** Monitor Developer Edition ist für die Verwendung in Entwicklung und Tests vorgesehen. Das Tool wird standardmäßig mit SQL Anywhere installiert und nutzt die installierte Software auf dem Backend-Server.
- **SQL Anywhere-Monitor - Produktionsversion** Die Produktionsversion ist für die Verwendung in Deployments und Produktion vorgesehen. Sie wird getrennt installiert und als Dienst ausgeführt und enthält eine vollständig in sich geschlossene SQL Anywhere-Installation. Diese Edition ist nur für bestimmte Editionen der Software verfügbar.

## Anforderungen

### Für den Computer, auf dem der Monitor installiert ist

- Um den SQL Anywhere-Monitor auf einem Windows-System mit aktivierter Windows-Firewall ausführen zu können, müssen Sie eine Ausnahme für Port 4950 hinzufügen.
- Der Monitor reserviert beim Starten 384 MB virtuellen Adressraum. Beim Starten des Monitors unter Linux müssen Sie sich vergewissern, dass mindestens so viel virtueller Speicher zur Verfügung steht.

- Wenn Sie Ressourcen überwachen möchten, die mithilfe von FIPS-zertifizierter Verschlüsselung gesichert sind, benötigen Sie eine separate Lizenz.
- Der Monitor kann auf demselben Computer ausgeführt werden wie die überwachten Ressourcen. Besonders in Produktionsumgebungen wird jedoch empfohlen, dass Sie den Monitor auf einem anderen Computer ausführen, um die Auswirkungen auf den Datenbankserver, den MobiLink-Server, die Relay Server-Farm oder andere Anwendungen möglichst gering zu halten.
- Es wird empfohlen, in der Produktionsumgebung die Monitor Production Edition auszuführen.
- Wenn Sie die Monitor Developer Edition ausführen möchten, muss SQL Anywhere 16 oder höher installiert sein. Die Monitor Developer Edition verwendet die SQL Anywhere-Installation auf dem Backend.

### Weitere Informationen zu dem Computer, der auf den Monitor zugreift

- Installieren Sie die neueste Version des Adobe Flash Players für Ihr Betriebssystem. Der Monitor ist kompatibel mit Version 10 von Adobe Flash Player. Um die richtige Version zu ermitteln, besuchen Sie <http://www.adobe.com/products/flashplayer/systemreqs/>.
- Aktivieren Sie JavaScript in Ihrem Browser.
- Stellen Sie sicher, dass der Computer, auf dem Sie über einen Browser auf den Monitor zugreifen, mit dem Netzwerk verbunden sein, in dem der Monitor installiert ist.

Sie können über den Computer auf den Monitor zugreifen, auf dem er ausgeführt wird, aber insbesondere für Produktionsumgebungen wird empfohlen, über einen anderen Computer auf den Monitor zuzugreifen.

### Einschränkungen

- Sie können auf einem Computer nur eine Version des Monitors gleichzeitig ausführen.
- Unter Linux kann die Monitor Developer Edition nur von dem Benutzer ausgeführt werden, der sie installiert hat.
- Unter Linux kann nur der Benutzer mit Linux-Administratorprivileg die Monitor Production Edition installieren und ausführen.
- Der Monitor stellt Verbindungen mit Datenbanken über TCP/IP her. Um eine Datenbank zu überwachen, die auf dem lokalen Datenbankserver (dbeng16) läuft, starten Sie den Datenbankserver mit der Option -x all oder Option -x tcpip.
- Sie können den Monitor nicht verwenden, um Abfragen zu optimieren oder die Geschwindigkeit Ihrer Anwendung zu ermitteln. Wenn Sie die Performance von Datenbanken und Anwendungen verbessern möchten, können Sie spezielle Tools einsetzen, etwa den **Assistenten für die Anwendungsprofilerstellung**, den **Sybase Central-Systemmonitor** oder den **Windows-Systemmonitor**.
- Der SQL Anywhere-Monitor stellt keine Informationen über einzelne Synchronisationen bereit. Detaillierte Informationen zu einzelnen Synchronisationen, einschließlich Timing- und anderer Synchronisationsstatistiken, erhalten Sie mithilfe des MobiLink-Profilers.

- Weitere Hinweise zu den Versionen von Datenbanken, MobiLink-Servern, MobiLink-Serverfarmen und Relay Server-Farmen, die der Monitor unterstützt, finden Sie unter den [unterstützten Plattformen](#).

### Siehe auch

- „Monitor Production Edition“ auf Seite 1194
- „Sicherheit der Monitor-Kommunikation“ auf Seite 1197.
- „MobiLink-Profiler“ [*MobiLink - Serveradministration*].

## Schnellstart zur Verwendung des Monitors

Die folgenden Schritte sind erforderlich, um die Überwachung von Datenbanken, MobiLink-Servern und MobiLink-Serverfarmen sowie Relay Server-Farmen einzurichten:

1. Starten Sie die Datenbank, den MobiLink-Server oder die Relay Server-Farm für die Überwachung (falls noch nicht geschehen).
2. Installieren Sie den Monitor auf einem Computer, der ständig mit Ihrem Netzwerk verbunden ist.

Der Monitor kann auf demselben Computer ausgeführt werden wie die überwachten Ressourcen. Besonders in Produktionsumgebungen wird jedoch empfohlen, dass Sie den Monitor auf einem anderen Computer ausführen, um die Auswirkungen auf die Ressourcen oder andere Anwendungen möglichst gering zu halten.

3. Starten Sie den Monitor und öffnen Sie ihn in Ihrem Browser. Siehe „[Monitor starten](#)“ auf Seite 1120.
4. Melden Sie sich beim Monitor als Administrator an. Der Standardbenutzer ist ein Administrator mit dem Namen **admin** und dem Kennwort **admin**.

#### Hinweis

Sie müssen beim Monitor als Administrator angemeldet sein, um die folgenden Aufgaben auszuführen. Siehe „[Monitor-Benutzer](#)“ auf Seite 1175.

5. Klicken Sie als Monitor-Administrator im linken Navigationsmenü auf **Extras » Administration** und fügen Sie die zu überwachende Ressource hinzu. Siehe „[Datenbankressourcen hinzufügen](#)“ auf Seite 1133 und „[MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen](#)“ auf Seite 1135.
6. Fügen Sie als Monitor-Administrator neue Benutzer hinzu und ändern Sie das Kennwort für den Admin-Benutzer. Siehe „[Monitor-Benutzer erstellen](#)“ auf Seite 1176.
7. Konfigurieren Sie als Monitor-Administrator Alarm-Schwellenwerte für die Ressourcen. Siehe „[Alarmer](#)“ auf Seite 1181.
8. Konfigurieren Sie als Monitor-Administrator den Sicherungs- und Wartungszeitplan. Siehe „[Sichern des Monitors](#)“ auf Seite 1191.
9. Klicken Sie auf **Schließen**, um das Fenster **Administration** zu verlassen.

10. Klicken Sie auf **Übersicht**. Im Widget **Ressourcenliste** finden Sie die überwachten Ressourcen. Siehe „Dashboards“ auf Seite 1124.

## Monitor starten

Starten Sie den Monitor und melden Sie sich an.

### Voraussetzungen

Vergewissern Sie sich, dass keine andere Kopie des Monitors auf dem Computer läuft.

### Kontext und Bemerkungen

Standardmäßig wird die Monitor Production Edition nach dem Installieren automatisch als Dienst ausgeführt und beim Hochfahren des Computers gestartet. Wenn Sie die Monitor Production Edition gestoppt haben, können Sie ihn anhand dieser Anweisungen neu starten.

### Aufgabe

1. Starten Sie den Monitor auf dem Computer, auf dem er installiert ist.

#### Unter Windows

- a. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » SQL Anywhere-Monitor**.
- b. Alternativ können Sie für die Monitor Production Edition die Batchdatei *samonitor* im Verzeichnis *bin32* oder *bin64* im Monitor-Installationsverzeichnis ausführen, um den Dienst neu zu starten.

```
samonitor.bat start
```

**Unter Linux** Führen Sie das Skript *samonitor.sh* im Verzeichnis *bin32* oder *bin64* im Monitor-Installationsverzeichnis aus:

```
./samonitor.sh launch
```

Der Monitor stellt Verbindungen mit den Ressourcen her und beginnt mit dem Sammeln von Metriken für alle zu überwachenden Ressourcen.

#### Hinweis

Beim Starten der Monitor Developer Edition wird das Monitor-Symbol in der Taskleiste angezeigt.

2. Wechseln Sie zur URL für das Anmelden beim Monitor. Die Standard-URL ist *http://localhost:4950*.

#### Hinweis

Wenn Sie über ein Netzwerk auf den Monitor zugreifen, navigieren Sie zu **http://computer-name:4950**, wobei *computer-name* der Name des Computers ist, auf dem der Monitor läuft. Siehe „Anmelden beim Monitor von einem entfernten Computer aus“ auf Seite 1122.

### 3. Melden Sie sich an.

Im Browser geben Sie Ihren Benutzernamen und Ihr Kennwort für den Monitor ein. Bei Benutzernamen und Kennwort für den Monitor spielt die Groß- und Kleinschreibung eine Rolle. Es gibt drei verschiedenen Benutzertypen: Administratoren, Operatoren und Benutzer ohne Schreibrechte. Jeder Benutzertyp hat unterschiedliche Privilegien. Der Standardbenutzer ist ein Monitor-Administrator mit dem Namen **admin** und dem Kennwort **admin**.

Sie können auf **Anmeldedaten auf diesem Computer speichern** klicken, damit Ihre Sitzung für zwei Wochen oder bis zu Ihrer Abmeldung bestehen bleibt. Wenn **Anmeldedaten auf diesem Computer speichern** nicht aktiviert ist, läuft die Sitzung ab, wenn Sie den Browser schließen oder sich abmelden.

## Ergebnisse

Der Monitor wird gestartet.

## Nächste Schritte

Der Monitor ist so ausgelegt, dass er dialogfrei im Hintergrund ausgeführt wird. Die Interaktion mit dem Monitor erfolgt über dessen Browserschnittstelle. Es wird empfohlen, dass Sie den Monitor kontinuierlich im Hintergrund ausführen, um Metriken zu sammeln.

## Siehe auch

- [„Monitor-Benutzer“ auf Seite 1175](#)
- [„Stoppen des Monitors“ auf Seite 1121](#)
- [„Abmelden vom Monitor“ auf Seite 1123](#)
- [„Dashboards“ auf Seite 1124](#)

# Stoppen des Monitors

Beim Stoppen der Monitor Production Edition wird der Monitor-Dienst gestoppt und das Sammeln der Metriken beendet.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

### Vorsicht

Für die meisten Fälle wird empfohlen, dass Sie den Monitor aktiv lassen, aber den Browser schließen. Das Schließen des Browsers beendet nicht die Sammlung der Metriken.

Weitere Hinweise dazu, wie Sie die Überwachung einer bestimmten Datenbank, eines MobiLink-Servers oder einer MobiLink-Serverfarm sowie einer Relay Server-Farm stoppen können, finden Sie unter [„Überwachung der Ressourcen stoppen“ auf Seite 1144](#).

## Aufgabe

- Stoppen Sie den Monitor.
  - **Unter Windows** Wählen Sie eine der folgenden Optionen:

Option	Aktion
Monitor Developer Edition	Rechtsklicken Sie in der Taskleiste auf das Monitor-Symbol und klicken Sie auf <b>SQL Anywhere-Monitor beenden</b> .
Monitor Production Edition	Führen Sie <i>samonitor.bat</i> im Verzeichnis <i>bin32</i> im Monitor-Installationsverzeichnis aus:  <code>samonitor.bat stop</code>

- **Unter Linux** Wählen Sie eine der folgenden Optionen:

Option	Aktion
Monitor Developer Edition	<code>./samonitor.sh stop</code>
Monitor Production Edition	<code>samonitor.sh stop</code>

Führen Sie das Skript *samonitor.sh* im Verzeichnis *bin32* oder *bin64* im Monitor-Installationsverzeichnis aus:

## Ergebnisse

Der Monitor wird gestoppt und beendet das Sammeln von Metriken für alle Ressourcen.

## Siehe auch

- „Monitor starten“ auf Seite 1120
- „Anmelden beim Monitor von einem entfernten Computer aus“ auf Seite 1122
- „Abmelden vom Monitor“ auf Seite 1123
- „Dashboards“ auf Seite 1124

## Anmelden beim Monitor von einem entfernten Computer aus

Jeder Benutzer kann sich von einem entfernten Computer aus beim Monitor anmelden, indem er zur URL für den Monitor navigiert.

## Voraussetzungen

Der Computer, von dem aus Sie sich beim Monitor anmelden, muss mit dem Netzwerk verbunden sein, in dem der Monitor läuft.

## Aufgabe

1. Starten Sie den Monitor auf dem Computer, auf dem er installiert ist.
2. Navigieren Sie auf dem Computer, der auf den Monitor zugreift, zur Standard-URL für die Anmeldung beim Monitor: **http://computer-name:4950**, wobei *computer-name* der Name des Computers ist, auf dem der Monitor läuft. Beispiel: *http://samplehost:4950*.
3. Nach Aufforderung geben Sie Ihren Benutzernamen und Ihr Kennwort für den Monitor ein. Der Benutzername und das Kennwort für den Monitor berücksichtigen die Groß- und Kleinschreibung.

## Ergebnisse

Sie werden vom entfernten Computer aus beim Monitor angemeldet.

## Siehe auch

- „Monitor starten“ auf Seite 1120
- „Monitor-Benutzer“ auf Seite 1175
- „Stoppen des Monitors“ auf Seite 1121
- „Abmelden vom Monitor“ auf Seite 1123
- „Dashboards“ auf Seite 1124

# Abmelden vom Monitor

Jeder Benutzer kann sich vom Monitor abmelden, indem er auf **Abmelden** klickt.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Das Abmelden vom Monitor hat *keine* Auswirkungen auf das Sammeln der Metriken.

## Aufgabe

- Klicken Sie in der oberen rechten Ecke auf **Abmelden**.

Wenn Sie während des Anmeldens beim Monitor auf **Anmeldedaten auf diesem Computer speichern** klicken, werden Sie beim Schließen des Browsers nicht vom Monitor abgemeldet.

## Ergebnisse

Sie werden vom Monitor abgemeldet.

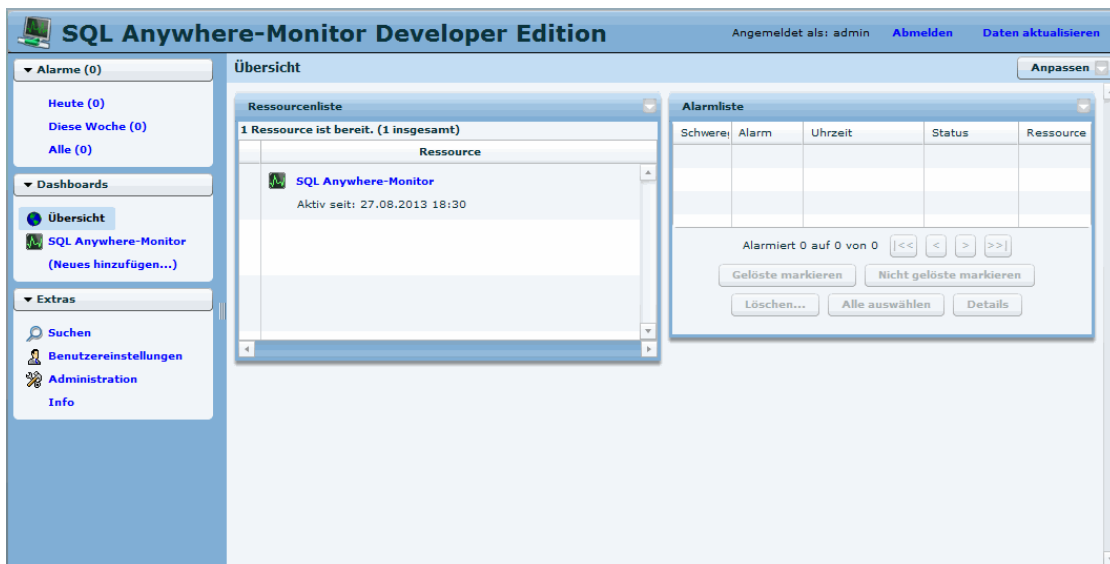
## Siehe auch

- „Überwachung der Ressourcen stoppen“ auf Seite 1144
- „Monitor starten“ auf Seite 1120
- „Stoppen des Monitors“ auf Seite 1121
- „Anmelden beim Monitor von einem entfernten Computer aus“ auf Seite 1122
- „Dashboards“ auf Seite 1124

## Dashboards

Das Dashboard **Übersicht** bietet einen Überblick über Zustand und Verfügbarkeit der überwachten Ressourcen (z.B. Datenbanken, MobiLink-Server und MobiLink-Serverfarmen oder Relay Serverfarmen).

Standardmäßig enthält das Dashboard **Übersicht** die Widgets **Ressourcenliste** und **Alarmliste**.






## Widget Ressourcenliste

Das Widget **Ressourcenliste** enthält eine Tabelle mit den überwachten Ressourcen und gibt Hinweise zum allgemeinen Zustand der einzelnen Ressourcen. Die Tabelle enthält immer die Standardressource mit dem Namen **SQL Anywhere-Monitor**, welche Berichte über den Zustand des Monitors selbst liefert. Sie können die Ressource **SQL Anywhere-Monitor** nicht ändern und ihre Überwachung nicht stoppen.

Wenn Sie Detailinformationen zu einer Ressource anzeigen möchten, klicken Sie in der **Ressourcenliste** auf den Ressourcennamen. Dadurch wird das Dashboard für die ausgewählte Ressource geöffnet.

Im Widget **Ressourcenliste** enthält die Spalte **Zustand** Informationen über die Verbindungen zwischen dem Monitor und seinen Ressourcen. Die Spalte **Status** gibt an, ob die Ressource die Durchführung einer Aktion erfordert.




Der Überwachungsstatus der Ressource kann sein:

Symbol	Status	Beschreibung
Kein Symbol vorhanden	<b>Problemlos</b>	Es gibt keine nicht aufgelösten Alarme für die Ressourcen.
	<b>Alarme vorhanden</b>	Mindestens ein nicht aufgelöster Alarm ist für die Ressource vorhanden.
	<b>Nicht verfügbar</b>	Die Ressource steht nicht mehr zur Verfügung. Beispiel: Die Ressource wurde heruntergefahren.
	<b>Überwachung angehalten</b>	Die Ressource wird nicht überwacht, entweder aufgrund eines Blackouts oder weil ein Benutzer die Überwachung der Ressource manuell angehalten hat.



### Widget Alarmliste


Das Widget **Alarmliste** enthält die Alarme für die überwachten Datenbanken, MobiLink-Server und MobiLink-Serverfarmen sowie Relay Server-Farmen. Wenn Sie Detailinformationen zu einem Alarm anzeigen möchten, klicken Sie in der **Alarmliste** auf den Alarm und klicken Sie anschließend auf **Details**. Dadurch wird ein Fenster mit den Details des Alarms geöffnet.

Der Status des Alarms kann sein:

Symbol	Status	Beschreibung
	<b>Aktiv</b>	Die Alarmbedingung gilt noch immer. Niemand hat den Alarm gelöst.
	<b>Inaktiv</b>	Das Problem, durch das der Alarm ausgelöst wurde, besteht zwar nicht mehr, aber der Alarm wurde nicht gelöst oder gelöscht.
	<b>Gelöst</b>	Ein Monitor-Administrator oder -Operator hat den Alarm als aufgelöst markiert.

Ein Alarm hat einen der folgenden Schweregrade:

Symbol	Schweregrad	Beschreibung
	Schweregrad "Hoch"	Alarme des Schweregrads "Hoch" zeigen Probleme an, die sofort die Aufmerksamkeit eines Benutzers erfordern. Wenn zum Beispiel eine Ressource den Schwellenwert "Festplattenspeicher wird knapp" überschreitet, wird ein Alarm des Schweregrads "Hoch" ausgegeben.
	Schweregrad "Mittel"	Alarme des Schweregrads "Mittel" zeigen Probleme an, die die Aufmerksamkeit eines Benutzers erfordern, da sie eskalieren könnten. Wenn zum Beispiel eine Ressource den Schwellenwert für die CPU-Nutzung überschreitet, wird ein Alarm des Schweregrads "Mittel" ausgegeben.

Symbol	Schweregrad	Beschreibung
	Schweregrad "Niedrig"	Alarme des Schweregrads "Niedrig" zeigen Probleme an. Wenn zum Beispiel bei einer Ressource eine fehlgeschlagene Verbindung vorliegt, wird ein Alarm des Schweregrads "Niedrig" ausgegeben.

#### Siehe auch

- [„Dashboards verwalten“ auf Seite 1126](#)
- [„Widgets“ auf Seite 1127](#)
- [„Alarme“ auf Seite 1181](#)

## Dashboards verwalten

Dashboards sind benutzerspezifisch. Jeder Benutzer kann eigene Dashboards hinzufügen, bearbeiten oder löschen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Dashboards hinzufügen
  - a. Im Fensterausschnitt **Dashboards** klicken Sie auf **Neues hinzufügen**.
  - b. Befolgen Sie die Anweisungen im Fenster, um ein Dashboard hinzuzufügen.
  - c. Klicken Sie auf **OK**.  
Der Monitor erstellt und öffnet das neue Dashboard. Der Dashboard-Name erscheint auch in der Liste **Dashboards** im linken Navigationsmenü.
3. Dashboards bearbeiten oder löschen
  - a. Öffnen Sie das Dashboard.
  - b. Klicken Sie in der oberen rechten Ecke des Dashboards auf **Anpassen** und anschließend auf eine der folgenden Optionen:
    - **Einstellungen** Bearbeitet die Dashboard-Einstellungen.
    - **Löschen** Löscht das Dashboard.

### Ergebnisse

Das Dashboard wird hinzugefügt, bearbeitet bzw. gelöscht.

#### Siehe auch

- [„Widgets“ auf Seite 1127](#)

## Dashboard-Vorlagen erstellen

Ein neu erstelltes Dashboard wird mit Standard-Widgets gefüllt. Sie können die mit einem neuen Dashboard angezeigten Standard-Widgets ändern, indem Sie den Monitor für die Verwendung von Widgets und Layout eines bestimmten Dashboards konfigurieren.

### Voraussetzungen

Sie können das Vorlagen-Dashboard nur auf der Basis Ihrer eigenen Ressourcen festlegen. Die SQL Anywhere-Monitor-Ressource kann nicht als Basis für ein Vorlagen-Dashboard verwendet werden.

### Aufgabe

1. Öffnen Sie das Dashboard, das Sie als Vorlage verwenden wollen.
2. Klicken Sie in der oberen rechten Ecke des Dashboards auf **Anpassen** und dann auf **Als Vorlage festlegen**.

### Ergebnisse

Wenn Sie ein neues Dashboard hinzufügen, enthält es dieselben Widgets und dasselbe Layout wie das Vorlagen-Dashboard.

### Siehe auch

- „Widgets“ auf Seite 1127

## Widgets

Jeder Benutzer kann die in seinen Dashboards vorhandenen Widgets hinzufügen, bearbeiten oder löschen. Ein neu erstelltes Dashboard wird mit Standard-Widgets gefüllt.

Die folgende Tabelle enthält die verschiedenen Typen der Metrik-Widgets, die Sie für Ihre Ressourcen erstellen können:

Typ der Metrik	Beschreibung
<b>Metriken</b>	Zeigt Informationen an, die für eine überwachte Ressource gesammelt wurden. Sie können wählen, Metriken entweder als Diagramm oder Tabelle anzuzeigen. Siehe „Metriken“ auf Seite 1149.
<b>Alarme</b>	Zeigt eine Liste von Alarmen für die Ressourcen an. Siehe <a href="#">Widget Alarmliste auf Seite 1125</a> .
<b>Ressourcen</b>	Zeigt eine Liste von Ressourcen an. Siehe <a href="#">Widget Ressourcenliste auf Seite 1124</a> .
<b>SQL Anywhere-Verbindungen</b>	Zeigt eine Liste von Datenbankverbindungen an. Siehe „Schließen einer Verbindung mit dem Monitor“ auf Seite 1130.

Typ der Metrik	Beschreibung
<b>SQL Anywhere-Scale-Out-Topologie</b>	Zeigt eine Topologie von Datenbankspiegelungs- und Scale-Out-Systemen an. Siehe „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129 und „Lektion 9: (Optional) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen“ auf Seite 1214.

#### Siehe auch

- „Dashboards verwalten“ auf Seite 1126
- „Dashboards“ auf Seite 1124

## Widgets hinzufügen

Sie können Widgets zu Ihrem Dashboard hinzufügen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Öffnen Sie das Dashboard.
2. Klicken Sie in der oberen rechten Ecke des Dashboards auf **Anpassen** und dann auf **Widget hinzufügen**.
3. Klicken Sie im Feld **Welchen Typ von Widget möchten Sie?** auf den gewünschten Widget-Typ und anschließend auf **Weiter**.
4. Geben Sie im Feld **Wie möchten Sie dieses Widget nennen?** einen Namen für das Widget an.
5. Geben Sie im Feld **Welche Ressource interessiert Sie?** die Ressource an.
6. Befolgen Sie die weiteren Anweisungen im Fenster **Widget hinzufügen**, um ein Widget hinzuzufügen.
7. Klicken Sie auf **Erstellen**.

### Ergebnisse

Das neue Widget wird hinzugefügt.

## Widgets verwalten

Sie können ein Widget aus dem Widget heraus bearbeiten oder löschen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Aufgabe

1. Klicken Sie rechts oben im Widget auf den Dropdown-Pfeil.
2. Klicken Sie auf eine der beiden folgenden Optionen:
  - **Einstellungen** Bearbeitet die Widget-Einstellungen.
  - **Löschen** Löscht das Widget.

## Ergebnisse

Das Widget wird bearbeitet bzw. gelöscht.

## Widget Topologie des SQL Anywhere-Scale-Out

Sie können die Topologie von Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen anzeigen, indem Sie ein Widget vom Typ **Topologie des SQL Anywhere-Scale-Out** erstellen.

### Anzeige eines Scale-Out-Systems mit Schreibschutz in einem Topologie-Widget

Das **Topologie des SQL Anywhere-Scale-Out**-Widget für ein Scale-Out-System mit Schreibschutz zeigt folgende Felder und ihre möglichen Werte an:

- **Servername** Der Name des Knotens im Scale-Out-System.
- **Typ** Der Servertyp. Der Typ ist entweder **Partner - Primärserver** oder **Kopie**, abhängig davon, wie der Server definiert wurde, als das Scale-Out-System mit Schreibschutz erstellt wurde.
- **Status** Der Verbindungsstatus des Knotens. Kann **Verbunden** oder **Getrennt** sein.
- **Verbindungen** Die aktuelle Anzahl von Verbindungen mit diesem Knoten.
- **Zuletzt aktualisiert** Der Zeitpunkt, zu dem der Server seinen Status zuletzt aktualisiert hat.

### Anzeige eines Datenbankspiegelungssystems in einem Topologie-Widget

Das **Topologie des SQL Anywhere-Scale-Out**-Widget für ein Datenbankspiegelungssystem zeigt folgende Felder und ihre möglichen Werte an:

- **Servername** Zeigt die Namen der Datenbankserver im Spiegelungssystem an.
- **Typ** Zeigt den Servertyp und einen der folgenden Werte an:
  - Partner - Primärserver** Dieser Wert kennzeichnet den Server, der derzeit als Primärserver agiert.
  - Partner - Spiegelserver** Dieser Wert kennzeichnet den Server, der derzeit als Spiegelserver agiert.
  - Arbiter** Dieser Wert kennzeichnet den Arbiterserver.
- **Status** Zeigt den Verbindungsstatus der einzelnen Server.

- **Verbindungen** Zeigt die Anzahl von aktuellen Verbindungen zum Server.
- **Zuletzt aktualisiert** Zeigt den Zeitpunkt der letzten Änderung des Serverstatus.

### Siehe auch

- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sa\_mirror\_server\_status-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankspiegelung“ auf Seite 1467
- „SQL Anywhere-Scale-Out mit Schreibschutz“ auf Seite 1536
- „SQL Anywhere-Monitor“ auf Seite 1115
- „Praktische Einführung: Überwachen von Ressourcen mit dem Monitor“ auf Seite 1200
- „Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“ auf Seite 1556
- „Praktische Einführung: Datenbankspiegelungssysteme erstellen“ auf Seite 1509

## Schließen einer Verbindung mit dem Monitor

Jeder Benutzer kann mithilfe des Monitors Verbindungen zu Datenbankressourcen anzeigen und schließen, vorausgesetzt, der Benutzer kennt für die betreffende Datenbank den Benutzernamen und das Kennwort eines Benutzers mit DROP CONNECTION-Systemprivileg.

### Voraussetzungen

Sie benötigen den Benutzernamen und das Kennwort eines Benutzers der Datenbank, der das DROP CONNECTION-Systemprivileg hat.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Öffnen Sie das Dashboard für die Datenbankressource.

Klicken Sie auf **Dashboards** » *name-of-dashboard*.

3. Wählen Sie im Widget **Verbindungen** eine Verbindung aus und klicken Sie dann auf das **x** neben dem Namen der Verbindung.
4. Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen und das Kennwort für die Datenbank ein.

Diese Anmeldeinformationen werden verwendet, um eine Verbindung mit der Datenbank herzustellen und die angegebene Verbindung zu schließen. Anschließend werden die Anmeldeinformationen aus dem Monitor entfernt.

5. Klicken Sie auf **OK**.

### Ergebnisse

Die Verbindung wird geschlossen.

## Einführung in die Zeitanzeige

Alle im Monitor angezeigten Zeitangaben basieren auf der 24-Stunden-Uhr und entsprechen der lokalen Zeit des Computers, auf dem der Monitor läuft.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Anmelden beim Monitor
2. Öffnen Sie das Dashboard für die Ressource.
3. Suchen Sie im Widget **Serverinformationen** nach der Metrik **Serverzeit-Offset**.

### Ergebnisse

Der **Serverzeit-Offset** protokolliert den Zeitunterschied zwischen der Zeit auf dem Computer, auf dem der Monitor läuft, und die Zeit auf dem Computer, auf dem Sie die Monitor-Daten anzeigen.

### Siehe auch

- [„Metriken“ auf Seite 1149](#)

## Fenster Administration für den Monitor

### Hinweis

Nur Monitor-Administratoren haben Zugriff auf das Fenster **Administration**. Weitere Hinweise zu Monitor-Administratoren finden Sie unter [„Monitor-Benutzer“ auf Seite 1175](#).

Als Monitor-Administrator können Sie die zu überwachenden Ressourcen (z.B. Datenbanken, MobiLink-Server und MobiLink-Serverfarmen oder Relay Server-Farmen) auswählen und folgende Vorgänge ausführen:

- Ressourcen hinzufügen, bearbeiten und löschen. Siehe [„Ressourcen“ auf Seite 1132](#).
- Benutzer hinzufügen und bearbeiten. Siehe [„Monitor-Benutzer“ auf Seite 1175](#).
- Den Monitor konfigurieren. Siehe [„Sichern des Monitors“ auf Seite 1191](#).
- Das Nachrichtenlog anzeigen. Siehe [„Anzeigen des Nachrichtenlogs“ auf Seite 1132](#).
- Die Ausnahmebedingungsberichte anzeigen. Siehe [„Ausnahmebedingungsberichte anzeigen“ auf Seite 1132](#).

### Siehe auch

- [„Metriken“ auf Seite 1149](#)

## Anzeigen des Nachrichtenlogs

Das **Meldungslog** enthält informative Meldungen aus dem Monitor zu dessen Betrieb. Meldungen werden in einer Tabelle angezeigt, beginnend mit der neuesten Meldung.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Nachrichtenlog**.

### Ergebnisse

Sie können das **Meldungslog** anzeigen.

## Ausnahmebedingungsberichte anzeigen

Wenn im Monitor ein schwerwiegender Fehler oder ein Absturz auftritt, wird ein Ausnahmebedingungsbericht erstellt, aus dem die Ereignisse zum Zeitpunkt des Fehlers hervorgehen.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Ausnahmebedingungsberichte**.

### Ergebnisse

Sie können den Ausnahmebedingungsbericht anzeigen.

## Ressourcen

Eine **Ressource** ist eine Datenbank (einschließlich Datenbanken in Scale-Out-Systemen mit Schreibschutz oder Spiegelungssystemen), ein MobiLink-Server, eine MobiLink-Serverfarm oder eine Relay Server-Farm. Als Monitor-Administrator fügen Sie Ressourcen zum Monitor hinzu und beginnen dann mit deren Überwachung.

## Ressource SQL Anywhere-Monitor

Die Standardressource namens **SQL Anywhere-Monitor** erstellt Berichte über den Zustand des Monitors selbst. Diese Standardressource ist nützlich für die Überwachung des Computers, auf dem der Monitor läuft, und zum Senden von Alarmen bei Problemen mit dem Monitor. Sie können diese Ressource nicht ändern und diese Überwachung nicht stoppen.

### Siehe auch

- [Widget Ressourcenliste auf Seite 1124](#)

## Datenbankressourcen hinzufügen

Fügen Sie eine Datenbank (einschließlich Datenbanken in Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen) im Monitor als Ressource hinzu.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

Wenn Sie eine Datenbank der Version 16 hinzufügen möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle hat. Wenn Sie eine Datenbank einer früheren Version hinzufügen möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die DBA-Berechtigung hat.

### Kontext und Bemerkungen

Sie können Ressourcen einzeln hinzufügen oder über eine CSV-Datei mehrere Ressourcen importieren.

Es gibt keinen Unterschied in der Ressourcenkonfiguration für einen Stammknoten in einem Scale-Out-System mit Schreibschutz und andere Datenbankserver. Beim Konfigurieren der Ressource erkennt der Monitor, dass die Ressource der Stammknoten in einem Scale-Out-System mit Schreibschutz ist.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf **Hinzufügen**.
5. Im Fenster **Ressource hinzufügen** führen Sie Folgendes durch:
  - a. Klicken Sie auf **SQL Anywhere Server**
  - b. Klicken Sie auf **Weiter**.
  - c. Geben Sie im Feld **Name** einen Namen für die Ressource ein. Dieser Name wird im Monitor angezeigt. Klicken Sie anschließend auf **Weiter**.

- d. Geben Sie im Feld **Host** den Hostnamen oder die IP-Adresse des Computers an, auf dem der Datenbankserver läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen. Dieser Wert ist erforderlich.  
Wenn Sie die Primärdatenbank in einem Spiegelungssystem überwachen möchten, geben Sie die Hostnamen und Portnummern der Computer, auf denen Primär- und Spiegelserver ausgeführt werden, in einer kommasetrennten Liste an. z.B. `my-primary-server:2638,my-mirror-server:49152`.
  - e. (Optional) Geben Sie im Feld **Port** den TCP/IP-Port an, an dem die Datenbank läuft.  
Wenn Sie die Primärdatenbank in einem Spiegelungssystem überwachen möchten, vergewissern Sie sich, dass das Feld **Port** leer ist.
  - f. (Optional) Geben Sie im Feld **Datenbanken** den Datenbanknamen an.
  - g. (Optional) Geben Sie im Feld **Server** den Servernamen an.  
Wenn Sie die Primärdatenbank in einem Spiegelungssystem überwachen möchten, geben Sie im Feld **Server** den alternativen Servernamen für den Primärserver ein, d.h., geben Sie den Namen an, den Clients für Verbindungen mit dem Datenbankserver verwenden, der im Datenbankspiegelungssystem als Primärserver fungiert.
  - h. (Optional) Geben Sie im Feld **Andere** eine durch Semikola getrennte Zeichenfolge von Verbindungsparametern an.
  - i. Klicken Sie auf **Weiter**.
  - j. Befolgen Sie die weiteren Anweisungen.
  - k. Klicken Sie auf **Erstellen**.
6. Wenn Sie dazu aufgefordert werden, geben Sie die Benutzer-ID und das Kennwort eines Benutzers ein, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle bzw. die DBA-Berechtigung hat, und klicken Sie anschließend auf **Schließen**.

Diese Anmeldeinformationen werden für Folgendes verwendet:

- Herstellen einer Verbindung mit der Datenbank.
  - Erstellen eines neuen Benutzers namens `sa_monitor_user`. Der Monitor verwendet den Benutzer "sa\_monitor\_user", um eine Verbindung mit der Datenbank herzustellen und sie zu überwachen.
  - Installieren der Datenbankobjekte, die `sa_monitor_user` für die Überwachung der Datenbank benötigt.
  - Verwerfen der Anmeldeinformationen des Benutzers aus dem Monitor. Da der Benutzer "sa\_monitor\_user" zur überwachten Datenbank hinzugefügt wird, ist es nicht notwendig, die Anmeldeinformationen außerhalb der überwachten Datenbank zu speichern.
7. Klicken Sie auf **Schließen**.
  8. Klicken Sie auf **Schließen**.

## Ergebnisse

Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch. Die Ressource erscheint im Dashboard **Übersicht** in der **Ressourcenliste**.

## Nächste Schritte

Optional können Sie ein Dashboard für die Ressource hinzufügen. Standardmäßig wird beim Hinzufügen einer Ressource kein Dashboard hinzugefügt.

Sie können ein Widget zu Ihrem Dashboard hinzufügen. Wenn Sie die Topologie von Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen anzeigen möchten, müssen Sie ein Widget vom Typ **Topologie des SQL Anywhere-Scale-Out** hinzufügen.

## Siehe auch

- „Mehrere Ressourcen mit einer CSV-Datei hinzufügen“ auf Seite 1138
- „Host-Verbindungsparameter“ auf Seite 363
- „Liste der vom Monitor installierten Datenbankobjekte“ auf Seite 1193
- „Dashboards verwalten“ auf Seite 1126
- „Widgets“ auf Seite 1127
- „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129
- „Monitor starten“ auf Seite 1120
- „MobiLink-Benutzer“ [*MobiLink - Clientadministration*]

## MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen

Fügen Sie im Monitor einen MobiLink-Server oder eine Relay Server-Farm als zu überwachende Ressource hinzu.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Kontext und Bemerkungen

Sie können Ressourcen einzeln hinzufügen oder über eine CSV-Datei mehrere Ressourcen importieren.

Wenn Sie einen MobiLink-Server vor Version 16 überwachen möchten, der ECC-Verschlüsselung verwendet, müssen Sie beim Starten des MobiLink-Servers eine zweite Gruppe von Netzwerkprotokolloptionen angeben.

Der Monitor unterstützt keine ECC-Verschlüsselung. Wenn Sie einen MobiLink-Server vor Version 16 überwachen möchten, der ECC-Verschlüsselung verwendet, müssen Sie beim Starten des MobiLink-Servers zwei Portnummern angeben. Wenn Sie im Monitor dazu aufgefordert werden, die Portnummer für die MobiLink-Serverressource anzugeben, geben Sie die Nummer an, die nicht der ECC-Verschlüsselung zugeordnet ist.

## Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf **Hinzufügen**.
5. Im Fenster **Ressource hinzufügen** führen Sie Folgendes durch:
  - a. Klicken Sie auf den Typ der Ressource, die Sie überwachen möchten.
  - b. Klicken Sie auf **Weiter**.
  - c. Geben Sie im Feld **Name** einen Namen für die Ressource ein. Dieser Name wird im Monitor angezeigt. Klicken Sie anschließend auf **Weiter**.
  - d. Geben Sie im Feld **Host** den Hostnamen oder die IP-Adresse des Computers an, auf dem der Datenbankserver, der MobiLink-Server bzw. die Relay Server-Farm ausgeführt wird. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen. Dieser Wert ist erforderlich.
  - e. Klicken Sie auf **Weiter**.
  - f. Befolgen Sie die weiteren Anweisungen.

Für MobiLink müssen Sie eine Benutzer-ID und ein Kennwort eingeben, die für die Verbindung mit dem MobiLink-Server verwendet werden. Die MobiLink-Benutzer-ID und das MobiLink-Kennwort werden im Monitor gespeichert.
  - g. Klicken Sie auf **Erstellen**.
6. Klicken Sie auf **Schließen**.
7. Klicken Sie auf **Schließen**.

## Ergebnisse

Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch. Die Ressource erscheint im Dashboard **Übersicht** in der **Ressourcenliste**.

## Nächste Schritte

Optional können Sie ein Dashboard für die Ressource hinzufügen. Standardmäßig wird beim Hinzufügen einer Ressource kein Dashboard hinzugefügt.

Sie können ein Widget zu Ihrem Dashboard hinzufügen. Wenn Sie die Topologie von Scale-Out-Systemen mit Schreibschutz und Spiegelungssystemen anzeigen möchten, müssen Sie ein Widget vom Typ **Topologie des SQL Anywhere-Scale-Out** hinzufügen.

**Siehe auch**

- „Mehrere Ressourcen mit einer CSV-Datei hinzufügen“ auf Seite 1138
- „Host-Verbindungsparameter“ auf Seite 363
- „Liste der vom Monitor installierten Datenbankobjekte“ auf Seite 1193
- „Dashboards verwalten“ auf Seite 1126
- „Widgets“ auf Seite 1127
- „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129
- „Monitor starten“ auf Seite 1120
- „MobiLink-Benutzer“ [*MobiLink - Clientadministration*]

## MobiLink-Serverfarm als Ressourcen hinzufügen

Um eine MobiLink-Serverfarm überwachen zu können, müssen Sie die Ressource zum Monitor hinzufügen.

**Voraussetzungen**

Sie müssen Monitor-Administrator sein.

Alle Server in der MobiLink-Serverfarm müssen bereits als Ressourcen zum Monitor hinzugefügt sein, bevor die MobiLink-Serverfarm hinzugefügt werden kann.

**Kontext und Bemerkungen**

Sie können Ressourcen einzeln hinzufügen oder über eine CSV-Datei mehrere Ressourcen importieren.

**Aufgabe**

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf **Hinzufügen**.
5. Befolgen Sie die Anweisungen im Fenster **Ressource hinzufügen**, um eine Ressource für die Überwachung eines MobiLink-Servers hinzuzufügen.

Der Monitor sammelt Metriken für die MobiLink-Serverfarm sowie für jeden Server, der Teil der Farm ist. Wenn Sie eine MobiLink-Serverfarm als Ressource hinzufügen, müssen Sie die Server angeben, die Teil der Farm sind.

6. Klicken Sie auf **Erstellen**.
7. Klicken Sie auf **Schließen**.
8. Klicken Sie auf **Schließen**.

### Ergebnisse

Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch. Die Ressource erscheint im Dashboard **Übersicht** in der **Ressourcenliste**.

### Nächste Schritte

Optional können Sie ein Dashboard für die Ressource hinzufügen. Standardmäßig wird beim Hinzufügen einer Ressource kein Dashboard hinzugefügt.

### Siehe auch

- „Mehrere Ressourcen mit einer CSV-Datei hinzufügen“ auf Seite 1138
- „Host-Verbindungsparameter“ auf Seite 363
- „Liste der vom Monitor installierten Datenbankobjekte“ auf Seite 1193
- „Dashboards verwalten“ auf Seite 1126
- „Widgets“ auf Seite 1127
- „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129
- „Monitor starten“ auf Seite 1120
- „MobiLink-Benutzer“ [*MobiLink - Clientadministration*]

## Mehrere Ressourcen mit einer CSV-Datei hinzufügen

Sie können mehrere Ressourcen zum Monitor hinzufügen, indem Sie eine Datei mit kommagetrennten Werten (CSV) erstellen und die Datei anschließend importieren.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Kontext und Bemerkungen

Wenn Sie eine Primärdatenbank in einem Datenbankspiegelungssystem als Ressource hinzufügen möchten, können Sie keine CSV-Datei verwenden. Verwenden Sie stattdessen das Fenster **Administration**.

### Aufgabe

1. Erstellen Sie eine CSV-Datei.

Jede Zeile in der CSV-Datei enthält Informationen über eine einzelne Ressource. Jeder kommagetrennte Begriff innerhalb einer Zeile beschreibt ein Attribut der Ressource. Die Reihenfolge der Begriffe ist wichtig.

Für optionale Begriffe müssen vorangehende Begriffe (einschließlich anderer optionaler Begriffe) angegeben werden. Wenn Sie beispielsweise den Datenbanknamen angeben möchten, müssen Sie auch den Servernamen und die Portnummer angeben. Wenn Sie den Verschlüsselungstyp angeben möchten, müssen Sie auch den Verbindungstyp angeben. Wenn Sie das Monitoring-URL-Suffix angeben möchten, müssen Sie auch die Portnummer angeben.

- **CSV-Dateiformat für Datenbankressourcen** Für optionale Begriffe müssen vorangehende Begriffe (einschließlich anderer optionaler Begriffe) angegeben werden. Wenn Sie beispielsweise den Datenbanknamen angeben möchten, müssen Sie auch den Servernamen und die Portnummer angeben.

Position in der Zeile	Begriff	Beschreibung
1	Ressourcentyp	Geben Sie <b>sa</b> ein, um anzugeben, dass die Ressource eine Datenbank ist. Dieser Begriff ist erforderlich.
2	Ressourcenname	Geben Sie den Ressourcenamen an, den die Datenbank im Monitor erhält. Dieser Begriff ist erforderlich.
3	Benutzername	Geben Sie den Benutzernamen an, der für die Verbindung mit der Datenbank verwendet wird. Wenn Sie eine Datenbank der Version 16 hinzufügen möchten, müssen Sie den Benutzernamen für einen Benutzer in der Datenbank angeben, der die SYS_SAMONITOR_ADMIN_ROLE-Rolle hat. Wenn Sie eine Datenbank einer früheren Version hinzufügen möchten, müssen Sie den Benutzernamen für einen Benutzer in der Datenbank angeben, der die DBA-Berechtigung hat.
4	Kennwort	Geben Sie das Benutzerkennwort an, das für die Verbindung mit der Datenbank verwendet wird. Dieser Begriff ist erforderlich.
5	Host	Geben Sie den Hostnamen oder die IP-Adresse des Computers an, auf dem der Datenbankserver läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen. Dieser Begriff ist erforderlich.
6	Port	Geben Sie die Portnummer des laufenden Datenbankservers an. Die Standard-Portnummer ist 2638. Dieser Begriff ist optional. Standardwert ist "0".
7	Server	Geben Sie den Namen des Datenbankservers an, mit dem die Datenbank verbunden ist. Dieser Begriff ist optional.
8	Datenbank	Geben Sie den Namen der Datenbank an. Dieser Begriff ist optional.

Position in der Zeile	Begriff	Beschreibung
9	Verbindungsparameter	Geben Sie zusätzliche Verbindungsparameter an, die für die Verbindung mit der Datenbank verwendet werden. Geben Sie die Verbindungsparameter als durch Semikola getrennte Liste von Option=Wert-Paaren an. Der Standardwert ist "". Dieser Begriff ist optional.

Im Folgenden finden Sie ein Beispiel für eine CSV-Datei, die zwei Datenbankressourcen enthält.

```
sa,demo,DBA,sql,localhost,2638,demo16
sa,demo3,DBA,sql,localhost,49152,demo16,demo
```

- **CSV-Dateiformat für MobiLink-Ressourcen** Für optionale Begriffe müssen vorangehende Begriffe (einschließlich anderer optionaler Begriffe) angegeben werden. Wenn Sie beispielsweise den Verschlüsselungstyp angeben möchten, müssen Sie auch den Verbindungstyp angeben.

Position in der Zeile	Begriff	Beschreibung
1	Ressourcentyp	Geben Sie <b>ml</b> ein, um anzugeben, dass die Ressource ein MobiLink-Server ist.  Dieser Begriff ist erforderlich.
2	Ressourcenname	Geben Sie den Ressourcenamen so ein, wie er im Monitor erscheinen wird. Dieser Begriff ist erforderlich.
3	Benutzername	Geben Sie den Benutzernamen an, der für die Verbindung mit der Datenbank verwendet wird. Dieser Begriff ist erforderlich.
4	Kennwort	Geben Sie das Kennwort an, das für die Verbindung mit der Datenbank verwendet wird. Dieser Begriff ist erforderlich.
5	Host (MobiLink-Server)	Geben Sie den Hostnamen oder die IP-Adresse des Computers an, auf dem der Server läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen. Dieser Begriff ist erforderlich.

Position in der Zeile	Begriff	Beschreibung
6	Port (MobiLink-Server)	Geben Sie die Portnummer des laufenden MobiLink-Servers an. Die Standard-Portnummer für MobiLink ist 2439. Dieser Begriff ist optional. Standardwert ist "0".
7	Verbindungstyp (MobiLink-Server)	Geben Sie die Methode an, nach der die Verbindung mit der Ressource hergestellt werden soll. Verwenden Sie eine der folgenden Optionen: <ul style="list-style-type: none"> <li>○ <b>tcpip</b> Dies ist die Standardeinstellung.</li> <li>○ <b>http</b></li> <li>○ <b>https</b></li> <li>○ <b>tls</b></li> </ul> Dieser Begriff ist optional.
8	Verschlüsselungstyp (MobiLink-Server)	Geben Sie die Methode an, mit der die Verbindung verschlüsselt wird. Geben Sie eine der folgenden Optionen ein: <ul style="list-style-type: none"> <li>○ <b>N</b> Keine Verschlüsselung. Dies ist die Standardeinstellung.</li> <li>○ <b>R</b> RSA-Verschlüsselung.</li> <li>○ <b>F</b> FIPS-zertifizierte RSA-Verschlüsselung.</li> </ul> Dieser Begriff ist optional.
9	Verbindungsparameter (MobiLink-Server)	Geben Sie zusätzliche Verbindungsparameter an, die für die Verbindung mit der Datenbank verwendet werden. Geben Sie die Verbindungsparameter als durch Semikola getrennte Liste von Option=Wert-Paaren an. Dieser Begriff ist optional.

Im Folgenden finden Sie ein Beispiel für eine Importdatei, die zwei MobiLink-Serverressourcen enthält.

```
ml,demo2,DBA,sql,localhost
ml,demo4,DBA,sql,localhost,0,tcpip,N
```

• **CSV-Dateiformat für MobiLink-Serverfarm-Ressourcen**

Position in der Zeile	Begriff	Beschreibung
1	Ressourcentyp	Geben Sie <b>mf</b> ein, um anzugeben, dass die Ressource eine MobiLink-Serverfarm ist.  Dieser Begriff ist erforderlich.
2	Ressourcenname	Geben Sie den Ressourcenamen so ein, wie er im Monitor erscheinen wird. Dieser Begriff ist erforderlich.
3	MobiLink-Servername	Geben Sie die MobiLink-Serverressourcen an, die in die MobiLink-Serverfarm einbezogen werden sollen. Verwenden Sie dazu eine kommagetrennte Liste. Dieser Begriff ist erforderlich.

Im Folgenden finden Sie ein Beispiel für eine Importdatei, die zwei MobiLink-Serverressourcen und eine MobiLink-Serverfarm-Ressource enthält.

```
ml,demo2,DBA,sql,localhost
ml,demo4,DBA,sql,localhost,0,tcpip,N
mf,collection_demo,demo2,demo4
```

- **CSV-Dateiformat für Relay Server-Farm-Ressourcen** Für optionale Begriffe müssen vorangehende Begriffe (einschließlich anderer optionaler Begriffe) angegeben werden. Wenn Sie beispielsweise das Monitoring-URL-Suffix angeben möchten, müssen Sie auch die Portnummer angeben.

Position in der Zeile	Begriff	Beschreibung
1	Ressourcentyp	Geben Sie <b>rf</b> ein, um anzugeben, dass die Ressource eine Relay Server-Farm ist.  Dieser Begriff ist erforderlich.
2	Ressourcenname	Geben Sie den Ressourcenamen so ein, wie er im Monitor erscheinen wird. Dieser Begriff ist erforderlich.

Position in der Zeile	Begriff	Beschreibung
3	Host (Relay Server-Farm)	Geben Sie den Hostnamen oder die IP-Adresse des Computers an, auf dem der Server läuft. Sie können den Namen "localhost" verwenden, um das aktuelle System zu bezeichnen. Dieser Begriff ist erforderlich.
4	Port (Relay Server-Farm)	Geben Sie die Portnummer der laufenden Relay Server-Farm an. Dieser Begriff ist optional. Standardwert ist "0".
5	URL-Suffix überwachen	Geben Sie das URL-Suffix für die Suche nach dem Überwachungsprogramm auf der Relay Server-Farm an. Dieser Begriff ist optional.
6	Ist HTTPS?	Geben Sie <b>True</b> an, wenn der Monitor für die Verbindung mit der Relay Server-Farm HTTPS verwenden soll. Dieser Begriff ist optional.  Der Standardwert ist <b>False</b> . Dieser Begriff ist optional.
7	Benutzername für HTTP-Authentifizierung	Falls erforderlich, geben Sie den Benutzernamen für die HTTPS-Authentifizierung an. Dieser Begriff ist optional.
8	Kennwort für HTTP-Authentifizierung	Falls erforderlich, geben Sie das Kennwort für die HTTPS-Authentifizierung an. Dieser Begriff ist optional.

Im Folgenden finden Sie ein Beispiel für eine Importdatei, die zwei MobiLink-Serverressourcen, eine MobiLink-Serverfarm-Ressource und eine Relay Server-Farm-Ressource enthält.

```
rf,rf_demo,rstest02.website.com
```

2. Melden Sie sich beim Monitor an.
3. Klicken Sie auf **Administration**.
4. Klicken Sie auf **Ressourcen**.

5. Klicken Sie auf **Importieren**.
6. Navigieren Sie zur CSV-Datei und klicken Sie auf **Öffnen**.

Die Ressourcen aus der CSV-Datei werden dem Monitor hinzugefügt und die Überwachung beginnt.

7. Klicken Sie auf **Schließen**.
8. Klicken Sie auf **Schließen**.

### Ergebnisse

Die importierte Ressource wird der **Ressourcenliste** im Dashboard **Übersicht** hinzugefügt.

### Siehe auch

- [„Datenbankressourcen hinzufügen“ auf Seite 1133](#)
- [„MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135](#)

## Ressourcenüberwachung starten

Die Überwachung einer Ressource startet auf folgende Arten:

- Automatisch beim Start des Monitors. Wenn Sie den Monitor starten, verbindet er sich standardmäßig mit den Ressourcen und sammelt Metriken für *alle* Ressourcen im Monitor.
- Automatisch, wenn ein Monitor-Administrator eine Ressource hinzufügt. Nachdem eine Ressource hinzugefügt wurde, versucht der Monitor, sich mit der Ressource zu verbinden, und startet die Überwachung.
- Automatisch am Ende einer Blackoutperiode. Der Monitor versucht automatisch, sich mit der Ressource zu verbinden und die Überwachung wieder aufzunehmen.
- Wenn ein Monitor-Administrator das Fenster **Administration** öffnet, auf **Ressourcen** klickt, in der Liste eine Ressource auswählt und auf **Start** klickt.

### Siehe auch

- [„Datenbankressourcen hinzufügen“ auf Seite 1133](#)
- [„MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135](#)

## Überwachung der Ressourcen stoppen

Stoppen Sie die Überwachung von Ressourcen, wenn der Monitor keine Metriken sammeln soll. Sie stoppen die Überwachung beispielsweise, wenn Sie wissen, dass die Ressource nicht verfügbar sein wird, da Sie sonst fortlaufend Alarme erhalten, bis die Ressource wieder verfügbar ist. Mit Ausnahme der Standard-Monitor-Ressource können Sie die Überwachung einer Ressource jederzeit stoppen.

Wenn Sie die Überwachung einer Ressource stoppen, veranlassen Sie beim Monitor folgende Maßnahmen:

- Er stoppt die Sammlung von Metriken für die Ressource.
- Er stoppt die Meldung von Alarmen für die Ressource.

Es gibt zwei Methoden, die Überwachung einer Ressource zu stoppen:

- **Planung einer regelmäßigen, wiederholten Blackoutperiode** Diese Methode ist sinnvoll, wenn folgende Bedingungen gegeben sind:
  - Sie müssen die Überwachung der Ressource wiederholt stoppen. Ein Beispiel dafür wäre, wenn Sie regelmäßige Wartungsarbeiten am Monatsende durchführen.
  - Sie wissen vorher, wie lange die Ressource nicht verfügbar sein wird. Ein Beispiel dafür wäre, wenn Sie wissen, dass die reguläre Wartung vier Stunden in Anspruch nimmt.
  - Sie wollen, dass die Überwachung automatisch neu startet. Wenn eine Blackoutperiode abläuft, versucht der Monitor, sich wieder mit der Ressource zu verbinden und die Sammlung der Metriken fortzusetzen.

Um diese Methode zu verwenden, konfigurieren Sie Blackouts, damit der Monitor die Überwachung zu festgelegten Zeiten automatisch stoppt.

- **Überwachung manuell stoppen** Diese Methode ist sinnvoll, wenn folgende Bedingungen gegeben sind:
  - Sie müssen die Überwachung zur Durchführung seltener oder einmaliger Aufgaben stoppen. Ein Beispiel dafür wäre, wenn Sie die Überwachung stoppen müssen, weil der Computer, auf dem die Ressource läuft, für eine außergewöhnliche Wartung vom Netz genommen werden muss.
  - Sie sind bereit, die Überwachung danach wieder zu starten. Wenn eine Ressource manuell gestoppt wurde, wartet der Monitor darauf, dass Sie die Überwachung wieder starten.

Wenn Sie die Überwachung einer Ressource dauerhaft stoppen möchten, können Sie sie aus dem Monitor entfernen.

#### Siehe auch

- [„Konfigurieren von Blackouts“ auf Seite 1145](#)
- [„Überwachung von Ressourcen stoppen“ auf Seite 1146](#)
- [„Ressourcen entfernen“ auf Seite 1148](#)

## Konfigurieren von Blackouts

Blackouts sind Perioden, in denen der Monitor keine Metriken sammeln soll. Nach Abschluss eines Blackouts verbindet sich der Monitor wieder mit den betreffenden Ressourcen und fährt mit dem Sammeln der Metriken fort.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

## Kontext und Bemerkungen

Blackouts richten sich nach der Ortszeit der Ressource.

## Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf die Ressource und anschließend auf **Konfigurieren**.
5. Klicken Sie auf **Blackouts**.
6. Klicken Sie auf **Neu**.
7. Im Fenster **Neue Blackoutperiode** geben Sie das Datum und die Zeit (24-Stunden-Uhr) für das Blackout ein.

Als Zeit wird die Ortszeit des Computers verwendet, auf dem die Datenbank, der MobiLink-Server bzw. die Relay Server-Farm läuft.

8. Klicken Sie auf **Speichern**.
9. Klicken Sie auf **Speichern**.
10. Klicken Sie auf **Schließen**.
11. Klicken Sie auf **Schließen**.

## Ergebnisse

Das Blackout wird konfiguriert.

## Siehe auch

- „Einführung in die Zeitanzeige“ auf Seite 1131
- „Datenbankressourcen hinzufügen“ auf Seite 1133
- „MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135
- „Überwachung von Ressourcen stoppen“ auf Seite 1146
- „Überwachung der Ressourcen stoppen“ auf Seite 1144

## Überwachung von Ressourcen stoppen

Sie können die Überwachung von Ressourcen stoppen.

## Voraussetzungen

Sie müssen Monitor-Administrator sein.

**Aufgabe**

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf die Ressource und anschließend auf **Stopp**.

**Hinweis**

Wenn Sie die Überwachung einer MobiLink-Serverfarm stoppen, wird die Überwachung für jeden einzelnen MobiLink-Server gestoppt, der Teil der Farm ist.

5. Klicken Sie auf **Schließen**.

**Ergebnisse**

Die Überwachung der angegebenen Ressource wird gestoppt.

**Siehe auch**

- [„Datenbankressourcen hinzufügen“ auf Seite 1133](#)
- [„MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135](#)
- [„Konfigurieren von Blackouts“ auf Seite 1145](#)
- [„Überwachung der Ressourcen stoppen“ auf Seite 1144](#)

**Fehler in Datenbankressourcen beheben**

Bei der Reparatur einer Ressource werden die Datenbankobjekte neu installiert, die Sie für die Überwachung der Ressource benötigen. Die Überwachungsoptionen bleiben unverändert.

**Voraussetzungen**

Sie müssen Monitor-Administrator sein.

**Kontext und Bemerkungen**

Sie können nur Fehler in Datenbankressourcen beheben. In der Standardressource für den Monitor (**SQL Anywhere-Monitor**) können Sie keine Fehler beheben. Bei jeder Fehlerbehebung in einer Datenbank der Version 16 müssen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank angeben, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle hat. Bei jeder Fehlerbehebung in einer Datenbank einer früheren Version müssen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank angeben, der die DBA-Berechtigung hat.

**Aufgabe**

1. Melden Sie sich beim Monitor an.

2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf die Datenbankressource, die Sie reparieren möchten.
5. Wenn die Ressource gerade überwacht wird, klicken Sie auf **Stopp**.
6. Klicken Sie auf **Reparieren**.
7. Wenn Sie dazu aufgefordert werden, geben Sie die Benutzer-ID und das Kennwort für die Datenbank ein. Die Anmeldeinformationen werden für die Verbindung mit der Datenbank verwendet und anschließend aus dem Monitor entfernt.
8. Klicken Sie auf **Reparieren**.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf **Start**, um die Überwachung der Ressource neu zu starten.
11. Klicken Sie auf **Schließen**.

### Ergebnisse

Die Fehler in der Ressource werden behoben.

### Siehe auch

- [„Liste der vom Monitor installierten Datenbankobjekte“ auf Seite 1193](#)
- [„Ressourcen“ auf Seite 1132](#)

## Ressourcen entfernen

Wenn eine Ressource entfernt wird, stoppt der Monitor dauerhaft die Überwachung der Ressource und verwirft die Metriken, die für die Ressource gesammelt wurden. Sie sollten Ressourcen nur entfernen, wenn Sie sicher sind, dass Sie sie nicht überwachen müssen, z.B. weil eine Ressource nicht mehr verwendet wird.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Kontext und Bemerkungen

Sie können die Ressource **SQL Anywhere-Monitor** nicht löschen.

Wenn Sie eine Datenbankressource entfernen, löscht der Monitor nicht die in der Datenbank installierten Überwachungsobjekte.

## Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf die Ressource.
5. Klicken Sie auf **Löschen**.
6. Klicken Sie auf **Ja**.

### Hinweis

Wenn Sie eine MobiLink-Serverfarm entfernen, fordert der Monitor Sie auf, die MobiLink-Server zu entfernen, die Teil der Farm sind. Klicken Sie auf **Ja**, um die angegebenen MobiLink-Server zu entfernen, oder klicken Sie auf **Nein**, um nur die MobiLink-Serverfarm und nicht die angegebenen MobiLink-Server zu entfernen.

7. Klicken Sie auf **Schließen**.

## Ergebnisse

Die Ressource wird entfernt.

## Siehe auch

- [Monitor-Objekte löschen auf Seite 1194](#)
- [„Überwachung der Ressourcen stoppen“ auf Seite 1144](#)

## Metriken

Der Monitor sammelt und speichert Metriken von Datenbanken, MobiLink-Servern und MobiLink-Serverfarmen sowie Relay Server-Farmen, um unter anderem Folgendes zu ermitteln:

- Ob die Ressource läuft.
- Ob der Computer, auf dem die Ressource läuft, störungsfrei arbeitet und mit dem Netzwerk verbunden ist.
- Ob die Ressource Anforderungen empfängt und verarbeitet.
- Ob offensichtliche Probleme wie zu lang laufende Abfragen oder blockierte Benutzer vorliegen.
- Die Anzahl von Synchronisationen, die der MobiLink-Server über eine bestimmte Dauer durchführt.
- Die durchschnittliche Zeit, die der Backend-Server für die Verarbeitung einer HTTP-Anforderung benötigt.

## Liste von Metriken für Datenbankressourcen

Metrik	Beschreibung
<b>Aktive HTTP-Anforderungen</b>	Gibt die Anzahl der HTTP-Verbindungen zurück, die aktiv eine HTTP-Anforderung abarbeiten. HTTP-Verbindungen, die ihre Antwort gesendet haben, sind nicht enthalten. Siehe <a href="#">HttpNumActiveReq-Servereigenschaft auf Seite 750</a> .
<b>Aktive HTTPS-Anforderungen</b>	Gibt die Anzahl der HTTPS-Verbindungen zurück, die aktiv eine HTTPS-Anforderung abarbeiten. HTTPS-Verbindungen, die ihre Antwort gesendet haben, sind nicht enthalten. Siehe <a href="#">HttpsNumActiveReq-Servereigenschaft auf Seite 751</a> .
<b>Arbiter-Status</b>	Gibt einen der folgenden Werte zurück: <ul style="list-style-type: none"> <li>• <b>Verbunden</b> Der Arbiterserver ist mit dem Primärserver verbunden.</li> <li>• <b>Getrennt</b> Der Arbiterserver ist nicht mit dem Primärserver verbunden.</li> <li>• <b>0</b> Es gibt keinen Arbiterserver in dieser Konfiguration.</li> </ul>
<b>Veränderte Daten im Cache</b>	Gibt die Anzahl der Cacheseiten zurück, die verändert wurden (und ausgeschrieben werden müssten). Siehe <a href="#">CacheFileDirty-Servereigenschaft auf Seite 746</a> .
<b>Vorgemerkte Cacheseiten</b>	Gibt die Anzahl der vorgemerkten Cacheseiten zurück. Siehe <a href="#">CachePinned-Servereigenschaft auf Seite 746</a> .
<b>Cacheersetzungen</b>	Gibt die Anzahl von Seiten im Cache zurück, die ersetzt wurden. Siehe <a href="#">CacheReplacements-Servereigenschaft auf Seite 746</a> .
<b>Cachegröße</b>	Gibt die aktuelle Cachegröße in kB zurück. Siehe <a href="#">CurrentCacheSize-Servereigenschaft auf Seite 748</a> .
<b>Verbindungsanzahl</b>	Gibt die aktuelle Anzahl der Verbindungen zur Datenbank zurück. Siehe „sa_conn_info-Systemprozedur“ [ <i>SQL Anywhere Server - SQL-Referenzhandbuch</i> ].
<b>CPU-Nutzung</b>	Gibt den Prozentsatz der CPU-Zeit zurück, die vom Datenbankserver belegt wird.
<b>Datenbankname</b>	Gibt den Namen der Datenbank zurück. Siehe <a href="#">Name-Datenbankeigenschaft auf Seite 780</a> .
<b>Festplatten-Lesevorgänge</b>	Gibt die Rate zurück, mit der Daten von der Festplatte gelesen werden (in kB pro Sekunde). Dieser Wert wird basierend auf der Eigenschaft DiskRead berechnet. Siehe <a href="#">DiskRead-Datenbankeigenschaft auf Seite 772</a> .
<b>Festplatten-Schreibvorgänge</b>	Gibt die Rate zurück, mit der Daten auf die Festplatte geschrieben werden (in kB pro Sekunde). Dieser Wert wird basierend auf der Eigenschaft DiskWrite berechnet. Siehe <a href="#">DiskWrite-Datenbankeigenschaft auf Seite 773</a> .

Metrik	Beschreibung
<b>Dateigröße</b>	Gibt die Größe der Hauptdatenbankdatei zurück. Siehe <a href="#">„Vordefinierte DBSpaces“ auf Seite 127</a> .
<b>Freier Speicherplatz</b>	Gibt die Menge des freien Speicherplatzes auf Ihrer Festplatte zurück. Siehe <a href="#">„sa_disk_free_space-Systemprozedur“ [SQL Anywhere Server - SQL-Referenz-handbuch]</a> .
<b>Host</b>	Gibt den Namen des Computers zurück, auf dem der Datenbankserver läuft. Das ist üblicherweise der Hostname des Computers. Siehe <a href="#">MachineName-Servereigenschaft auf Seite 753</a> .
<b>HTTP-Verbindungen</b>	Gibt die Anzahl der HTTP-Verbindungen zurück, die derzeit im Datenbankserver geöffnet sind. Diese können eine Anforderung aktiv abarbeiten oder in der Warteschlange von langlebigen (keep-alive) Verbindungen warten. Siehe <a href="#">HttpNumConnections-Servereigenschaft auf Seite 751</a> .
<b>HTTP-Sitzungen</b>	Gibt die Anzahl von aktiven und nicht-aktiven HTTP-Sitzungen im Datenbankserver zurück. Siehe <a href="#">HttpNumSessions-Servereigenschaft auf Seite 751</a> .
<b>HTTPS-Verbindungen</b>	Gibt die Anzahl der HTTPS-Verbindungen zurück, die derzeit im Datenbankserver geöffnet sind. Diese können eine Anforderung aktiv abarbeiten oder in der Warteschlange von langlebigen (keep-alive) Verbindungen warten. Siehe <a href="#">HttpsNumConnections-Servereigenschaft auf Seite 751</a> .
<b>Uhrzeit der letzten Prüfung</b>	Gibt den Zeitpunkt zurück, zu dem der Monitor die letzten Daten für die Ressource abgerufen hat.
<b>Lizenztyp</b>	Gibt den Lizenztyp zurück. Kann Networked Seat (pro Arbeitsplatz) oder CPU-basiert sein. Siehe <a href="#">LicenseType-Servereigenschaft auf Seite 753</a> .
<b>Lizenziertes Unternehmen</b>	Gibt den Namen des lizenzierten Unternehmens zurück. Siehe <a href="#">CompanyName-Servereigenschaft auf Seite 747</a> .
<b>Lizenzierte Arbeitsplätze</b>	Gibt die Anzahl der lizenzierten Arbeitsplätze oder Prozessoren zurück. Siehe <a href="#">LicenseCount-Servereigenschaft auf Seite 752</a> .
<b>Lizenzierter Benutzer</b>	Gibt den Namen des lizenzierten Benutzers zurück. Siehe <a href="#">LicensedUser-Servereigenschaft auf Seite 752</a> .
<b>Zu lang laufende Abfragen</b>	Gibt Abfragen zurück, die den Schwellenwert für lang laufende Abfragen überschreiten.
<b>Haupt-Heap-Seiten</b>	Gibt die Anzahl der Seiten zurück, die für globale Server-Datenstrukturen verwendet werden. Siehe <a href="#">MainHeapPages-Servereigenschaft auf Seite 753</a> .

Metrik	Beschreibung
<b>Max. Cachegröße</b>	Gibt die maximale zulässige Cachegröße in KB zurück. Siehe <a href="#">MaxCacheSize-Serveigenschaft auf Seite 753</a> .
<b>Spiegelmodus</b>	Gibt <b>Spiegelung ist für diese Datenbank nicht aktiviert</b> zurück, wenn die Datenbankspiegelung nicht verwendet wird. Bei aktivierter Datenbankspiegelung lautet die Anzeige <b>Synchron</b> , wenn der Synchronisationsmodus gemäß SET MIRROR OPTION als synchron festgelegt wurde, ansonsten <b>Asynchron</b> .
<b>Spiegelstatus</b>	Gibt einen der folgenden Werte zurück: <ul style="list-style-type: none"> <li>• <b>Synchronisation läuft</b> Der Spiegelserver ist nicht verbunden oder hat noch nicht alle Logseiten des Primärservers gelesen. Dieser Wert wird auch zurückgegeben, wenn der Synchronisationsmodus asynchron ist.</li> <li>• <b>Synchronisiert</b> Der Spiegelserver ist verbunden und hat alle Änderungen übernommen, die auf dem Primärserver festgeschrieben wurden.</li> </ul>
<b>Betriebssystem</b>	Gibt das Betriebssystem zurück, auf dem die Software läuft. Siehe <a href="#">Platform-Serveigenschaft auf Seite 757</a> .
<b>Betriebssystem-version</b>	Gibt das Betriebssystem zurück, auf dem die Software läuft, einschließlich Build-Nummern und Service-Packs. Siehe <a href="#">PlatformVer-Serveigenschaft auf Seite 757</a> .
<b>Partnerstatus</b>	Gibt einen der folgenden Werte zurück: <ul style="list-style-type: none"> <li>• <b>Verbunden</b> Der Spiegelserver ist mit dem Primärserver verbunden.</li> <li>• <b>Getrennt</b> Der Spiegelserver ist nicht mit dem Primärserver verbunden.</li> </ul>
<b>Spitzen-Cachegröße</b>	Gibt den höchsten Wert zurück, den der Cache in der aktuellen Sitzung erreicht hat, in kB. Siehe <a href="#">PeakCacheSize-Serveigenschaft auf Seite 757</a> .
<b>Prozessorarchitektur</b>	Gibt eine Zeichenfolge zurück, die den Prozessortyp identifiziert. Siehe <a href="#">ProcessorArchitecture-Serveigenschaft auf Seite 758</a> .
<b>Verarbeitete Abfragen</b>	Gibt die Rate (Abfragen/Sekunde) zurück, mit der Abfragen verarbeitet werden. Siehe <a href="#">QueryOptimized-Datenbankeigenschaft auf Seite 783</a> , <a href="#">QueryReused-Datenbankeigenschaft auf Seite 783</a> und <a href="#">QueryBypassed-Datenbankeigenschaft auf Seite 782</a> .
<b>Anzahl der Arbeitsplätze</b>	Gibt die Anzahl der mit einem Netzwerk-Datenbankserver verbundenen eindeutigen Client-Netzwerkadressen zurück. Siehe <a href="#">UniqueClientAddresses-Serveigenschaft auf Seite 763</a> .
<b>Serversprache</b>	Gibt die Sprachumgebung zurück, also die Sprache, die von Benutzern des Datenbankservers wahrscheinlich verwendet wird. Siehe „ <a href="#">Sprache der Sprachumgebung</a> “ auf Seite 510.

Metrik	Beschreibung
<b>Servername</b>	Gibt den Namen des Datenbankservers für die aktuelle Verbindung zurück. Siehe <a href="#">„Verbindungsparameter ServerName (Server)“</a> auf Seite 383.
<b>Serverzeit-Offset</b>	Gibt den Zeitunterschied zwischen der Zeit auf dem Computer, auf dem der Monitor läuft, und die Zeit auf dem Computer, auf dem Sie die Monitor-Daten anzeigen, zurück. Siehe <a href="#">„Einführung in die Zeitanzeige“</a> auf Seite 1131.
<b>Servertyp</b>	Gibt den Typ (Personal oder Netzwerk) des überwachten Datenbankservers zurück.
<b>Serverversion</b>	Gibt die Version der ausgeführten Software zurück. Siehe <a href="#">ProductVersion-Servereigenschaft</a> auf Seite 758.
<b>Startzeit</b>	Gibt die Zeit zurück, zu der die Datenbank gestartet wurde.
<b>Gesamter Speicherplatz</b>	Gibt die Größe der Festplatte zurück.
<b>Nicht verfügbar seit</b>	Gibt die Zeit zurück, seit der die Ressource nicht mehr zur Verfügung steht.
<b>Nicht geplante Anforderungen</b>	Gibt die Anzahl der nicht geplanten Anforderungen zurück. Siehe <a href="#">UnschReq-Servereigenschaft</a> auf Seite 763.
<b>Nicht gesendete Fehlerberichte</b>	Gibt die Anzahl von nicht gesendeten Fehlerberichten für die Datenbank zurück. Ein Fehlerbericht wird eingeschendet, wenn die Software abstürzt. Siehe <a href="#">„Unterdrücken von Alarmen für nicht gesendete Fehlerberichte aus Ressourcen“</a> auf Seite 1185.

#### Liste von Metriken für MobiLink-Serverressourcen

Metrik	Beschreibung
<b>Synchronisationen werden authentifiziert</b>	Zeigt die Anzahl der Anforderungen im Server, die sich derzeit in der Phase der Benutzerauthentifizierung befinden. Hinweise zu den Synchronisationsphasen finden Sie unter „mlsrv16-Option -v“ [ <a href="#">MobiLink - Serveradministration</a> ].
<b>Zwischengespeicherte entfernte Aufgabenanforderungen</b>	Zeigt die Anzahl der im Cache gespeicherten entfernten Aufgabenanforderungen. Siehe „SIRT_NUM_REQUESTS“ [ <a href="#">MobiLink - Serveradministration</a> ].
<b>Länge der Befehlsprozessor-Phase</b>	Zeigt die Länge der Warteschlange für Synchronisationsaufgaben. Siehe „CMD_PROCESSOR_STAGE_LEN“ [ <a href="#">MobiLink - Serveradministration</a> ].
<b>Festschreiberate</b>	Zeigt die Rate, mit der Festschreibungen durchgeführt werden.

Metrik	Beschreibung
<b>Festschreibungen</b>	Zeigt die Gesamtzahl der Festschreibungen. Siehe <a href="#">“NUM_COMMITS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anteil von abgeschlossenen Synchronisationen</b>	Zeigt die Rate der erfolgreich abgeschlossenen Synchronisationen für den Server an.
<b>Verbundene Clients</b>	Zeigt die Anzahl von verbundenen Synchronisationsclients. Siehe <a href="#">“ML_NUM_CONNECTED_CLIENTS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate geschlossener Verbindungen</b>	Zeigt die Rate, mit der TCP-Verbindungen geschlossen werden.
<b>Rate geöffneter Verbindungen</b>	Zeigt die Rate, mit der TCP-Verbindungen geöffnet werden.
<b>Rate abgelehnter Verbindungen</b>	Zeigt die Rate, mit der TCP-Verbindungen vom Server abgelehnt werden.
<b>Typ der konsolidierten Datenbank</b>	Zeigt den Typ der konsolidierten Datenbank an, z. B. <b>SQL Anywhere</b> .
<b>Version der konsolidierten Datenbank</b>	Zeigt die Version der konsolidierten Datenbank an.
<b>CPU-Gesamtzeit</b>	Zeigt den Umfang der vom MobiLink-Server verwendeten CPU-Zeit in Mikrosekunden. Siehe <a href="#">“CPU_USAGE”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>CPU-Nutzung</b>	Zeigt den Prozentsatz der CPU-Zeit, der vom MobiLink-Server belegt wird.
<b>CPUs</b>	Zeigt die Anzahl der verwendeten CPUs.
<b>Aktuelle TCP-Verbindungen</b>	Zeigt die Anzahl der TCP-Verbindungen, die derzeit von diesem MobiLink-Server benutzt werden.
<b>Verwendete Datenbankverbindungen</b>	Zeigt die Anzahl der derzeit verwendeten Datenbankverbindungen. Siehe <a href="#">“DB_CONNECTIONS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Zähler Datenbank-Worker-Threads</b>	Zeigt die Anzahl von Datenbank-Worker-Threads. Siehe <a href="#">„mlsrv16-Option -w“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Download der Synchronisationen</b>	Zeigt die aktuelle Anzahl der Synchronisationen an, die in den Phasen "Download vorbereiten", "Download abrufen", "Auf Download-Quittierung warten" oder "Synch_Ende" sind. Hinweise zu den Synchronisationsphasen finden Sie unter <a href="#">„mlsrv16-Option -v“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Treibername</b>	Zeigt den Namen des Treibers für die konsolidierte Datenbank.

Metrik	Beschreibung
<b>Treiberversion</b>	Zeigt die Version des Treibers für die konsolidierte Datenbank.
<b>Fehler</b>	Zeigt die Gesamtzahl der Fehler. Siehe <a href="#">“NUM_ERRORS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anteil von fehlgeschlagenen Synchronisationen</b>	Zeigt die Rate der fehlgeschlagenen Synchronisationen des Servers in Synchronisationen pro Sekunde.
<b>Fehlgeschlagene Synchronisationen</b>	Zeigt die Gesamtzahl der fehlgeschlagenen Synchronisationen. Siehe <a href="#">“NUM_FAILED_SYNCS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Dateiübertragungen</b>	Zeigt die Anzahl der derzeitigen MobiLink-Dateiübertragungen. Siehe <a href="#">“NUM_CONNECTED_FILE_XFERS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Abgeschlossener Synchronisationsanteil</b>	Zeigt die Rate, mit der Synchronisationen abgeschlossen werden.
<b>Freier Festplattenspeicher für MobiLink-Cache</b>	Zeigt den verfügbaren Festplattenspeicher auf der temporären Festplatte für den MobiLink-Cache in Byte. Siehe <a href="#">“FREE_DISK_SPACE”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Heartbeat-Phase</b>	Zeigt die Länge der Warteschlange für periodische Aufgaben, die nicht im Rahmen der Synchronisation ausgeführt werden. Siehe <a href="#">“HEARTBEAT_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Host</b>	Zeigt den Namen des Computers, auf dem der MobiLink-Server läuft. Das ist üblicherweise der Hostname des Computers.
<b>Ist der konsolidierte Typ verfügbar?</b>	Zeigt <b>True</b> , wenn der MobiLink-Server eine Verbindung zur konsolidierten Datenbank herstellen kann.
<b>Ist die konsolidierte Datenbank eine Clustered-Version?</b>	Zeigt <b>True</b> , wenn der MobiLink-Server eine Clustered-Version der konsolidierten Datenbank verwendet.
<b>Ist der Primärserver bekannt?</b>	Zeigt <b>Ja</b> , wenn der Primärserver dem Server bekannt ist. Zeigt <b>Nein</b> , wenn der Primärserver unbekannt ist oder wenn der Server nicht wissen muss, um welchen Primärserver es sich handelt. Siehe <a href="#">“PRIMARY_IS_KNOWN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Primärserver?</b>	Zeigt <b>Ja</b> , wenn der Server der Primärserver ist. Siehe <a href="#">“SERVER_IS_PRIMARY”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Uhrzeit der letzten Prüfung</b>	Zeigt den Zeitpunkt, zu dem der Monitor die letzten Daten für die Ressource abgerufen hat.

Metrik	Beschreibung
<b>Lizenziertes Unternehmen</b>	Zeigt den Namen des lizenzierten Unternehmens.
<b>Lizenzierter Benutzer</b>	Zeigt den Namen des lizenzierten Benutzers.
<b>Listener</b>	Zeigt die Anzahl der derzeit verbundenen Listener. Siehe <a href="#">“NUM_CONNECTED_LISTENERS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Cachegröße</b>	Zeigt die maximale vom MobiLink-Server verwendete Cachegröße.
<b>Max. Clients</b>	Zeigt die maximale Anzahl von Clients. Siehe <a href="#">„mlsrv16-Option -sm“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Datenbankverbindungen</b>	Zeigt die maximale Anzahl von Datenbankverbindungen gemäß der Einstellung in der Option -cn oder -w für mlsrv16. Siehe <a href="#">„mlsrv16-Option -cn“</a> [ <i>MobiLink - Serveradministration</i> ] und <a href="#">„mlsrv16-Option -w“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Synchronisationszeit</b>	Zeigt die maximale Zeit an, die eine Synchronisation gedauert hat. Das Alter der ältesten Synchronisation in Mikrosekunden. Siehe <a href="#">“LONGEST_SYNC”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. TCP-Verbindungen</b>	Zeigt die maximale Anzahl von TCP-Verbindungen gemäß der Option -nc für mlsrv16. Siehe <a href="#">„mlsrv16-Option -nc“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. zulässige Uploads</b>	Zeigt die maximale Anzahl gleichzeitiger Uploads in die Datenbank. Siehe <a href="#">„mlsrv16-Option -wu“</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Wartezeit für Verbindung</b>	Zeigt den längsten Zeitraum, den eine aktive Synchronisation auf die Datenbank warten musste. Siehe <a href="#">“LONGEST_DB_WAIT”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Verwendeter Speicher</b>	Zeigt die Anzahl der vom RAM-Speicher verwendeten Byte. Zeigt die protokollierte Speichernutzung, wenn der Server auf einer anderen Plattform als Windows läuft. Siehe <a href="#">“MEMORY_USED”</a> [ <i>MobiLink - Serveradministration</i> ] und <a href="#">“TRACKED_MEMORY”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Monitore</b>	Zeigt die Anzahl der derzeit verbundenen Monitore und MobiLink-Profiler. Siehe <a href="#">“NUM_CONNECTED_MONITORS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Notifier-Phase</b>	Zeigt die Länge der Notifier-Arbeitswarteschlange. Siehe <a href="#">“NOTIFIER_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Betriebssystem</b>	Zeigt das Betriebssystem, auf dem die Software läuft.

Metrik	Beschreibung
<b>Länge der Outbound Enabler-Phase</b>	Zeigt die Länge der Arbeitswarteschlange für den integrierten Outbound Enabler. Siehe <a href="#">“OE_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Seiten im Datenstrom-Stack</b>	Zeigt die Anzahl der Seiten, die in den Netzwerkdatenströmen enthalten sind. Siehe <a href="#">“PAGES_IN_STREAMSTACK”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Gesperrte Seiten</b>	Zeigt die Anzahl der Cacheseiten, die in den Speicher geladen wurden. Siehe <a href="#">“PAGES_LOCKED”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Eingelesene Seiten</b>	Zeigt die Gesamtzahl aller von der Festplatte gelesenen Seiten. Siehe <a href="#">“PAGES_SWAPPED_IN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate der eingelagerten Seiten</b>	Zeigt die Rate, mit der die Seiten von der Festplatte gelesen werden. Siehe <a href="#">“PAGES_SWAPPED_IN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Ausgelagerte Seiten</b>	Zeigt die Gesamtzahl aller auf die Festplatte ausgelagerten Seiten. Siehe <a href="#">“PAGES_SWAPPED_OUT”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate der ausgelagerten Seiten</b>	Zeigt die Rate, mit der die Seiten auf die Festplatte ausgelagert werden. Siehe <a href="#">“PAGES_SWAPPED_OUT”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Verwendete Seiten</b>	Die Anzahl der verwendeten Cacheseiten. Diese umfasst auch die Seiten, die auf den Plattenspeicher ausgelagert werden, sodass sie die Cachegröße überschreiten kann. Siehe <a href="#">“PAGES_USED”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Prozent von verbundenen Clients</b>	Zeigt den Prozentsatz der Clients an, die gerade verbunden sind. Diese Metrik wird abgeleitet, indem der Wert für <b>Anzahl von verbundenen Clients</b> durch den Wert für <b>Maximale Anzahl von Clients</b> dividiert und das Ergebnis mit 100 multipliziert wird.
<b>Prozentwert der benutzten Verbindungen</b>	Zeigt den Prozentsatz der Verbindungen die derzeit verwendet werden.
<b>Prozentwert von Seiten im Datenstrom-Stack</b>	Zeigt den Prozentsatz der Seiten, die in den Netzwerkdatenströmen enthalten sind.
<b>Prozent gesperrter Seiten</b>	Zeigt den Prozentsatz der Seiten, die gesperrt sind.
<b>Prozent verwendeter Seiten</b>	Zeigt den Prozentsatz der Seiten, die derzeit verwendet werden. Diese umfasst auch die Seiten, die auf den Plattenspeicher ausgelagert werden, sodass sie die Cachegröße überschreiten kann. Siehe <a href="#">“PAGES_USED”</a> [ <i>MobiLink - Serveradministration</i> ].

Metrik	Beschreibung
<b>Pings</b>	Die Anzahl der derzeit verbundenen Clients, die einen Ping senden. Siehe “ <a href="#">NUM_CONNECTED_PINGS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Prozessorarchitektur</b>	Zeigt eine Zeichenfolge, die den Prozessortyp identifiziert.
<b>Länge der RAW-TCP-Phase</b>	Zeigt die Länge der Warteschlange für Netzwerkaufgaben. Siehe “ <a href="#">RAW_TCP_STAGE_LEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen</b>	Zeigt die Anzahl der gültigen Anforderungen, die bearbeitet werden.
<b>Anforderungen in der Phase der Upload-durchführung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Upload-Übernahme sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase der Benutzer-authentifizierung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Benutzerauthentifizierung sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase des Synchronisationsbeginns</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Synchronisationsbeginns sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in Verbindungsphase für Downloadbestätigung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Verbindungsphase für die Downloadbestätigung sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in Verbindungsphase</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Verbindungsphase sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase der Synchronisationsbeendigung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Synchronisationsbeendigung sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase des Downloadabrufs</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Downloadabrufs sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen im DB-Worker-Abruf für die Downloadbestätigungsphase</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Abrufs der Datenbank-Worker-Threads sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in Datenbank-Worker-Abrufphase</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Abrufs der Datenbank-Worker-Threads sind. Siehe <a href="#">mlsrv16-Option -vm</a> [ <i>MobiLink - Serveradministration</i> ].

Metrik	Beschreibung
<b>Anforderungen in der Phase der nicht blockierenden Downloadbestätigung</b>	Zeigt die Anzahl von Synchronisationen, die derzeit in der Phase der nicht blockierenden Downloadbestätigung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Anforderungen in der Phase der Downloadvorbereitung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Downloadvorbereitung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Anforderungen in der Upload-Empfangsphase</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Upload-Empfangsphase sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Anforderungen in der Phase des Download-Sendevorgangs</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Download-Sendevorgangs sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Anforderungen in der Phase der Synchronisationsanforderung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Synchronisationsanforderung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Anforderungen in der Wartephase der Downloadbestätigung</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Wartephase der Downloadbestätigung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Rücksetzungsrate</b>	Zeigt die Rate, mit der Rollbacks durchgeführt werden. Siehe <a href="#">“NUM_ROLLBACKS” [MobiLink - Serveradministration]</a> .
<b>Rollbacks</b>	Zeigt die Gesamtzahl der Rollbacks. Siehe <a href="#">“NUM_ROLLBACKS” [MobiLink - Serveradministration]</a> .
<b>Download-Zeilen</b>	Zeigt die Gesamtzahl der an die entfernten Datenbanken gesendeten Zeilen. Siehe <a href="#">“NUM_ROWS_DOWNLOADED” [MobiLink - Serveradministration]</a> .
<b>Zeilen-Downloadrate</b>	Zeigt die Rate, mit der Zeilen an die entfernten Datenbanken gesendet werden. Siehe <a href="#">“NUM_ROWS_DOWNLOADED” [MobiLink - Serveradministration]</a> .
<b>Upload-Zeilen</b>	Zeigt die Gesamtzahl der von den entfernten Datenbanken empfangenen Zeilen. Siehe <a href="#">“NUM_ROWS_UPLOADED” [MobiLink - Serveradministration]</a> .
<b>Zeilen-Uploadrate</b>	Zeigt die Rate, mit der Zeilen von den entfernten Datenbanken empfangen werden. Siehe <a href="#">“NUM_ROWS_UPLOADED” [MobiLink - Serveradministration]</a> .

Metrik	Beschreibung
<b>RTNotifier Lightweight-Polling-Trefferrate</b>	Zeigt die Rate, mit der bei Lightweight-Abrufen von Agenten für entfernte Aufgaben mindestens eine Anforderung gefunden wurde.
<b>RTNotifier Lightweight-Polling-Trefferrate</b>	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben, bei denen mindestens eine Anforderung gefunden wurde. Siehe “ <a href="#">SIRT_NUM_LWP_HITS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>RTNotifier Lightweight-Polling-Fehlslagrate</b>	Zeigt die Rate, mit der bei Lightweight-Abrufen von Agenten für entfernte Aufgaben keine Anforderung gefunden wurde.
<b>RTNotifier Lightweight-Polling-Fehlsläge</b>	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben, bei denen keine Anforderung gefunden wurde. Siehe “ <a href="#">SIRT_NUM_LWPS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>RTNotifier Lightweight-Polling-Rate</b>	Zeigt die Rate der Lightweight-Abrufe von Agenten für entfernte Aufgaben.
<b>RTNotifier Lightweight-Polling</b>	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben. Siehe “ <a href="#">SIRT_NUM_REQUESTS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Server-Cachegröße</b>	Zeigt die Größe des Server-Cache.
<b>Servername</b>	Zeigt den Namen des MobiLink-Servers, wie er in der Option -zs für den verbundenen Server angegeben ist. Der Standardwert ist <default>. Siehe „ <a href="#">mlsrv16-Option -zs</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Serverzeit-Offset</b>	Zeigt den Zeitunterschied zwischen der Zeit auf dem Computer, auf dem der Monitor läuft, und die Zeit auf dem Computer, auf dem Sie die Monitor-Daten anzeigen. Siehe „ <a href="#">Einführung in die Zeitanzeige</a> “ auf Seite 1131.
<b>Vom Server protokollierte Speichernutzung</b>	Zeigt den vom Server zugewiesenen Speicherplatz. Verwenden Sie diese Metrik für Nicht-Windows-Systeme, in denen die MEMORY_USED-Metrik nicht zur Verfügung steht. Auf Microsoft Windows-Systemen können Sie mit der MEMORY_USED-Metrik eine höhere Genauigkeit erzielen. Siehe “ <a href="#">TRACKED_MEMORY</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Startzeit</b>	Zeigt die Zeit, zu der der MobiLink-Server gestartet wurde.
<b>Teil der Synchronisation hat begonnen</b>	Zeigt die Rate, mit der Synchronisationen gestartet werden.
<b>Länge der Datenstromphase</b>	Zeigt die Länge der Warteschlange für Netzwerkaufgaben einer hohen Ebene. Siehe “ <a href="#">STREAM_STAGE_LEN</a> ” [ <i>MobiLink - Serveradministration</i> ].

Metrik	Beschreibung
<b>Erfolgreiche Synchronisationen</b>	Zeigt die Gesamtzahl der erfolgreichen Synchronisationen. Siehe “ <a href="#">NUM_SUCCESS_SYNCs</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Synchronisationsfehleranteil</b>	Zeigt die Rate der Synchronisationsfehler.
<b>Anteil von Synchronisationswarnungen</b>	Zeigt die Rate der Synchronisationswarnungen für den Server.
<b>Synchronisationen</b>	Zeigt die Anzahl der derzeit verbundenen Datensynchronisationen. Siehe <a href="#">NUM_CONNECTED_SYNCs</a> .
<b>Blockierte Synchronisationen</b>	Zeigt die Anzahl der Synchronisationen, die derzeit auf eine Datenbankverbindung warten.
<b>Fertiggestellte Synchronisationen</b>	Zeigt die Gesamtzahl der abgeschlossenen Synchronisationen.
<b>Gestartete Synchronisationen</b>	Zeigt die Gesamtzahl der gestarteten Synchronisationen.
<b>Gelesene TCP-Byte</b>	Zeigt die Gesamtzahl aller gelesenen Byte. Siehe “ <a href="#">TCP_BYTES_READ</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Rate gelesener TCP-Byte</b>	Zeigt die Rate, mit der Byte aus dem Netzwerk gelesen werden. Siehe “ <a href="#">TCP_BYTES_READ</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geschriebene TCP-Byte</b>	Zeigt die Gesamtzahl aller geschriebenen Byte. Siehe “ <a href="#">TCP_BYTES_WRITTEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Rate geschriebener TCP-Byte</b>	Zeigt die Rate, mit der Byte in das Netzwerk geschrieben werden. Siehe “ <a href="#">TCP_BYTES_WRITTEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geschlossene TCP-Verbindungen</b>	Zeigt die Gesamtzahl aller geschlossenen Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_CLOSED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geöffnete TCP-Verbindungen</b>	Zeigt die Gesamtzahl aller geöffneten Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_OPENED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Zurückgewiesene TCP-Verbindungen</b>	Zeigt die Gesamtzahl aller abgelehnten Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_REJECTED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Phase für zeitlich begrenzte Arbeit</b>	Zeigt die Länge der Arbeitswarteschlange für das dynamische Caching. Siehe “ <a href="#">TIMED_WORK_STAGE_LEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Nicht verfügbar seit</b>	Zeigt den Zeitpunkt, ab dem die Ressource nicht mehr zur Verfügung stand.

Metrik	Beschreibung
<b>Unbekannter Verbundene Clients</b>	Zeigt die Anzahl der verbundenen Clients, deren Ursprünge unbekannt sind.
<b>Nicht gesendete Fehlerberichte</b>	Zeigt die Anzahl von nicht gesendeten Fehlerberichten für den Server. Ein Fehlerbericht wird eingesendet, wenn die Software abstürzt. Siehe „ <a href="#">Unterdrücken von Alarmen für nicht gesendete Fehlerberichte aus Ressourcen</a> “ auf Seite 1185.
<b>Verwendete Upload-Verbindungen</b>	Zeigt die Anzahl der derzeit verwendeten Upload-Verbindungen. Siehe „ <a href="#">NUM_UPLOAD_CONNS_IN_USE</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Upload der Synchronisationen</b>	Zeigt die Anzahl der Synchronisationen, die derzeit in der Upload-Phase sind.
<b>Version</b>	Zeigt die Version der ausgeführten Software an.
<b>Speichernutzung der VM</b>	Zeigt den von zugeordneten VMs genutzten Speicherplatz. Siehe „ <a href="#">VM_MEM_USE</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Warten auf Datenbankverbindung</b>	Anzahl der Anforderungen, die auf eine Datenbankverbindung warten.
<b>Warnungen</b>	Zeigt die Gesamtzahl der Warnungen. Siehe „ <a href="#">NUM_WARNINGS</a> “ [ <i>MobiLink - Serveradministration</i> ].

#### Liste von Metriken für MobiLink-Serverfarm-Ressourcen

Metrik	Bereich	Beschreibung
<b>Synchronisationen werden authentifiziert</b>	Mittelwert	Zeigt die Anzahl der Anforderungen im Server, die sich derzeit in der Phase der Benutzerauthentifizierung befinden. Hinweise zu den Synchronisationsphasen finden Sie unter „ <a href="#">mlsrv16-Option -v</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Rate gelesener Byte</b>	Mittelwert	Zeigt die Rate, mit der Byte aus dem Netzwerk gelesen werden. Siehe „ <a href="#">TCP_BYTES_READ</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Rate geschriebener Byte</b>	Mittelwert	Zeigt die Rate, mit der Byte in das Netzwerk geschrieben werden. Siehe „ <a href="#">TCP_BYTES_WRITTEN</a> “ [ <i>MobiLink - Serveradministration</i> ].
<b>Zwischengespeicherte entfernte Aufgabenanforderungen</b>	Mittelwert	Zeigt die Anzahl der im Cache gespeicherten entfernten Aufgabenanforderungen. Siehe „ <a href="#">SIRT_NUM_REQUESTS</a> “ [ <i>MobiLink - Serveradministration</i> ].

Metrik	Bereich	Beschreibung
<b>Länge der Befehlsprozessor-Phase</b>	Mittelwert	Zeigt die Länge der Warteschlange für Synchronisationsaufgaben. Siehe <a href="#">“CMD_PROCESSOR_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Festschreiberate</b>	Mittelwert	Zeigt die Rate, mit der Festschreibungen durchgeführt werden.
<b>Festschreibungen</b>	Mittelwert	Zeigt die Gesamtzahl der Festschreibungen. Siehe <a href="#">“NUM_COMMITS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Anteil von abgeschlossenen Synchronisationen</b>	Summe	Zeigt die Rate der erfolgreich abgeschlossenen Synchronisationen für den Server an.
<b>Verbundene Clients</b>	Mittelwert	Zeigt die Anzahl von verbundenen Synchronisationsclients. Siehe <a href="#">“ML_NUM_CONNECTED_CLIENTS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate geschlossener Verbindungen</b>	Mittelwert	Zeigt die Rate, mit der TCP-Verbindungen geschlossen werden.
<b>Rate geöffneter Verbindungen</b>	Mittelwert	Zeigt die Rate, mit der TCP-Verbindungen geöffnet werden.
<b>Rate abgelehnter Verbindungen</b>	Mittelwert	Zeigt die Rate, mit der Verbindungen vom Server abgelehnt werden.
<b>CPU-Gesamtzeit</b>	Summe	Zeigt den Umfang der vom MobiLink-Server verwendeten CPU-Zeit in Mikrosekunden. Siehe <a href="#">“CPU_USAGE”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>CPU-Nutzung</b>	Mittelwert	Zeigt den Prozentsatz der CPU-Kapazität, der vom MobiLink-Server belegt wird.
<b>Aktuelle TCP-Verbindungen</b>	Summe	Zeigt die Anzahl der TCP-Verbindungen, die derzeit von diesem MobiLink-Server benutzt werden.
<b>Verwendete Datenbankverbindungen</b>	Summe	Zeigt die Anzahl der derzeit verwendeten Datenbankverbindungen. Siehe <a href="#">“DB_CONNECTIONS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Download der Synchronisationen</b>	Mittelwert	Zeigt die aktuelle Anzahl der Synchronisationen an, die in den Phasen "Download vorbereiten", "Download abrufen", "Auf Download-Quittierung warten" oder "Synch_Ende" sind. Hinweise zu den Synchronisationsphasen finden Sie unter „ <a href="#">mlsrv16-Option - v</a> “ [ <i>MobiLink - Serveradministration</i> ].

Metrik	Bereich	Beschreibung
<b>Fehler</b>	Mittelwert	Zeigt die durchschnittliche Anzahl von Fehlern. Siehe “ <a href="#">NUM_ERRORS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Anteil von fehlgeschlagenen Synchronisationen</b>	Summe	Zeigt die Rate der fehlgeschlagenen Synchronisationen für den Server.
<b>Fehlgeschlagene Synchronisationen</b>	Mittelwert	Zeigt die Gesamtzahl der fehlgeschlagenen Synchronisationen. Siehe “ <a href="#">NUM_FAILED_SYNCs</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Dateiübertragungen</b>	Summe	Zeigt die Anzahl der derzeitigen MobiLink-Dateiübertragungen. Siehe “ <a href="#">NUM_CONNECTED_FILE_XFERS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Abgeschlossener Synchronisationsanteil</b>	Summe	Zeigt die Rate, mit der Synchronisationen abgeschlossen werden.
<b>Freier Festplattenspeicher für MobiLink-Cache</b>	Mittelwert	Zeigt den verfügbaren Festplattenspeicher auf der temporären Festplatte für den MobiLink-Cache in Byte. Siehe “ <a href="#">FREE_DISK_SPACE</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Heartbeat-Phase</b>	Mittelwert	Zeigt die Länge der Warteschlange für periodische Aufgaben, die nicht im Rahmen der Synchronisation ausgeführt werden. Siehe “ <a href="#">HEARTBEAT_STAGE_LEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Listener</b>	Summe	Zeigt die Anzahl der derzeit verbundenen Listener. Siehe “ <a href="#">NUM_CONNECTED_LISTENERS</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Synchronisationszeit</b>	Maximum	Zeigt die maximale Zeit an, die eine Synchronisation gedauert hat. Das Alter der ältesten Synchronisation in Mikrosekunden. Siehe “ <a href="#">LONGEST_SYNC</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Max. Wartezeit für Verbindung</b>	Maximum	Zeigt den längsten Zeitraum, den eine aktive Synchronisation auf die Datenbank warten musste. Siehe “ <a href="#">LONGEST_DB_WAIT</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Verwendeter Speicher</b>	Mittelwert	Zeigt die Anzahl der vom RAM-Speicher verwendeten Byte. Zeigt die protokollierte Speichernutzung, wenn der Server auf einer anderen Plattform als Windows läuft. Siehe “ <a href="#">MEMORY_USED</a> ” [ <i>MobiLink - Serveradministration</i> ] und “ <a href="#">TRACKED_MEMORY</a> ” [ <i>MobiLink - Serveradministration</i> ].

Metrik	Bereich	Beschreibung
<b>Monitore</b>	Summe	Zeigt die Anzahl der derzeit verbundenen Monitore und Mobi-Link-Profiler. Siehe <a href="#">“NUM_CONNECTED_MONITORS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Notifier-Phase</b>	Mittelwert	Zeigt die Länge der Notifier-Arbeitswarteschlange. Siehe <a href="#">“NOTIFIER_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Outbound Enabler-Phase</b>	Mittelwert	Zeigt die Länge der Arbeitswarteschlange für den integrierten Outbound Enabler. Siehe <a href="#">“OE_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Seiten im Datenstrom-Stack</b>	Mittelwert	Zeigt die Anzahl der Seiten, die in den Netzwerkdatenströmen enthalten sind. Siehe <a href="#">“PAGES_IN_STREAMSTACK”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Gesperrte Seiten</b>	Mittelwert	Zeigt die Anzahl der Cacheseiten, die in den Speicher geladen wurden. Siehe <a href="#">“PAGES_LOCKED”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Eingelesene Seiten</b>	Mittelwert	Zeigt die Gesamtzahl aller von der Festplatte gelesenen Seiten. Siehe <a href="#">“PAGES_SWAPPED_IN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate der eingelagerten Seiten</b>	Mittelwert	Zeigt die Rate, mit der die Seiten von der Festplatte gelesen werden. Siehe <a href="#">“PAGES_SWAPPED_IN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Ausgelagerte Seiten</b>	Mittelwert	Zeigt die Gesamtzahl aller auf die Festplatte ausgelagerten Seiten. Siehe <a href="#">“PAGES_SWAPPED_OUT”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Rate der ausgelagerten Seiten</b>	Mittelwert	Zeigt die Rate, mit der die Seiten auf die Festplatte ausgelagert werden. Siehe <a href="#">“PAGES_SWAPPED_OUT”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Verwendete Seiten</b>	Mittelwert	Die Anzahl der verwendeten Cacheseiten. Diese umfasst auch die Seiten, die auf die Festplatte ausgelagert werden, sodass sie die Cachegröße überschreiten kann. Siehe <a href="#">“PAGES_USED”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Prozent von verbundenen Clients</b>	Mittelwert	Zeigt den Prozentsatz der Clients an, die gerade verbunden sind. Diese Metrik wird abgeleitet, indem der Wert für <b>Anzahl von verbundenen Clients</b> durch den Wert für <b>Maximale Anzahl von Clients</b> dividiert und das Ergebnis mit 100 multipliziert wird.

Metrik	Bereich	Beschreibung
<b>Prozentwert der benutzten Verbindungen</b>	Mittelwert	Zeigt den Prozentsatz der Verbindungen die derzeit verwendet werden.
<b>Prozentwert von Seiten im Datenstrom-Stack</b>	Mittelwert	Zeigt den Prozentsatz der Seiten, die in den Netzwerkdatenströmen enthalten sind.
<b>Prozent gesperrter Seiten</b>	Mittelwert	Zeigt den Prozentsatz der Seiten, die gesperrt sind.
<b>Prozent verwendeter Seiten</b>	Mittelwert	Zeigt den Prozentsatz der Seiten, die derzeit verwendet werden. Diese umfasst auch die Seiten, die auf die Festplatte ausgelagert werden, sodass sie die Cachegröße überschreiten kann. Siehe <code>PAGES_USED</code> .
<b>Pings</b>	Summe	Die Anzahl der derzeit verbundenen Clients, die einen Ping senden. Siehe <code>"NUM_CONNECTED_PINGS"</code> [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der RAW-TCP-Phase</b>	Mittelwert	Zeigt die Länge der Warteschlange für Netzwerkaufgaben. Siehe <code>"RAW_TCP_STAGE_LEN"</code> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen</b>	Summe	Zeigt die Anzahl der gültigen Anforderungen, die bearbeitet werden.
<b>Anforderungen in der Phase der Uploaddurchführung</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Upload-Übernahme sind. Siehe <code>mlsrv16-Option -vm</code> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase der Benutzerauthentifizierung</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Benutzerauthentifizierung sind. Siehe <code>mlsrv16-Option -vm</code> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in der Phase des Synchronisationsbeginns</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Synchronisationsbeginns sind. Siehe <code>mlsrv16-Option -vm</code> [ <i>MobiLink - Serveradministration</i> ].
<b>Anforderungen in Verbindungsphase für Downloadbestätigung</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Verbindungsphase für die Downloadbestätigung sind. Siehe <code>mlsrv16-Option -vm</code> [ <i>MobiLink - Serveradministration</i> ].

Metrik	Bereich	Beschreibung
Anforderungen in Verbindungsphase	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Verbindungsphase sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase der Synchronisationsbeendigung	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Synchronisationsbeendigung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase des Downloadabrufs	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Downloadabrufs sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen im DB-Worker-Abruf für die Downloadbestätigungsphase	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Abrufs der Datenbank-Worker-Threads sind. Siehe “ <a href="#">NUM_IN_GET_DB_WORKER_FOR_ACK</a> ” <a href="#">[MobiLink - Serveradministration]</a> .
Anforderungen in Datenbank-Worker-Abrufphase	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Abrufs der Datenbank-Worker-Threads sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase der nicht blockierenden Downloadbestätigung	Mittelwert	Zeigt die Anzahl von Synchronisationen, die derzeit in der Phase der nicht blockierenden Downloadbestätigung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase der Downloadvorbereitung	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Downloadvorbereitung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Upload-Empfangsphase	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Upload-Empfangsphase sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase des Download-Sendevorgangs	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase des Download-Sendevorgangs sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
Anforderungen in der Phase der Synchronisationsanforderung	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Phase der Synchronisationsanforderung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .

Metrik	Bereich	Beschreibung
<b>Anforderungen in der Wartephase der Downloadbestätigung</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Wartephase der Downloadbestätigung sind. Siehe <a href="#">mlsrv16-Option -vm [MobiLink - Serveradministration]</a> .
<b>Rücksetzungsrate</b>	Mittelwert	Zeigt die Gesamtzahl der Rollbacks. Siehe <a href="#">“NUM_ROLLBACKS” [MobiLink - Serveradministration]</a> .
<b>Rollbacks</b>	Mittelwert	Zeigt die Gesamtzahl der Rollbacks. Siehe <a href="#">“NUM_ROLLBACKS” [MobiLink - Serveradministration]</a> .
<b>Download-Zeilen</b>	Mittelwert	Zeigt die Gesamtzahl der an die entfernten Datenbanken gesendeten Zeilen. Siehe <a href="#">“NUM_ROWS_DOWNLOADED” [MobiLink - Serveradministration]</a> .
<b>Zeilen-Download-rate</b>	Mittelwert	Zeigt die Gesamtzahl der an die entfernten Datenbanken gesendeten Zeilen. Siehe <a href="#">“NUM_ROWS_DOWNLOADED” [MobiLink - Serveradministration]</a> .
<b>Upload-Zeilen</b>	Mittelwert	Zeigt die Gesamtzahl der von den entfernten Datenbanken empfangenen Zeilen. Siehe <a href="#">“NUM_ROWS_UPLOADED” [MobiLink - Serveradministration]</a> .
<b>Zeilen-Uploadrate</b>	Mittelwert	Zeigt die Gesamtzahl der von den entfernten Datenbanken empfangenen Zeilen. Siehe <a href="#">“NUM_ROWS_UPLOADED” [MobiLink - Serveradministration]</a> .
<b>RTNotifier Lightweight-Polling-Trefferrate</b>	Mittelwert	Zeigt die Rate, mit der bei Lightweight-Abrufen von Agenten für entfernte Aufgaben mindestens eine Anforderung gefunden wurde.
<b>RTNotifier Lightweight-Polling-Treffer</b>	Mittelwert	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben, bei denen mindestens eine Anforderung gefunden wurde. Siehe <a href="#">“SIRT_NUM_LWP_HITS” [MobiLink - Serveradministration]</a> .
<b>RTNotifier Lightweight-Polling-Fehlschlagrate</b>	Mittelwert	Zeigt die Rate, mit der bei Lightweight-Abrufen von Agenten für entfernte Aufgaben keine Anforderung gefunden wurde.
<b>RTNotifier Lightweight-Polling-Fehlschläge</b>	Mittelwert	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben, bei denen keine entfernten Aufgaben gefunden wurden. Siehe <a href="#">“SIRT_NUM_LWPS” [MobiLink - Serveradministration]</a> .

Metrik	Bereich	Beschreibung
<b>RTNotifier Lightweight-Polling-Rate</b>	Mittelwert	Zeigt die Rate der Lightweight-Abrufe von Agenten für entfernte Aufgaben.
<b>RTNotifier Lightweight-Polling</b>	Mittelwert	Zeigt die Anzahl der Lightweight-Abrufe von Agenten für entfernte Aufgaben. Siehe <a href="#">“SIRT_NUM_REQUESTS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Server-Cachegröße</b>	Mittelwert	Zeigt die Größe des Server-Cache.
<b>Vom Server protokollierte Speichernutzung</b>	Mittelwert	Zeigt den vom Server zugewiesenen Speicherplatz. Verwenden Sie diese Metrik für Nicht-Windows-Systeme, in denen die MEMORY_USED-Metrik nicht zur Verfügung steht. Auf Microsoft Windows-Systemen können Sie mit der MEMORY_USED-Metrik eine höhere Genauigkeit erzielen. Siehe <a href="#">“TRACKED_MEMORY”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Teil der Synchronisation hat begonnen</b>	Summe	Zeigt die Rate, mit der Synchronisationen gestartet werden.
<b>Länge der Datenstromphase</b>	Mittelwert	Zeigt die Länge der Warteschlange für Netzwerkaufgaben einer hohen Ebene. Siehe <a href="#">“STREAM_STAGE_LEN”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Erfolgreiche Synchronisationen</b>	Mittelwert	Zeigt die Gesamtzahl der erfolgreichen Synchronisationen. Siehe <a href="#">“NUM_SUCCESS_SYNCS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Synchronisationsfehleranteil</b>	Summe	Zeigt die Rate der Synchronisationsfehler.
<b>Anteil von Synchronisationswarnungen</b>	Summe	Zeigt die Rate der Synchronisationswarnungen für den Server.
<b>Synchronisationen</b>	Summe	Zeigt die Anzahl der derzeit verbundenen Datensynchronisationen. Siehe NUM_CONNECTED_SYNCS <a href="#">“NUM_CONNECTED_SYNCS”</a> [ <i>MobiLink - Serveradministration</i> ].
<b>Blockierte Synchronisationen</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit auf eine Datenbankverbindung warten.
<b>Fertiggestellte Synchronisationen</b>	Summe	Anzahl von Synchronisationen:

Metrik	Bereich	Beschreibung
<b>Gestartete Synchronisationen</b>	Summe	Zeigt die Gesamtzahl der gestarteten Synchronisationen.
<b>Gelesene TCP-Byte</b>	Mittelwert	Zeigt die Gesamtzahl aller gelesenen Byte. Siehe “ <a href="#">TCP_BYTES_READ</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geschriebene TCP-Byte</b>	Mittelwert	Zeigt die Gesamtzahl aller geschriebenen Byte. Siehe “ <a href="#">TCP_BYTES_WRITTEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geschlossene TCP-Verbindungen</b>	Mittelwert	Zeigt die Gesamtzahl aller geschlossenen Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_CLOSED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Geöffnete TCP-Verbindungen</b>	Mittelwert	Zeigt die Gesamtzahl aller geöffneten Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_OPENED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Zurückgewiesene TCP-Verbindungen</b>	Mittelwert	Zeigt die Gesamtzahl aller abgelehnten Verbindungen. Siehe “ <a href="#">TCP_CONNECTIONS_REJECTED</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Länge der Phase für zeitlich begrenzte Arbeit</b>	Mittelwert	Zeigt die Länge der Arbeitswarteschlange für das dynamische Caching. Siehe “ <a href="#">TIMED_WORK_STAGE_LEN</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Unbekannter Verbundene Clients</b>	Mittelwert	Zeigt die Anzahl der verbundenen Clients, deren Ursprünge unbekannt sind.
<b>Verwendete Upload-Verbindungen</b>	Mittelwert	Zeigt die Anzahl der derzeit verwendeten Upload-Verbindungen. Siehe “ <a href="#">NUM_UPLOAD_CONNS_IN_USE</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Upload der Synchronisationen</b>	Mittelwert	Zeigt die Anzahl der Synchronisationen, die derzeit in der Upload-Phase sind.
<b>Speichernutzung der VM</b>	Mittelwert	Zeigt den von zugeordneten VMs genutzten Speicherplatz. Siehe “ <a href="#">VM_MEM_USE</a> ” [ <i>MobiLink - Serveradministration</i> ].
<b>Warten auf Datenbankverbindung</b>	Mittelwert	Anzahl der Anforderungen, die auf eine Datenbankverbindung warten.
<b>Warnungen</b>	Mittelwert	Zeigt die durchschnittliche Anzahl von Warnungen. Siehe “ <a href="#">NUM_WARNINGS</a> ” [ <i>MobiLink - Serveradministration</i> ].

**Liste von Metriken für Relay Server-Farmressourcen**

<b>Metrik</b>	<b>Beschreibung</b>
Aktive Anforderungen	Zeigt die Gesamtzahl der gleichzeitigen Anforderungen.
Durchschnittliche Verarbeitungszeit des Backend-Servers	Misst die durchschnittliche Zeit, die der Backend-Server für die Verarbeitung einer HTTP-Anforderung benötigt.
Durchschnittliche Anforderungsabschlusszeit	Misst die durchschnittliche Zeit, die der Relay Server nach dem Senden einer Antwort an den Client darauf wartet, dass eine Backend-Verbindung geschlossen wird.
Durchschnittliche Anforderungszeit	Misst die durchschnittliche Zeit, die der Relay Server auf den Empfang der gesamten HTTP-Anforderung vom Client wartet.
Durchschnittliche Zeit des Antwortzyklus für die Anforderung	Misst die durchschnittliche Zeit, die der Relay Server benötigt, um eine Anforderung zu verarbeiten und eine Antwort zu empfangen.
Durchschnittliche Antwortzeit	Misst die durchschnittliche Zeit, die der Relay Server benötigt, um die gesamte HTTP-Antwort vom Backend-Server zu empfangen.
Kanal-Timeout	Die maximale Verarbeitungszeit für den Relay Server zur Erkennung von Blackouts bei Backend-Diensten.
CPU-Nutzung	Misst den Prozentsatz der CPU-Zeit, der vom Relay Server belegt wird.
Heruntergeladene Kanal-Byte	Zeigt die Gesamtzahl der Byte, die während der letzten Sammlungsperiode vom Outbound Enabler an die Backend-Server Erweiterung geliefert wurden.
Fehlerzahl	Zeigt die Gesamtzahl der während der letzten Sammlungsperiode aufgetretenen Fehler. Diese Anzahl enthält die Fehlerzahl der untergeordneten Elemente.

Metrik	Beschreibung
Farmstatus	<p>Zeigt den aktuellen Status der Relay Server-Farm:</p> <ul style="list-style-type: none"> <li>● <b>0</b> Die Relay Server-Farm ist aktiviert und kann den Dienst normal bereitstellen.</li> <li>● <b>1</b> Die Relay Server-Farm ist deaktiviert, sodass der Outbound Enabler keine Verbindung herstellen und keinen Dienst bereitstellen kann. Die Clients können ebenfalls nicht über Relay Server auf diese Backend-Farm zugreifen.</li> <li>● <b>2</b> Die Relay Server-Farm ist aktiviert, aber einige der Outbound Enabler sind nicht mit allen Relay Servern in der Relay Server-Farm verbunden. Die Qualität des Dienstes kann beeinträchtigt sein.</li> <li>● <b>3</b> Die Relay Server-Farm ist aktiviert, aber keiner der Backend Server ist verbunden. Daher kann kein Client auf diese Backend-Farm zugreifen.</li> </ul>
Freier Speicherplatz für Logdatei	Zeigt den verfügbaren Speicherplatz für die Logdatei der Relay Server-Farm.
Host	Zeigt den Namen des Computers, auf dem die Relay Server-Farm läuft.
Betriebssystemversion	Zeigt das Betriebssystem, auf dem die Relay Server-Software läuft, einschließlich Build-Nummern und Service-Packs.
Spitzenwert aktiver Anforderungen	Zeigt die maximale Anzahl von gleichzeitigen Anforderungen seit dem Start des Relay Servers.
Spitzennutzung des gemeinsamen Speichers	Zeigt die maximale Nutzung des gemeinsamen Speichers für den Relay Server seit dem Start des Relay Servers.
Prozessorarchitektur	Zeigt den Typ des Prozessors, auf dem die Relay Server-Farm läuft.
Relay Server-Startzeit	Zeigt die Startzeit für den Relay Server. Bei einem Backend Server wird die Zeit angezeigt, zu der der Outbound Enabler eine Verbindung mit der Backend-Servererweiterung herstellt.
Relay Server-Status	Zeigt den Status des Relay Servers.
Relay Server-Version	Zeigt die Version der ausgeführten Relay Server-Software an.
Anforderungsbyte	Zeigt die Gesamtzahl der Bytes aus HTTP-Anforderungen, die vom Client an die Clienterweiterung geliefert werden.

Metrik	Beschreibung
Anforderung abgeschlossen	Zeigt die Gesamtzahl der abgeschlossenen Antwortzyklen für Anfragen.
Antwortbyte	Zeigt die Gesamtzahl der Bytes aus HTTP-Anforderungen, die von der Clienterweiterung an den Client geliefert werden.
Sitzungen erstellt	Zeigt die Gesamtzahl der neu erstellten HTTP-Sitzungen.
Grenzwert für gemeinsamen Speicher	Zeigt die Gesamtgröße des gemeinsamen Speichers an, der dem Relay Server zur Verfügung steht.
Nicht verfügbar seit	Zeigt den Zeitpunkt, ab dem die Ressource nicht mehr zur Verfügung stand.
Heraufgeladene Kanal-Byte	Zeigt die Gesamtzahl der Byte, die von der Backend-Servererweiterung an den Outbound Enabler geliefert werden.
Webserver-Version	Zeigt die Version der ausgeführten Webserver-Software an.

## Sammlungsintervalle für Ressourcen festlegen

Sie können die Rate ändern, mit der Metriken vom Monitor gesammelt werden. Die im Monitor angezeigten Metriken sind nur so genau wie das Sammlungsintervall, das standardmäßig 30 Sekunden lang ist.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Kontext und Bemerkungen

Das Sammlungsintervall für eine Ressource unterscheidet sich von der Aktualisierungsrate der Monitor-Anzeige. Weitere Hinweise finden Sie unter „[Metriken aktualisieren](#)“ auf Seite 1175.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Ressourcen**.
4. Klicken Sie auf die Ressource und anschließend auf **Konfigurieren**.
5. Klicken Sie auf **Sammlungsintervall**.
6. Geben Sie das Intervall an, in dem Metriken gesammelt werden (*hours:minutes:seconds*). Das Sammlungsintervall muss mindestens 10 Sekunden lang sein.

7. Klicken Sie auf **Speichern**.
8. Geben Sie Ihre Benutzer-ID und Ihr Kennwort ein und klicken Sie auf **OK**.
9. Klicken Sie auf **Schließen**.
10. Klicken Sie auf **Schließen**.

### Ergebnisse

Das Sammlungsintervall für die Ressource wird festgelegt..

## Exportieren von Metriken

Sie können Metriken, mit denen ein Diagramm oder eine Tabelle verknüpft ist, in eine XML-Datei exportieren. Beispiel: Die meisten Metriken im Widget **Wichtigste Performance-Metriken** können exportiert werden. Die maximale Menge der Daten, die in eine Datei exportiert werden kann, beträgt 25 Metriken oder 1 Million Punkte.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Öffnen Sie ein Dashboard.
3. Klicken Sie in einem Widget, in dem die Metriken angezeigt werden, auf den Pfeil am Dropdown-Menü, klicken Sie anschließend auf **Exportieren** und befolgen Sie die Anweisungen im Fenster **Metriken exportieren**.

#### Hinweis

Sie können nicht mehr als 25 Metriken oder mehr als eine Million Punkte exportieren. Wenn Sie dies tun, erhalten Sie eine Fehlermeldung und kehren zum Exportbildschirm zurück, damit Sie weniger Metriken oder einen kleineren Zeitbereich auswählen können.

4. Klicken Sie auf **Exportieren**.
5. Wenn Sie dazu aufgefordert werden, geben Sie einen Dateinamen mit der Dateierweiterung *.xml* ein.
6. Klicken Sie auf **Speichern**.

### Ergebnisse

Eine XML-Datei mit den angegebenen Metriken wird erstellt.

## Metriken aktualisieren

Die Monitor-Anzeige wird standardmäßig jede Minute automatisch aktualisiert. Sie können das Aktualisierungsintervall ändern. Dies ist unabhängig von der Datensammlungsrate für eine Ressource.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Legen Sie die Aktualisierungsrate fest.
  - a. Klicken Sie auf **Extras » Benutzereinstellungen**.
  - b. Ändern Sie die Einstellungen nach Bedarf. Der Standardwert ist eine Minute.
  - c. Klicken Sie auf **Speichern**.
2. Klicken Sie auf **Daten aktualisieren**.

Der Monitor ruft die neuesten Metriken ab und zeigt sie an.

### Ergebnisse

Das Aktualisierungsintervall wird geändert.

### Nächste Schritte

Wenn Sie F5 drücken, lädt der Monitor den Browser neu, ruft die bisher vom Monitor gesammelten Metriken ab und zeigt sie an.

### Siehe auch

- [„Metriken“ auf Seite 1149](#)

## Monitor-Benutzer

Sie müssen sich beim Monitor mit einem Benutzernamen und einem Kennwort anmelden. Der Benutzername und das Kennwort für das Anmelden beim Monitor berücksichtigen die Groß- und Kleinschreibung.

Der Monitor unterstützt drei Arten von Benutzern:

Benutzertyp	Beschreibung
Benutzer ohne Schreibrechte	Diese Benutzer haben nur Lesezugriff zur Überwachung der Ressourcen. Benutzer ohne Schreibrechte können die Metriken anzeigen, haben aber keinen Zugriff auf das Fenster <b>Administration</b> . Wenn Sie einen Benutzer über das Anmeldefenster erstellen, handelt es sich um einen Benutzer ohne Schreibrechte. Ein Benutzername und ein Kennwort sind erforderlich.

Benutzertyp	Beschreibung
Operator	Dieser Benutzer hat Lesezugriff zur Überwachung der Ressourcen und kann Alarme empfangen. Operatoren können die Metriken anzeigen, E-Mail-Alarme empfangen sowie Alarme auflösen und löschen. Sie können jedoch nicht auf die Registerkarte <b>Administration</b> zugreifen. Ein Benutzername und ein Kennwort sind erforderlich.
Administrator	Administratoren haben denselben Zugriff wie Operatoren und können zusätzlich Ressourcen konfigurieren und Benutzer hinzufügen. Monitor-Administratoren können auch auf das Fenster <b>Administration</b> zugreifen. Der Standardbenutzer <b>admin</b> ist ein Monitor-Administrator. Ein Benutzername und ein Kennwort sind erforderlich.

Sie können Ihren Monitor-Benutzertyp überprüfen, indem Sie sich beim Monitor anmelden und anschließend auf **Extras » Benutzereinstellungen** klicken. Sie können auch Ihre Benutzereinstellungen ändern. Nur ein Monitor-Administrator kann den Typ eines Benutzers ändern.

### Standardbenutzer

Wenn Sie den Monitor zum ersten Mal starten, hat er standardmäßig einen Monitor-Administrator mit dem Benutzernamen **admin** und dem Kennwort **admin**. Es wird empfohlen, das Standardkennwort für den Monitor-Administrator zu ändern, um den Zugriff auf den Monitor einzuschränken. Siehe „[Monitor-Benutzer bearbeiten](#)“ auf Seite 1179.

### Siehe auch

- „[Monitor-Benutzer bearbeiten](#)“ auf Seite 1179
- „[Fenster Administration für den Monitor](#)“ auf Seite 1131

## Monitor-Benutzer erstellen

Mithilfe des Fensters **Administration** können Sie Benutzer beliebigen Typs erstellen, einschließlich Monitor-Administratoren.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration** und anschließend auf **Benutzer**.
3. Klicken Sie auf **Neu** und geben Sie die Informationen für den neuen Benutzer ein.

Eine E-Mail-Adresse ist nur für Monitor-Administratoren und -Operatoren erforderlich, die E-Mail-Alarme vom Monitor erhalten sollen.

Die angegebene Sprache legt die vom Monitor verwendete Sprache fest, einschließlich der Sprache für Alarme.

4. Klicken Sie auf **Weiter** und geben Sie die Ressourcen-Dashboards für den Benutzer an.
5. Klicken Sie auf **Speichern** und anschließend auf **Schließen**.

## Ergebnisse

Ein neuer Benutzer wird erstellt.

## Nächste Schritte

Wenn Sie einen Monitor-Administrator oder Operator erstellt haben, können Sie den Benutzer Ressourcen zuordnen und er kann Alarmbenachrichtigungen per E-Mail empfangen.

## Siehe auch

- [„Zuordnen von Monitor-Benutzern zu einer Ressource“ auf Seite 1178](#)
- [„Benutzererstellung auf Monitor-Administratoren einschränken“ auf Seite 1180](#)
- [„Alarm-E-Mails anpassen“ auf Seite 1188](#)
- [„Monitor-Benutzer“ auf Seite 1175](#)
- [„Monitor-Benutzer bearbeiten“ auf Seite 1179](#)

## Monitor-Benutzer ohne Schreibrechte erstellen

Standardmäßig können Sie einen eigenen Benutzer ohne Schreibrechte erstellen, der dann nur Lesezugriff auf den Monitor hat.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

Monitor-Administratoren können dieses Standardverhalten so ändern, dass nur Monitor-Administratoren Benutzer erstellen können.

## Aufgabe

1. Klicken Sie im Anmeldefenster auf **Neuen Benutzer erstellen**.

### Hinweis

Wenn der Link **Neuen Benutzer erstellen** nicht verfügbar ist, hat der Administrator das Standardverhalten so geändert, dass nur Monitor-Administratoren neue Benutzer erstellen können. Bitten Sie Ihren Monitor-Administrator, einen neuen Benutzer zu erstellen.

2. Geben Sie die Informationen für den neuen Benutzer ein.

Eine E-Mail-Adresse ist nur erforderlich, wenn der Benutzer E-Mail-Alarme vom Monitor erhalten soll. Nur Monitor-Administratoren und -Operatoren können E-Mail-Alarme erhalten. Bitten Sie Ihren Monitor-Administrator, Ihren Benutzertyp zu ändern und E-Mail-Alarme zu aktivieren.

### Ergebnisse

Ein neuer Benutzer ohne Schreibrechte wird erstellt.

### Nächste Schritte

Keine.

### Siehe auch

- [„Zuordnen von Monitor-Benutzern zu einer Ressource“ auf Seite 1178](#)
- [„Benutzererstellung auf Monitor-Administratoren einschränken“ auf Seite 1180](#)
- [„Alarm-E-Mails anpassen“ auf Seite 1188](#)
- [„Monitor-Benutzer“ auf Seite 1175](#)
- [„Monitor-Benutzer bearbeiten“ auf Seite 1179](#)

## Zuordnen von Monitor-Benutzern zu einer Ressource

Sie müssen einen Monitor-Benutzer einer Ressource zuordnen, wenn der Benutzer E-Mail-Alarme für die jeweilige Ressource erhalten soll. Nur Monitor-Administratoren und -Operatoren können E-Mail-Alarme für Ressourcen erhalten.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

Vergewissern Sie sich, dass der Monitor so eingerichtet ist, dass Alarmbenachrichtigungen per E-Mail gesendet werden.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration** und anschließend auf **Benutzer**.
3. Wählen Sie einen Monitor-Administrator oder -Operator aus und vergewissern Sie sich, dass der Benutzer in seinem Benutzerkonto eine E-Mail-Adresse angegeben hat.
4. Klicken Sie auf **Einstellungen für die E-Mail-Alarmbenachrichtigung**.
5. Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um den Benutzer Ressourcen zuzuordnen. Wenn Sie fertig sind, klicken Sie auf **OK**.

### Ergebnisse

Der Benutzer erhält E-Mail-Alarme für die angegebenen Ressourcen.

**Siehe auch**

- „Senden von Alarm-E-Mails im Monitor aktivieren“ auf Seite 1189
- „Alarm-E-Mails anpassen“ auf Seite 1188

## Monitor-Benutzer bearbeiten

Alle Benutzer können ihre Benutzereinstellungen ändern, aber nur ein Monitor-Administrator kann den Typ eines Benutzers ändern.

**Voraussetzungen**

Sie müssen Monitor-Administrator sein.

**Aufgabe**

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Benutzer**.
4. Klicken Sie auf den zu bearbeitenden Benutzer und anschließend auf **Bearbeiten**.
5. Ändern Sie die Einstellungen für den Benutzer nach Bedarf.

Eine E-Mail-Adresse ist nur für Monitor-Administratoren und -Operatoren erforderlich, die E-Mail-Alarme vom Monitor erhalten sollen.

6. Klicken Sie auf **Speichern**.
7. Klicken Sie auf **Schließen**.

**Ergebnisse**

Der Monitor-Benutzer wird bearbeitet.

**Nächste Schritte**

Wenn Sie einen Monitor-Administrator oder Operator erstellt haben, können Sie den Benutzer Ressourcen zuordnen und er kann Alarmbenachrichtigungen per E-Mail empfangen.

**Siehe auch**

- „Zuordnen von Monitor-Benutzern zu einer Ressource“ auf Seite 1178
- „Alarm-E-Mails anpassen“ auf Seite 1188
- „Monitor-Benutzer erstellen“ auf Seite 1176
- „Löschen von Monitor-Benutzern“ auf Seite 1180

## Löschen von Monitor-Benutzern

Wenn Sie einen Benutzer löschen, wird der Benutzer aus dem Monitor entfernt und seine Zuordnungen zu Ressourcen werden aufgehoben.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration** und anschließend auf **Benutzer**.
3. Wählen Sie den Benutzer aus und klicken Sie dann auf **Löschen**.
4. Klicken Sie auf **Ja**, um den ausgewählten Benutzer zu löschen.
5. Klicken Sie auf **Schließen**.

### Ergebnisse

Der Benutzer wird aus dem Monitor gelöscht.

### Siehe auch

- „Monitor-Benutzer erstellen“ auf Seite 1176
- „Monitor-Benutzer bearbeiten“ auf Seite 1179

## Benutzererstellung auf Monitor-Administratoren einschränken

Standardmäßig kann jeder Benutzer einen eigenen Benutzernamen und ein eigenes Kennwort erstellen und hat dann schreibgeschützten Zugriff auf den Monitor. Sie können diese Funktion deaktivieren, sodass nur Monitor-Administratoren Benutzer erstellen können.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Konfiguration**.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **Optionen**.

6. Deaktivieren Sie die Option **Jeder hat schreibgeschützten Zugang zum SQL Anywhere-Monitor**.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Schließen**.

## Ergebnisse

Nur Monitor-Administratoren können Benutzer erstellen.

### Siehe auch

- [„Monitor-Benutzer erstellen“ auf Seite 1176](#)
- [„Monitor-Benutzer bearbeiten“ auf Seite 1179](#)

## Alarme

Ein **Alarm** ist eine Bedingung oder ein Zustand einer Ressource, auf die ein Monitor-Administrator oder -Operator aufmerksam gemacht werden muss. Alarme werden vom Monitor aufgrund von Metriken erkannt, die gesammelt werden. Sie werden nicht in der überwachten Ressource erkannt.

Es gibt vordefinierte Alarme für Bedingungen wie mangelnden Festplattenspeicher, fehlgeschlagene Loginversuche und hohe Speichernutzung. Sie können die Standardschwellenwerte ändern, indem Sie die Ressource bearbeiten.

Wenn eine Alarmbedingung gegeben ist, wird der Alarm im Widget **Alarmliste** für die angegebene Ressource angezeigt. Außerdem können Sie den Monitor so konfigurieren, dass er eine E-Mail an Monitor-Administratoren und -Operatoren sendet, wenn ein Alarm auftritt.

Standardmäßig erscheinen Alarme in den **Alarmliste**-Widgets. Sie umfassen Informationen über die Ursache des Problems sowie Tipps zu dessen Lösung. In der **Ressourcenliste** ändert sich der Status der Ressource, um das Vorhandensein und den Schweregrad des Alarms anzuzeigen.

Nur die letzten 50 Alarme jeder Ressource werden durch den Monitor gespeichert und im **Alarmliste**-Widget angezeigt. Ältere Alarme werden gelöscht.

### Siehe auch

- [„Angabe von Alarm-Schwellenwerten“ auf Seite 1184](#)
- [„Alarm-E-Mails anpassen“ auf Seite 1188](#)

## Alarme anzeigen

Jeder angemeldete Benutzer kann Alarme anzeigen, aber nur Monitor-Administratoren und -Operatoren können Alarme auflösen und löschen.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Kontext und Bemerkungen

Nur die letzten 50 Alarme jeder Ressource werden vom Monitor gespeichert und in der **Alarmliste** angezeigt.

### Aufgabe

1. Klicken Sie auf **Alarme » Heute**.
2. Klicken Sie in der Liste auf einen Alarm und anschließend auf **Details**.

### Ergebnisse

Die Details des Alarms werden in einem Fenster angezeigt.

### Nächste Schritte

Um die Details des Alarms zu schließen, klicken Sie auf **OK**.

### Siehe auch

- „Lösen von Alarmen“ auf Seite 1182
- „Löschen von Alarmen“ auf Seite 1183
- „Alarm-E-Mails anpassen“ auf Seite 1188

## Lösen von Alarmen

Sie können den Alarm als aufgelöst markieren, nachdem das Problem, das den Alarm ausgelöst hat, behoben wurde.

### Voraussetzungen

Sie müssen Monitor-Administrator oder -Operator sein.

### Kontext und Bemerkungen

Wenn ein Alarm aufgelöst wird, veranlasst dies den Monitor, den **Status** des Alarms in **Gelöst von *user-name*** zu ändern. Der Alarm bleibt jedoch in der Alarmliste. Wenn Sie den Alarm aus der Liste entfernen möchten, müssen Sie ihn löschen.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Übersicht**.
3. Klicken Sie im Widget **Alarmliste** in der Liste auf einen Alarm und klicken Sie dann auf **Gelöste markieren**, um den ausgewählten Alarm zu lösen.

## Ergebnisse

Der Wert in der Spalte **Status** ändert sich in **Gelöst von *your-user-name***.

Wenn dieser Alarm der einzige nicht aufgelöste Alarm der Ressource war, ändert sich der Status der Ressource im Widget **Ressourcenliste** in "Problemlos" (und es wird kein Symbol angezeigt).

### Siehe auch

- „Dashboards“ auf Seite 1124
- „Löschen von Alarmen“ auf Seite 1183
- „Alarm-E-Mails anpassen“ auf Seite 1188
- „Alarmer anzeigen“ auf Seite 1181
- „Alarmer“ auf Seite 1181

## Löschen von Alarmen

Sie können jeden Alarm aus einem Widget vom Typ **Alarmliste** löschen, unabhängig von seinem Status. Das Löschen von Alarmen aus dem Widget **Alarmliste** hat keine Auswirkungen auf Alarm-E-Mails.

### Voraussetzungen

Sie müssen Monitor-Administrator oder -Operator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Übersicht**.
3. Klicken Sie im Widget **Alarmliste** in der Liste auf einen Alarm und klicken Sie dann auf **Löschen**.
4. Das Fenster **Alarmer löschen** wird angezeigt und Sie werden aufgefordert, eine der folgenden Optionen auszuwählen:
  - **Ausgewählte Alarmer löschen** Wählen Sie diese Option, um nur die Alarmer zu löschen, die im Widget **Alarmliste** ausgewählt sind.
  - **Alarmer löschen, die empfangen wurden vor** Wählen Sie diese Option, um alle Alarmer zu löschen, die vor dem angegebenen Zeitpunkt empfangen wurden. Klicken Sie auf das Datum neben dieser Option und geben Sie das Datum ein, vor dem Alarmer gelöscht werden sollen. Diese Option löscht nur die Alarmer für die Ressourcen, die im **Alarmliste**-Widget enthalten sind.
  - **Alle Alarmer für die folgende Ressource löschen** Wählen Sie diese Option, um alle Alarmer für die ausgewählte Ressource zu löschen.

Klicken Sie auf **OK**.

5. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**, um das Löschen zu bestätigen.

### Ergebnisse

Der Alarm wird aus dem Widget **Alarmliste** gelöscht.

### Siehe auch

- „Lösen von Alarmen“ auf Seite 1182
- „Alarm-E-Mails anpassen“ auf Seite 1188
- „Alarmer anzeigen“ auf Seite 1181
- „Alarmer“ auf Seite 1181

## Angeben von Alarm-Schwellenwerten

Sie können konfigurieren, wann Alarmer ausgegeben werden sollen. Sie können jedoch weder festlegen, welche Metriken der Monitor sammelt, noch die Standardressource **SQL Anywhere-Monitor** konfigurieren.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

Wenn Sie die Alarm-Schwellenwerte für eine Datenbank der Version 16 konfigurieren möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle hat. Wenn Sie die Alarm-Schwellenwerte für eine Datenbank einer früheren Version konfigurieren möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die DBA-Berechtigung hat.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Ressourcen** und wählen Sie in der Liste eine Ressource aus.
4. Klicken Sie auf **Konfigurieren**.
5. Klicken Sie auf **Alarm-Schwellenwerte**. Bearbeiten Sie die Schwellenwerte.
6. Konfigurieren Sie erforderlichenfalls die anderen Einstellungen.
7. Klicken Sie auf **Speichern**.
8. Wenn Sie eine Datenbankressource bearbeiten, werden Sie zur Eingabe von Autorisierungsinformationen aufgefordert. Geben Sie bei Datenbanken der Version 16 die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank an, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle hat. Geben Sie bei Datenbanken früherer Versionen die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank an, der die DBA-Berechtigung hat.

9. Klicken Sie auf **Schließen**.

10. Klicken Sie auf **Schließen**.

### Ergebnisse

Der Monitor ist so konfiguriert, dass er bei den angegebenen Schwellenwerten Alarme sendet.

### Siehe auch

- [„Metriken“ auf Seite 1149](#)
- [„Alarm-Definitionen und -Schwellenwerte“ auf Seite 1186](#)

## Unterdrücken von Alarmen für nicht gesendete Fehlerberichte aus Ressourcen

Sie können festlegen, ob der Monitor Alarme sendet, wenn Ressourcen nicht eingesendete Fehlerberichte aufweisen. Standardmäßig sendet der Monitor diese Alarme nicht.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Konfiguration**.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **Optionen**.
6. Klicken Sie auf **Nicht weitergegebene Fehlerberichtsalarme aus den Ressourcen unterdrücken**.
7. Klicken Sie auf **Speichern**.
8. Klicken Sie auf **Schließen**.

### Ergebnisse

Der Monitor wird so konfiguriert, dass er Alarme sendet, wenn Ressourcen nicht eingesendete Fehlerberichte aufweisen.

### Siehe auch

- [„Fehlerbehandlung: Fehler in SQL Anywhere melden“ auf Seite 1108](#)

## Alarm-Definitionen und -Schwellenwerte

Als Monitor-Administrator können Sie die Schwellenwerte konfigurieren, die zum Auslösen von Alarmen verwendet werden.

Die folgende Liste beschreibt die Alarme und ihre Standard-Schwellenwerte.

Da jedes Synchronisationssystem ein anderes Verhalten und andere Integritätsregeln hat, können die Standardwerte für Ihre Umgebung ungeeignet sein. Sie sollten jeden Alarm-Schwellenwert überprüfen und nach Bedarf ändern.

### Alarm-Schwellenwerte für Datenbankressourcen

- **Alarm, wenn die CPU-Nutzung den angegebenen Schwellenwert länger als die angegebene Anzahl von Sekunden überschreitet**
  - **Schwellenwert (%)** Ein Alarm wird gemeldet, wenn die CPU-Nutzung der Ressource den angegebenen Prozentsatz erreicht. Standardwert ist 95 Prozent.
  - **Sekunden** Der Standardwert beträgt 30 Sekunden.
- **Alarm, wenn Speichernutzung über X% der maximalen Cachegröße ansteigt** Ein Alarm wird gemeldet, wenn die Speichernutzung der Ressource den angegebenen Prozentsatz erreicht. Standardwert ist 90 Prozent.
- **Alarm, wenn der freie Speicherplatz pro DBSpace geringer ist als X MB auf der Festplatte** Ein Alarm wird gemeldet, wenn der freie Festplattenspeicher pro DBSpace kleiner wird als der angegebene Wert. Standardwert ist 100 MB.
- **Alarm, wenn eine Verbindung länger als X Sekunden blockiert ist** Ein Alarm wird gemeldet, wenn eine Verbindung länger als die angegebene Zeit blockiert wird. Der Standardwert beträgt 10 Sekunden.
- **Alarm, wenn die Anzahl der benutzten Verbindungen X % des Lizenzlimits erreicht** Ein Alarm wird gemeldet, wenn die Anzahl von benutzten Verbindungen den angegebenen Prozentsatz des Lizenzlimits erreicht. Standardwert ist 85 Prozent.
- **Alarm, wenn eine Abfrage länger als X Sekunden läuft** Ein Alarm wird gemeldet, wenn eine Abfrage länger als die angegebene Zeit läuft. Der Standardwert beträgt 10 Sekunden.
- **Alarm, wenn die Anzahl der nicht geplanten Anforderungen folgenden Wert erreicht: X** Ein Alarm wird gemeldet, wenn die Anzahl der nicht geplanten Anforderungen den angegebenen Wert erreicht. Standardwert ist 5 Anforderungen.
- **Alarm, wenn mehr als die angegebene Anzahl von Tagen seit der letzten Sicherung vergangen sind** Ein Alarm wird ausgegeben, wenn die Anzahl der Tage seit der letzten serverseitigen Sicherung der Ressourcendatenbank die angegebene Anzahl von Tagen überschreitet. Standardwert ist 14 Tage.
- **Alarm, wenn die Anzahl der getrennten Scale-Out-Knoten den angegebenen Schwellenwert überschreitet** Ein Alarm wird gemeldet, wenn die Datenbank in einem Scale-Out-System mit

Schreibschutz oder einem Spiegelungssystem enthalten ist und das System den angegebenen Prozentsatz getrennter Knoten hat.

- **Alarme wegen derselben Ursache unterdrücken, wenn sie in folgenden Intervallen auftreten: X Minuten** Diese Option verhindert, dass Sie innerhalb einer bestimmten Periode mehrere identische Alarme erhalten. Standardwert ist 30 Minuten.

#### Alarm-Schwellenwerte für MobiLink-Serverressourcen

- **Alarm, wenn die CPU-Nutzung den angegebenen Schwellenwert länger als die angegebene Anzahl von Sekunden überschreitet** Der Standardwert für **Schwellenwert** ist 100 Prozent. Der Standardwert für **Sekunden** ist 300.
- **Alarm, wenn der Prozentsatz des benutzten Caches größer ist als (%):** Der Standardwert ist 100.
- **Alarm, wenn der Prozentsatz der gesperrten Cacheseiten größer ist als (%):** Der Standardwert ist 80.
- **Alarm, wenn die Anzahl der pro Sekunde aus- und eingelagerten Seiten den angegebenen Schwellenwert länger als die angegebene Anzahl von Sekunden überschreitet** Der Standardwert für den Schwellenwert ist 256. Der Standardwert für Sekunden ist 120.
- **Alarm, wenn die längste aktive Synchronisationszeit größer ist als (Sekunden):** Der Standardwert ist 600.
- **Alarm, wenn die Anzahl der fehlgeschlagenen Synchronisationen den angegebenen Schwellenwert länger als die angegebene Anzahl von Minuten überschreitet** Der Standardwert für den Schwellenwert der fehlgeschlagenen Synchronisationen ist 20. Der Standardwert für Minuten ist 60.
- **Alarm, wenn die Anzahl von Fehlern den angegebenen Schwellenwert länger als die angegebene Anzahl von Minuten überschreitet** Der Standardwert für den Schwellenwert (Fehleranzahl) ist 50. Der Standardwert für Minuten ist 60.
- **Alarm, wenn der freie Festplattenspeicher für den MobiLink-Cache geringer ist als (MB)** Der Standardwert ist 100.
- **Alarm, wenn die längste aktive Wartezeit für Datenbank-Worker-Thread länger ist als (Sekunden):** Standardwert ist 300.
- **Alarme wegen derselben Ursache unterdrücken, wenn sie in folgenden Intervallen auftritt: X Minuten** Diese Option verhindert, dass Sie innerhalb einer bestimmten Periode mehrere identische Alarme erhalten. Standardwert ist 30 Minuten.

#### Alarm-Schwellenwerte für Relay Server-Farm-Ressourcen

- **Alarm, wenn die CPU-Nutzung des Relay Servers den angegebenen Schwellenwert für die Anzahl von Sekunden überschreitet** Der Standardwert für **Schwellenwert** ist 80 Prozent. Der Standardwert für **Sekunden** ist 30.

- **Alarm, wenn eine Backend-Farm länger als die angegebene Anzahl von Sekunden nur partielle Konnektivität hat** Standardwert ist "30".
- **Alarm, wenn die Nutzung des gemeinsam genutzten Speichers durch den Relay Server den angegebenen Schwellenwert länger als die angegebene Anzahl von Sekunden überschreitet** Der Standardwert für **Schwellenwert** ist 80. Der Standardwert für **Sekunden** ist 30.
- **Alarm, wenn eine Backend-Farm länger als 2 Minuten nicht verfügbar ist** Diese Option ist standardmäßig deaktiviert.
- **Alarm, wenn ein schwerwiegender Fehler innerhalb der Relay Server-Farm auftritt** Diese Option ist standardmäßig ausgewählt.
- **Alarme wegen derselben Ursache unterdrücken, wenn sie in folgenden Intervallen auftritt: X Minuten** Diese Option verhindert, dass Sie innerhalb einer bestimmten Periode mehrere identische Alarme erhalten. Standardwert ist 30 Minuten.

**Siehe auch**

- [„Angaben von Alarm-Schwellenwerten“ auf Seite 1184](#)

## Alarm-E-Mails anpassen

Sie können den Monitor so konfigurieren, dass er eine E-Mail an angegebene Monitor-Administratoren und -Operatoren sendet, wenn ein Alarm für eine Ressource auftritt.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Vergewissern Sie sich, dass für den Monitor-Administrator oder -Operator eine E-Mail-Adresse konfiguriert wurde.
3. Ordnen Sie den Monitor-Administrator oder -Operator einer Ressource zu.
4. Aktivieren Sie im Monitor das Senden von E-Mails.

### Ergebnisse

Der Monitor wird so konfiguriert, dass er E-Mails sendet.

**Siehe auch**

- „Monitor-Benutzer erstellen“ auf Seite 1176
- „Monitor-Benutzer bearbeiten“ auf Seite 1179
- „Zuordnen von Monitor-Benutzern zu einer Ressource“ auf Seite 1178
- „Senden von Alarm-E-Mails im Monitor aktivieren“ auf Seite 1189

**Senden von Alarm-E-Mails im Monitor aktivieren**

Sie können den Monitor so konfigurieren, dass er E-Mails an Monitor-Administratoren und -Operatoren sendet, wenn Alarmer auftreten. Der Monitor unterstützt die Protokolle SMTP und MAPI für das Senden von E-Mails.

**Voraussetzungen**

Sie müssen Monitor-Administrator sein.

**Aufgabe**

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Extras » Administration**.
3. Klicken Sie auf **Konfiguration**.
4. Klicken Sie auf **Bearbeiten**.
5. Klicken Sie auf **Alarmkonfiguration**.
6. Klicken Sie auf **Alarmbenachrichtigung per E-Mail senden**.
7. Klicken Sie auf **SMTP** oder auf **MAPI** für das Feld **Welches Protokoll soll zum Senden der Alarmbenachrichtigungen per E-Mail verwendet werden?**.
8. Konfigurieren Sie erforderlichenfalls die anderen Einstellungen.
  - **MAPI**
    - **Benutzername** Geben Sie den Benutzernamen für den MAPI-Server ein.
    - **Kennwort** Geben Sie das Kennwort für den MAPI-Server ein.
  - **SMTP**
    - **Server** Geben Sie an, welcher SMTP-Server verwendet werden soll. Geben Sie den Servernamen oder die IP-Adresse für den SMTP-Server ein, z.B. *SMTP.yourcompany.com*.
    - **Port** Geben Sie die Portnummer für die Verbindung mit dem SMTP-Server ein. Standardwert ist "25".
    - **Name des Senders** Geben Sie einen Aliasnamen für die E-Mail-Adresse des Absenders ein, z.B. *JoeSmith*.
    - **Adresse des Senders** Geben Sie die E-Mail-Adresse des Absenders ein, z.B. *jsmith@emailaddress.com*.

- **Dieser SMTP-Server erfordert Authentifizierung** Wählen Sie diese Option, wenn Ihr SMTP-Server eine Authentifizierung erfordert.
  - **Benutzername** Geben Sie den Benutzernamen für SMTP-Server an, die eine Authentifizierung verlangen.
  - **Kennwort** Geben Sie das Kennwort für SMTP-Server an, die eine Authentifizierung verlangen.
- **Dieser SMTP-Server erfordert eine sichere Verbindung (TLS)** Wählen Sie diese Option, wenn Ihr SMTP-Server eine TLS-Verbindung erfordert.
  - **Vertrauenswürdige Zertifikat** Geben Sie den Pfad und den Dateinamen der Zertifikatsdatei ein, die der Monitor für die Authentifizierung im SMTP-Server verwendet.
  - **Zertifizierungsgesellschaft** Geben Sie den Namen der Zertifizierungsstelle oder der Organisation ein, die das Zertifikat erteilt hat. Der Wert des SMTP-Servers muss mit dem des Monitors übereinstimmen.
  - **Zertifizierungseinheit** Geben Sie die Zertifizierungseinheit ein. Sie wird auch als Organisationseinheit bezeichnet. Der Wert des SMTP-Servers muss mit dem des Monitors übereinstimmen.
  - **Zertifikatsname** Geben Sie den allgemeinen Namen des Zertifikats ein. Der Wert des SMTP-Servers muss mit dem des Monitors übereinstimmen.
- **Optionen für die Alarmkonfiguration**
  - **E-Mail-Benachrichtigungen nur für Alarme mit hoher Priorität senden** Wählen Sie diese Option aus, um nur dann E-Mail-Benachrichtigungen zu erhalten, wenn Alarme mit hoher Priorität ausgegeben werden. Alarme mit mittlerer und niedrigerer Priorität können weiterhin im **Alarmliste**-Widget angezeigt und gelöst werden.
  - **Nicht mehr als die angegebene Anzahl von E-Mail-Benachrichtigungen pro Tag senden** Wenn Sie diese Option auswählen, wird die Menge der E-Mail-Benachrichtigungen an einzelne Benutzer pro Tag beschränkt. Legen Sie die maximale Anzahl von Benachrichtigungen im Feld **E-Mail-Benachrichtigungen** fest. Standardwert ist 25.

Wenn der Benutzer die maximale Anzahl von Benachrichtigungen empfangen hat, wird eine E-Mail gesendet, die dem Benutzer mitteilt, wie die Grenze für Nachrichten eingestellt werden kann. Der Grenzwert wird automatisch um Mitternacht zurückgesetzt. Ab diesem Zeitpunkt erhält der Benutzer erneut die E-Mail-Benachrichtigungen. Der Benutzer kann den Grenzwert manuell zurücksetzen, indem er auf die Schaltfläche **Zählung der gesendeten E-Mail-Benachrichtigungen zurücksetzen** im Fenster **Alarmkonfiguration** klickt.

9. Klicken Sie auf **Test-E-Mail senden**.
10. Wenn Sie dazu aufgefordert werden, geben Sie eine E-Mail-Adresse ein, an die die Test-E-Mail gesendet werden soll, und klicken Sie auf **OK**.

Eine Test-E-Mail wird an die angegebene E-Mail-Adresse gesendet.

11. Klicken Sie auf **Speichern**.

12. Klicken Sie auf **Schließen**.

## Ergebnisse

Wenn ein Alarm auftritt, sendet der Monitor Alarm-E-Mails an Monitor-Administratoren und -Operatoren, die in ihren Benutzerkonten E-Mail-Adressen angegeben haben. Diese Benutzer erhalten E-Mails für die Ressourcen, denen sie zugeordnet sind.

### Siehe auch

- „Monitor-Benutzer erstellen“ auf Seite 1176
- „Zuordnen von Monitor-Benutzern zu einer Ressource“ auf Seite 1178
- „Lösen von Alarmen“ auf Seite 1182
- „Löschen von Alarmen“ auf Seite 1183
- „Alarme anzeigen“ auf Seite 1181
- „xp\_startsmtp-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Sichern des Monitors

Standardmäßig bereinigt der Monitor die Metriken automatisch einmal täglich um Mitternacht. Diese Bereinigung betrifft die Metriken, nicht die Alarme.

Als Monitor-Administrator können Sie Folgendes tun:

- Einen Zeitplan erstellen, nach dem der Monitor Metriken sichert.
- Steuern, wie lange Metriken aufbewahrt werden.
- Wartungsvorgänge bei Bedarf ausführen.

### Siehe auch

- „Einführung in die Zeitanzeige“ auf Seite 1131

## Metriken sichern

Sie können Metriken sichern und steuern, wie lange Metriken aufbewahrt werden.

### Voraussetzungen

Sie müssen Monitor-Administrator sein.

### Aufgabe

1. Melden Sie sich beim Monitor an.
2. Klicken Sie auf **Administration**.
3. Klicken Sie auf **Konfiguration** und anschließend auf **Bearbeiten**.

4. Klicken Sie auf **Wartung**.
5. Geben Sie eine Zeit (24-Stunden-Uhr) an, zu der der Monitor die Wartung durchführen soll. Standardmäßig wird die Wartung um Mitternacht durchgeführt. Es gilt die lokale Uhrzeit auf dem Computer, auf dem der Monitor läuft.
6. Geben Sie ein Verzeichnis an, in dem der Monitor die gesicherten Daten speichern soll. Das Verzeichnis muss sich auf dem Computer befinden, auf dem der Monitor läuft.
7. Passen Sie die Einstellungen für die **Datenreduktion** an:
  - **Metriken löschen, die älter sind als** Geben Sie eine Zeitspanne ein. Alle Metriken, die älter sind als die angegebene Zeitspanne, werden gelöscht. Der Standardwert beträgt fünf Tage.
8. Optional. Klicken Sie auf **Wartung jetzt durchführen**, um sofort die Sicherung auszuführen und veraltete Metriken zu löschen. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern**.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf **Abbrechen**.

### Ergebnisse

Der tägliche Zeitplan für die Sicherung und Löschung veralteter Metriken wird gespeichert.

## Sicherungskopien der Monitor-Datenbank wiederherstellen

Sie können die Monitor-Datenbank durch eine Sicherungskopie ersetzen.

### Voraussetzungen

Eine gültige Sicherungskopie der Monitor-Datenbank muss vorhanden sein.

### Aufgabe

1. Stoppen Sie den Monitor, falls er läuft.
2. Kopieren Sie aus Ihrem Sicherungsverzeichnis die Datenbankdatei *samonitor.db* und die Transaktionslogdatei *samonitor.log*.
3. Fügen Sie diese Dateien in das Verzeichnis ein, in dem die aktuelle Datenbank- und Transaktionslogdatei für den Monitor gespeichert sind. Wenn Sie dazu aufgefordert werden, überschreiben Sie die vorhandenen Dateien.

Die Standardspeicherorte für die Monitor-Datenbankdateien der Version 16.0 sind in der folgenden Tabelle aufgelistet:

Betriebssystem	Monitor-Verzeichnis
Windows XP (mit SQL Anywhere installiert)	C:\Documents and Settings\All Users\Documents\SQL Anywhere 16\Monitor\samonitor.db
Windows XP (auf einem separaten Computer installiert)	C:\Documents and Settings\All Users\Documents\SQL Anywhere 16 Monitor\samonitor.db
Windows Vista und höher (mit SQL Anywhere installiert)	C:\Users\Public\Documents\SQL Anywhere 16\Monitor\samonitor.db
Windows Vista und höher (auf einem separaten Computer installiert)	C:\Users\Public\Documents\SQL Anywhere 16 Monitor\samonitor.db
Linux (mit SQL Anywhere installiert)	/opt/sqlanywhere16/samonitor.db
Linux (auf einem separaten Computer installiert)	/opt/sqlanywhere16/samonitor.db

4. Starten Sie den Monitor neu.

## Ergebnisse

Die Datenbank wird aus einer Sicherung wiederhergestellt.

## Liste der vom Monitor installierten Datenbankobjekte

Die folgende Tabelle enthält eine Liste der Objekte, die installiert werden, wenn Sie eine Datenbank als zu überwachende Ressource hinzufügen.

Objektname	Objekttyp	Beschreibung
sa_monitor_user	Datenbankbenutzer	Dieser Benutzer ohne Schreibrechte wird der Datenbank hinzugefügt, um Metriken zu sammeln. Da dieser Benutzer zur überwachten Datenbank hinzugefügt wird, ist es nicht notwendig, die Anmeldeinformationen außerhalb der überwachten Datenbank zu speichern. Möglicherweise müssen Sie dem Benutzer "sa_monitor_user" erlauben, die Kennwortüberprüfung zu umgehen. Der Benutzer "sa_monitor_user" hat ein zufälliges Kennwort, das nur der Monitor kennt. Dieser Benutzer hat folgende Privilegien in der Datenbank: CREATE EXTERNAL REFERENCE, MONITOR, MANAGE ANY DBSPACE, BACKUP DATABASE.

Objektname	Objekttyp	Beschreibung
sa_monitor_connection_failure	Tabelle	Diese Tabelle enthält Metriken über fehlgeschlagene Verbindungsversuche und wird mit sa_monitor_connection_failed_event verwendet. Die Metriken dieser Tabelle werden gelöscht, wenn Metriken aus dem Monitor abgerufen werden.
sa_monitor_connection_failed_event	Ereignis	Dieses Ereignis wird beim Systemereignis ConnectFailed (jedes Mal, wenn ein Verbindungsversuch fehlschlägt) ausgelöst und fügt einen Datensatz in die Tabelle sa_monitor_connection_failure ein.
sa_monitor_count_unsubmitted_crash_reports	Funktion	Diese Funktion ruft die Prozedur xp_srvmon_count_unsubmitted_crash_reports auf, um die Anzahl der nicht gesendeten Absturzberichte zu ermitteln.

### Monitor-Objekte löschen

Da die Datenbankobjekte einem einzigen Eigentümer gehören, können Sie sie auf einmal löschen, indem Sie folgende Anweisung ausführen:

```
DROP USER sa_monitor_user;
```

### Überwachungsobjekte neu installieren

Weitere Hinweise zur erneuten Installation der Datenbankobjekte finden Sie unter [„Fehler in Datenbankressourcen beheben“ auf Seite 1147](#).

## Monitor Production Edition

Es wird empfohlen, insbesondere in Produktionsumgebungen, dass Sie:

1. Installieren Sie die Produktionsversion des Monitors (Production Edition) und führen Sie sie aus.

Das Ausführen der Produktionsversion des Monitors bietet folgende Vorteile:

- Der Monitor läuft im Hintergrund als Dienst.
- Der Monitor startet automatisch, wenn der Computer hochfährt.
- Upgrades und Aktualisierungen von SQL Anywhere überschreiben die Produktionsversion des Monitors nicht und haben keine Auswirkungen auf sie. Im Gegensatz dazu können Upgrades und Aktualisierungen von SQL Anywhere Auswirkungen auf die Monitor Developer Edition haben, da sie die Installation von SQL Anywhere auf dem Backend verwendet.

2. Installieren Sie den Monitor auf einem anderen Computer als demjenigen, auf dem die Ressourcen ausgeführt werden.

Das Ausführen des Monitors auf einem separaten Computer bietet z.B. folgende Vorteile:

- Die Auswirkungen auf den Datenbankserver, den MobiLink-Server, die Relay Server-Farm oder andere Anwendungen sind minimal.
- Die Überwachung ist nicht betroffen, wenn mit dem Computer, auf dem die Ressourcen installiert sind, etwas geschieht.

#### Siehe auch

- „Monitor-Benutzer“ auf Seite 1175

## Monitor Production Edition installieren (Windows)

Die Monitor Production Edition ist für die Verwendung in Deployments und Produktion vorgesehen. Sie wird getrennt installiert und als Dienst ausgeführt und enthält eine vollständig in sich geschlossene SQL Anywhere-Installation.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Führen Sie die Datei *setup.exe* im Verzeichnis *Monitor* Ihres Installationsdatenträgers aus und befolgen Sie die Anweisungen.

Unter Windows wird der Monitor-Dienst von der Installation gestartet.

2. Öffnen Sie die Standard-URL für das Anmelden beim Monitor: *http://localhost:4950*.

#### Hinweis

Wenn Sie über ein Netzwerk auf den Monitor zugreifen, navigieren Sie zu **http://computer-name:4950**, wobei *computer-name* der Name des Computers ist, auf dem der Monitor läuft. Siehe „Anmelden beim Monitor von einem entfernten Computer aus“ auf Seite 1122.

3. Melden Sie sich an.

Nach Aufforderung geben Sie Ihren Benutzernamen und Ihr Kennwort für den Monitor ein. Der Standardbenutzer ist ein Monitor-Administrator mit dem Namen **admin** und dem Kennwort **admin**.

### Ergebnisse

Die Monitor Production Edition wird installiert.

### Siehe auch

- „Architektur des Monitors“ auf Seite 1116
- „Monitor starten“ auf Seite 1120

## Monitor Production Edition installieren (Linux)

Die Monitor Production Edition ist für die Verwendung in Deployments und Produktion vorgesehen. Sie wird getrennt installiert und als Dienst ausgeführt und enthält eine vollständig in sich geschlossene SQL Anywhere-Installation.

### Voraussetzungen

Sie müssen der root-Benutzer sein.

### Aufgabe

1. Führen Sie als root-Benutzer die Datei *setup.tar* im Verzeichnis *Monitor* des Installationsdatenträgers aus und befolgen Sie die Anweisungen.

Unter Linux startet die Monitor Production Edition standardmäßig automatisch auch den Monitor-Dienst.

2. Öffnen Sie die Standard-URL für das Anmelden beim Monitor: *http://localhost:4950*.

#### Hinweis

Wenn Sie über ein Netzwerk auf den Monitor zugreifen, navigieren Sie zu **http://computer-name:4950**, wobei *computer-name* der Name des Computers ist, auf dem der Monitor läuft. Siehe „Anmelden beim Monitor von einem entfernten Computer aus“ auf Seite 1122.

3. Melden Sie sich an.

Nach Aufforderung geben Sie Ihren Benutzernamen und Ihr Kennwort für den Monitor ein. Der Standardbenutzer ist ein Monitor-Administrator mit dem Namen **admin** und dem Kennwort **admin**.

### Ergebnisse

Die Monitor Production Edition wird installiert.

### Nächste Schritte

Sie können den Monitor starten.

### Siehe auch

- „Architektur des Monitors“ auf Seite 1116

## Upgrade des Monitors durchführen sowie Ressourcen und Metriken migrieren

Siehe „Upgrade des SQL Anywhere-Monitors durchführen und Ressourcen migrieren“ [*SQL Anywhere 16 - Änderungen und Upgrades*].

## Sicherheit der Monitor-Kommunikation

Sie können die Kommunikation sowohl zwischen dem Monitor und Ihrem Browser als auch zwischen dem Monitor und den überwachten Ressourcen sichern.

### TLS-Sicherheit für den Monitor einrichten

Sie können die Transportschichtssicherheit (TLS) für die sichere Kommunikation zwischen dem Monitor und Ihrem Browser verwenden. Der Monitor führt einen Webserver aus, der HTTPS-Verbindungen mit SSL-Version 3.0 sowie TLS-Version 1.0 und 1.1 unterstützt.

#### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

#### Kontext und Bemerkungen

Weitere Hinweise finden Sie unter <http://www.sybase.com/detail?id=1063938>.

#### Aufgabe

1. Beziehen Sie digitale Zertifikate von einer Zertifizierungsstelle oder erstellen Sie mit dem Dienstprogramm zum Erstellen von Zertifikaten (createcert) selbstsignierte Zertifikate.
2. Ändern Sie die Monitor-Startzeilenzeichenfolge so, dass die Zertifikate verwendet werden.
3. Falls erforderlich, konfigurieren Sie Ihren Browser so, dass er Ihre neuen Zertifikate akzeptiert.

#### Ergebnisse

Die Kommunikation zwischen dem Monitor und Ihrem Browser wird gesichert.

#### Siehe auch

- „Dienstprogramm zum Erstellen von Zertifikaten (createcert)“ auf Seite 894

## Verbindungen zwischen dem Monitor und den Ressourcen sichern

Sie können für die Kommunikation zwischen dem Monitor und den von ihm überwachten Ressourcen FIPS-zertifizierte Verschlüsselung verwenden.

**Hinweis**

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [*SQL Anywhere 16 - Einführung*].

## Fehlerbehandlung für den Monitor

Zusätzlich zu den unten aufgelisteten Empfehlungen können Monitor-Administratoren mithilfe von Meldungslog und Ausnahmebedingungsberichten Fehler im Monitor beheben.

Problem	Empfehlung
Wenn Sie F5 drücken, um das Browserfenster zu aktualisieren, wird eine Anmeldung beim Monitor verlangt.	Aktivieren Sie JavaScript in Ihrem Browser.
Sie erhalten einen Netzwerkverbindungsfehler, wenn Sie sich beim Monitor anmelden wollen.	Starten Sie den Monitor. Siehe „ <a href="#">Monitor starten</a> “ auf Seite 1120.
Nach dem Upgrade auf die neueste Version des Adobe Flash Players erhalten Sie weiterhin Aufforderungen, ein Adobe Flash Player-Upgrade auszuführen.	Überprüfen Sie, ob die installierte Version des Adobe Flash Players von Ihrem Betriebssystem unterstützt wird. Der Monitor ist kompatibel mit Version 10 von Adobe Flash Player. Um die richtige Version zu ermitteln, besuchen Sie <a href="http://www.adobe.com/products/flashplayer/systemreqs/">http://www.adobe.com/products/flashplayer/systemreqs/</a> .
Der Monitor kann die Überwachung einer Datenbankressource nicht starten.	Überprüfen Sie, ob die Funktion für die Überprüfung des Kennworts und die Login-Prozeduren der Ressource dem Benutzer sa_monitor_user die Verbindung mit der Ressource gestatten.
Sie erhalten keine Alarm-E-Mails.	<p>Prüfen Sie, ob der Monitor richtig für den E-Mail-Versand konfiguriert ist, und senden Sie eine Test-E-Mail. Siehe „<a href="#">Senden von Alarm-E-Mails im Monitor aktivieren</a>“ auf Seite 1189.</p> <p>Prüfen Sie, ob die Alarm-E-Mails vom Monitor von einem Virus-Scanner blockiert werden. Siehe „<a href="#">xp_startsmtp-Systemprozedur</a>“ [<i>SQL Anywhere Server - SQL-Referenzhandbuch</i>].</p>

Problem	Empfehlung
<p>Die Anzahl der wartenden Anforderungen, die vom Monitor gemeldet werden, scheint geringer zu sein als die tatsächliche Anzahl der wartenden Anforderungen.</p>	<p>Wenn Sie Metriken über die Anzahl der wartenden Anforderungen sammeln, führt der Monitor eine Abfrage in der Ressource durch. Diese Abfrage könnte eine wartende Anforderung sein.</p> <p>Wartende Abfragen werden in der Reihenfolge ihres Eintreffens verarbeitet. Wenn daher wartende Anforderungen vorhanden sind und der Monitor versucht, seine Abfrage auszuführen, muss diese Abfrage warten, bis die bestehenden wartenden Anforderungen abgeschlossen sind.</p> <p>Wenn daher der Monitor die Anzahl der wartenden Anforderungen sammelt, enthält diese Anzahl nicht die wartenden Anforderungen, die zwischen dem Zeitpunkt des Absetzens der Abfrage durch den Monitor und deren Durchführung vorhanden waren.</p>
<p>Sie erhalten keine Alarme, wenn der Festplattenspeicher der Datenbank den angegebenen Schwellenwert überschreitet.</p>	<p>Zwischen zwei Monitor-Sammlungsintervallen kann eine Datenbank den angegebenen Schwellenwert für die Speicherplatzbelegung und die Menge des verfügbaren Speicherplatzes überschreiten. In diesem Fall antwortet die Datenbank nicht mehr, bevor der Monitor die Metriken über die Festplattennutzung sammeln und einen Alarm ausgeben kann.</p> <p>Wenn Ihre Datenbank rasch wächst, müssen Sie den Schwellenwert für die Speicherplatznutzung höher ansetzen, damit Sie einen Alarm erhalten können, bevor die Datenbank keinen Speicherplatz mehr hat. Siehe „<a href="#">Alarm-Definitionen und -Schwellenwerte</a>“ auf Seite 1186.</p>
<p>Sie können das Fenster <b>Administration</b> nicht sehen, wenn Sie beim Monitor angemeldet sind.</p>	<p>Sie müssen beim Monitor als Administrator angemeldet sein, um Zugriff auf das Fenster <b>Administration</b> zu haben. Siehe „<a href="#">Monitor-Benutzer</a>“ auf Seite 1175.</p>

Problem	Empfehlung
Sie haben den Monitor vor dem Migrieren Ihrer Ressourcen deinstalliert und nun sind Ihre Ressourcen verloren gegangen.	<p>Durch Deinstallieren des Monitors wird die Anwendung ebenso entfernt wie die Ressourcen und gesammelten Metriken. Bei einem Upgrade müssen Sie die neue Version des Monitors installieren, Ihre Ressourcen migrieren und dann die alte Version deinstallieren.</p> <p>Wenn Sie jedoch den Monitor regelmäßig gesichert haben, können Sie mit dem Migrator-Dienstprogramm die Daten aus den gesicherten Dateien in die neue Version des Monitors migrieren. Siehe <a href="#">„Sichern des Monitors“ auf Seite 1191</a> und <a href="#">„Upgrade des Monitors durchführen sowie Ressourcen und Metriken migrieren“ auf Seite 1197</a>.</p>

**Siehe auch**

- [„Anzeigen des Nachrichtenlogs“ auf Seite 1132](#)
- [„Ausnahmebedingungenberichte anzeigen“ auf Seite 1132](#)

## Praktische Einführung: Überwachen von Ressourcen mit dem Monitor

Verwenden Sie diese praktische Einführung, um die Überwachung einer Datenbank, eines MobiLink-Servers oder einer Relay Server-Farm einzurichten. In dieser praktischen Einführung wird die Monitor Developer Edition verwendet.

### Privilegien

Sie benötigen die Benutzer-ID und das Kennwort für einen Benutzer in der überwachten Datenbank, der das DROP CONNECTION-Systemprivileg hat.

Sie müssen beim Monitor als Administrator angemeldet sein, um die Lektionen dieser praktischen Einführung ausführen zu können. Benutzer ohne Schreibrechte und Operatoren können nur eine Teilmenge der Aufgaben ausführen, die ein Administrator ausführen kann. Wenn Sie Ihren Monitor-Benutzertyp überprüfen möchten, melden Sie sich beim Monitor an, klicken Sie auf

**Extras » Benutzereinstellungen** und überprüfen Sie die Einstellung **Benutzertyp**. Siehe [„Monitor-Benutzer“ auf Seite 1175](#).

Wenn Sie eine Datenbank der Version 16 hinzufügen möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle hat. Wenn Sie eine Datenbank vor Version 16.0 hinzufügen möchten, benötigen Sie die Benutzer-ID und das Kennwort für einen Benutzer in der Datenbank, der die DBA-Berechtigung hat. Diese Anmeldeinformationen werden für Folgendes verwendet:

- Herstellen einer Verbindung mit der Datenbank.

- Erstellen eines neuen Benutzers namens **sa\_monitor\_user**. Der Monitor verwendet den Benutzer "sa\_monitor\_user", um eine Verbindung mit der Datenbank herzustellen und sie zu überwachen.
- Installieren der Datenbankobjekte, die **sa\_monitor\_user** für die Überwachung der Datenbank benötigt.
- Verwerfen der angegebenen Anmeldeinformationen für die Benutzer-ID aus dem Monitor. Da der Benutzer "sa\_monitor\_user" zur überwachten Datenbank hinzugefügt wird, ist es nicht notwendig, die Anmeldeinformationen des Benutzers mit der SYS\_SAMONITOR\_ADMIN\_ROLE-Rolle bzw. der DBA-Berechtigung außerhalb der überwachten Datenbank zu speichern.

## Lektion 1: Beim Monitor anmelden

Melden Sie sich beim Monitor an, um Ressourcen hinzuzufügen und zu überwachen sowie Informationen über sie zu sammeln.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

### Aufgabe

1. Starten Sie den Monitor. Der Monitor darf nicht bereits im Hintergrund laufen.

**So starten Sie die Monitor Developer Edition (Windows)** Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » SQL Anywhere-Monitor**.

**So starten Sie Monitor Developer Edition (Linux)** Führen Sie das Skript *samonitor.sh* im Verzeichnis *bin32* oder *bin64* im Monitor-Installationsverzeichnis aus:

```
./samonitor.sh launch
```

Der Monitor beginnt mit dem Sammeln der Metriken und ein Browser öffnet die Standard-URL, über die Sie sich beim Monitor anmelden können: <http://localhost:4950>.

#### Hinweis

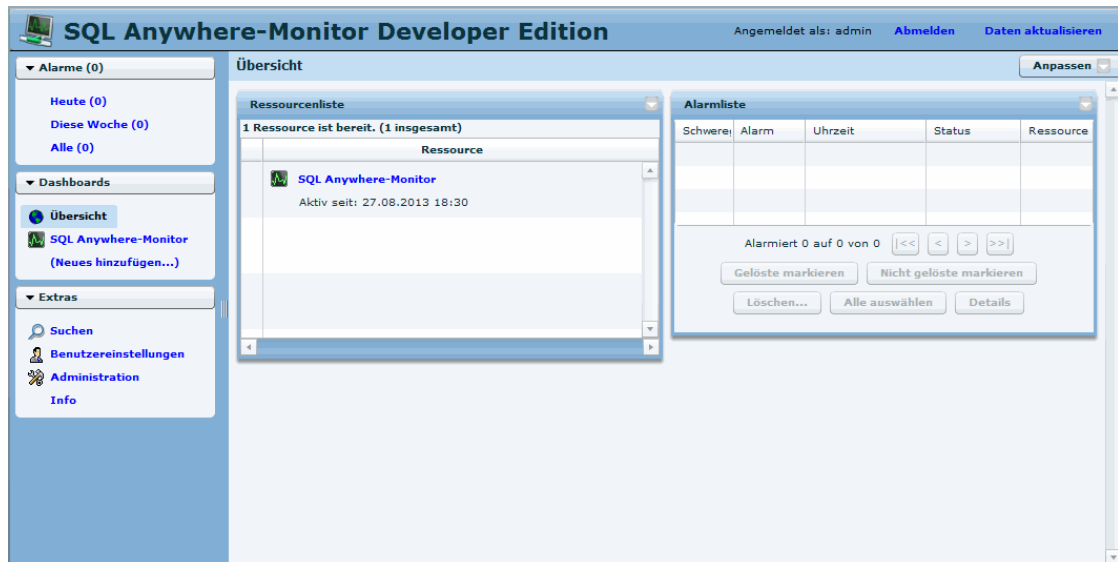
Wenn Sie über ein Netzwerk auf den Monitor zugreifen, navigieren Sie zu **<http://computer-name:4950>**, wobei *computer-name* der Name des Computers ist, auf dem der Monitor läuft.

2. Melden Sie sich beim Monitor als Standardadministrator an:
  - a. Im Feld **Benutzername** geben Sie **admin** ein.
  - b. Im Feld **Kennwort** geben Sie **admin** ein.
3. Standardmäßig öffnet der Monitor das Dashboard **Übersicht**, das die beiden folgenden Widgets enthält:

**Ressourcenliste** Dieses Widget enthält eine Liste der überwachten Ressourcen. Wenn Sie den Monitor erstmals öffnen, überwacht dieser sich lediglich selbst, über die Standardressource mit dem

Namen **SQL Anywhere-Monitor**. Sie können diese Ressource nicht ändern und diese Überwachung nicht stoppen.

**Alarmliste** Dieses Widget enthält eine Liste der Alarme von den überwachten Ressourcen.



### Ergebnisse

Sie haben sich beim Monitor als Administrator angemeldet.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 2: Ressourcen hinzufügen](#)“ auf Seite 1202.

### Siehe auch

- „[Monitor starten](#)“ auf Seite 1120

## Lektion 2: Ressourcen hinzufügen

In dieser Lektion fügen Sie die SQL Anywhere-Beispieldatenbank als zu überwachende Ressource hinzu.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beim Monitor anmelden](#)“ auf Seite 1201.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

## Aufgabe

1. Starten Sie die Ressource, die Sie überwachen möchten. Wenn Sie etwa die Beispieldatenbank starten möchten, klicken Sie auf **Start » Programme » SQL Anywhere 16 » SQL Anywhere » Netzwerkserver-Beispiel**.
2. Klicken Sie im Monitor auf **Extras » Administration**.
3. Klicken Sie auf **Ressourcen** und anschließend auf **Hinzufügen**.
4. Wählen Sie eine der folgenden Optionen:

### Datenbankressource hinzufügen

- a. Klicken Sie auf **SQL Anywhere Server** und anschließend auf **Weiter**.
- b. Im Feld **Name** geben Sie **demo16** ein und klicken dann auf **Weiter**.
- c. Im Feld **Host** geben Sie **localhost** und im Feld **Server** geben Sie **demo16** ein.
- d. Klicken Sie auf **Erstellen**.
- e. Wenn Sie nach der erforderlichen Autorisierung gefragt werden, geben Sie im Feld **Benutzer-ID** den Wert **DBA** ein und im Feld **Kennwort** den Wert **sql**. Klicken Sie auf **OK**.

Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch.

5. Klicken Sie zweimal auf **Schließen**.
6. Klicken Sie auf **Dashboards » Übersicht**.  
  
Die Ressource erscheint in der **Ressourcenliste**.
7. Klicken Sie auf die Ressource, um das Dashboard zu öffnen und die gesammelten Metriken anzuzeigen.

## Ergebnisse

Die Ressource wird hinzugefügt und überwacht.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: \(Optional\) Alarm-E-Mails einrichten](#)“ auf Seite 1203.

## Siehe auch

- „Datenbankressourcen hinzufügen“ auf Seite 1133
- „MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135
- „Liste der vom Monitor installierten Datenbankobjekte“ auf Seite 1193
- „Host-Verbindungsparameter“ auf Seite 363

## Lektion 3: (Optional) Alarm-E-Mails einrichten

Richten Sie den Monitor so ein, dass er Ihnen eine E-Mail sendet, wenn ein Alarm auftritt.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beim Monitor anmelden](#)“ auf Seite 1201.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

Wenden Sie sich an Ihren Systemadministrator, wenn Sie Informationen zu Ihrem E-Mail-Protokoll benötigen. Gehen Sie weiter zur nächsten Lektion, wenn Sie Ihr E-Mail-Protokoll nicht kennen.

## Aufgabe

1. Fügen Sie eine E-Mail-Adresse zu Ihrem Benutzerkonto hinzu.
  - a. Klicken Sie auf **Extras » Administration**.
  - b. Klicken Sie auf **Benutzer** und wählen Sie Ihre Benutzer-ID aus.
  - c. Klicken Sie auf **Bearbeiten**. Im Feld **E-Mail** geben Sie eine gültige E-Mail-Adresse ein.
  - d. Klicken Sie auf **Speichern**. Schließen Sie nicht das Fenster **Administration**.
2. Wählen Sie die Ressourcen aus, für die Sie Alarm-E-Mails erhalten möchten.
  - a. Klicken Sie auf der Registerkarte **Benutzer** auf **Einstellungen für die E-Mail-Alarmbenachrichtigung**.
  - b. Verwenden Sie die Schaltflächen **Hinzufügen** und **Entfernen**, um die Ressourcen auszuwählen, an denen Sie interessiert sind.
  - c. Klicken Sie auf **OK**. Schließen Sie nicht das Fenster **Administration**.
3. Konfigurieren Sie die E-Mail-Alarmbenachrichtigung.
  - a. Klicken Sie auf **Konfiguration** und anschließend auf **Bearbeiten**.
  - b. Klicken Sie auf der Registerkarte **Alarmkonfiguration** auf **Alarmbenachrichtigung per E-Mail senden**.
  - c. Geben Sie das E-Mail-Protokoll an.

Wenn Sie SMTP angeben, müssen Sie E-Mail-Server und Port eingeben und angeben, ob eine Authentifizierung erforderlich ist. Achten Sie beim Angeben von Name und Adresse des Absenders darauf, dass der Absendername ein eindeutiger Bezeichner ist.

Wenn Sie MAPI angeben, müssen Sie eine Benutzer-ID und ein Kennwort eingeben.
  - d. Klicken Sie auf **Test-E-Mail senden**, um zu testen, ob Sie die E-Mail-Benachrichtigung richtig konfiguriert haben.
  - e. Wenn Sie dazu aufgefordert werden, geben Sie eine E-Mail-Adresse ein, an die die Test-E-Mail gesendet werden soll, und klicken Sie auf **OK**.

Eine Test-E-Mail wird an die angegebene E-Mail-Adresse gesendet.
  - f. Klicken Sie auf **Speichern** und anschließend auf **Schließen**.

## Ergebnisse

Wenn ein Alarm auftritt, wird eine E-Mail mit Informationen über den Alarm an die angegebene E-Mail-Adresse gesendet.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 4: Alarme testen“ auf Seite 1205](#).

## Siehe auch

- [„Senden von Alarm-E-Mails im Monitor aktivieren“ auf Seite 1189](#)
- [„Monitor-Benutzer“ auf Seite 1175](#).

# Lektion 4: Alarme testen

In dieser Lektion lösen Sie absichtlich einen Alarm aus, um die Verarbeitung von Alarmen zu üben.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Beim Monitor anmelden“ auf Seite 1201](#).

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Überwachen von Ressourcen mit dem Monitor“](#).

## Aufgabe

1. Lösen Sie einen Alarm aus, indem Sie den Datenbankserver herunterfahren.

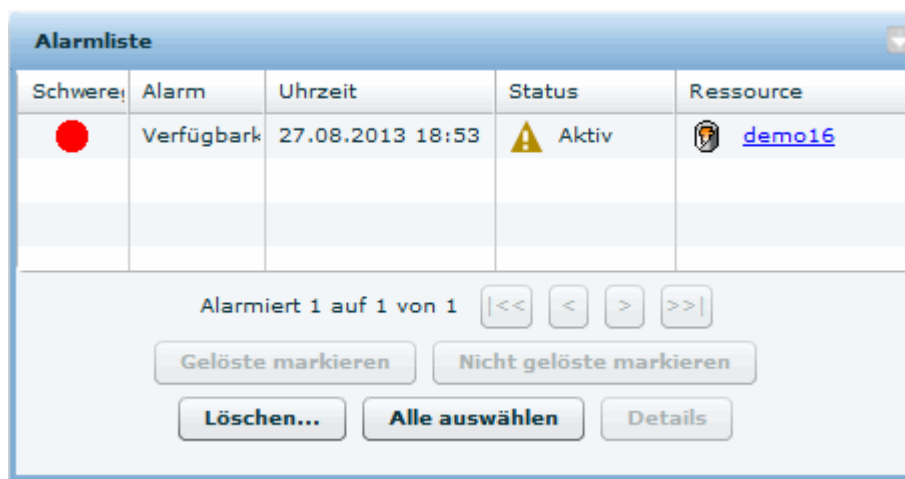
Unter Windows können Sie beispielsweise den Datenbankserver herunterfahren, indem Sie in der Taskleiste auf das Symbol des Netzwerkserver klicken und anschließend im Meldungsfenster des Datenbankserver auf **Herunterfahren**.

2. Klicken Sie im Monitor auf **Dashboards » Übersicht**.

In der **Ressourcenliste** erscheint neben der Ressource ein roter Kreis mit einem weißen X, um anzuzeigen, dass die Ressource nicht verfügbar ist.






Im Widget **Alarmliste** erscheint eine **Verfügbarkeitswarnung** für eine Datenbank, der Alarm **Server ausgefallen** für einen MobiLink-Server bzw. der Alarm **Fortwährender Ausfall des Relay Servers** für eine Relay Server-Farm mit dem Status **Aktiv**.



Es kann ein paar Sekunden dauern, bis diese Änderungen im Zustand und im Überwachungsstatus angezeigt werden. Standardmäßig sammelt der Monitor alle 30 Sekunden Ressourcen-Informationen.




3. Wählen Sie im Widget **Alarmliste** den Alarm aus und klicken Sie dann auf **Details**, um die Beschreibung zu lesen.
4. Klicken Sie auf **OK**, um den Alarm zu schließen.
5. Starten Sie die Ressource neu. Starten Sie beispielsweise die Beispieldatenbank neu, indem Sie auf **Start » Programme » SQL Anywhere 16 » SQL Anywhere » Netzwerkserver-Beispiel** klicken.

Im Widget **Ressourcenliste** ändert sich der **Status** für die Ressource in ein gelbes Dreieck. Dieses Symbol zeigt an, dass die Ressource überwacht wird und ein Alarm vorliegt. In der **Alarmliste** ändert sich der **Status** des Alarms in **Inaktiv**. Ein inaktiver Alarm bedeutet, dass zwar das Problem, durch das der Alarm ausgelöst wurde, nicht mehr besteht, aber der Alarm nicht aufgelöst oder gelöscht wurde.

Übersicht				
Alarmliste				
Schwere	Alarm	Uhrzeit	Status	Ressource
	Verfügbarkeitswarnung	28.08.2013 11:24	 Inaktiv	 <a href="#">demo16</a>

6. Lösen Sie den Alarm auf, indem Sie ihn auswählen und auf **Gelöste markieren** klicken.

Nun werden in der **Ressourcenliste** keine Symbole neben der Ressource angezeigt, was bedeutet, dass die Ressource überwacht wird und keine Alarme hat. Im Widget **Alarmliste** ändert sich der **Status** des Alarms in **Gelöst von admin**, wobei *admin* Ihr Monitor-Benutzername ist.

Übersicht				
Alarmliste				
Schwere	Alarm	Uhrzeit	Status	Ressource
	Verfügbarkeitswarnung	27.08.2013 18:53	 Gelöst ...	 <a href="#">demo16</a>

Alarmiert 1 auf 1 von 1 |<< < > >>| Gelöste markieren Nicht gelöste markieren Löschen... Alle auswählen Details

7. Löschen Sie den Alarm.
- Klicken Sie auf den Alarm und anschließend auf **Löschen**.
  - Klicken Sie auf **Ausgewählte Alarme löschen** und anschließend auf **OK**.
  - Wenn Sie dazu aufgefordert werden, klicken Sie auf **Ja**, um das Löschen zu bestätigen.

## Ergebnisse

Sie haben einen Alarm ausgelöst, aufgelöst und gelöscht.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 5: Neue Dashboards und Widgets hinzufügen](#)“ auf Seite 1208.

## Siehe auch

- „[Metriken](#)“ auf Seite 1149
- „[Monitor-Benutzer](#)“ auf Seite 1175.

# Lektion 5: Neue Dashboards und Widgets hinzufügen

Fügen Sie ein Dashboard und Widgets zum Monitor hinzu, um Informationen über Ressourcen anzuzeigen.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beim Monitor anmelden](#)“ auf Seite 1201.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

## Kontext und Bemerkungen

Dashboards sind benutzerspezifisch. Jeder Benutzer kann die in seinen Dashboards vorhandenen Widgets hinzufügen, bearbeiten oder löschen.

## Aufgabe

1. Klicken Sie auf **Dashboards » Neues hinzufügen**.
  - a. Klicken Sie auf **Ein Dashboard zur Überwachung der folgenden Ressource** und wählen Sie die Ressource.
  - b. Im Feld **Dashboard-Name** geben Sie **Benutzer\_Hans** ein.
  - c. Geben Sie im Feld **Anzahl von Spalten** den Wert **2** ein.
  - d. Klicken Sie auf **OK**.

Ein neues Dashboard wird angezeigt, mit den folgenden Widgets:

**Für Datenbanken** Alarmliste, Wichtigste Performance-Metriken, Serverinformationen und Verbindungen.

**Für MobiLink** Alarmliste, Wichtigste Performance-Metriken, Serverinformationen und Verbindungen.

**Für Relay Server** Alarmliste und Wichtigste Performance-Metriken.

2. Fügen Sie ein Metriken-Widget hinzu, um statt der Standard-Sparklines Diagramme anzuzeigen.

- a. Klicken Sie in der oberen rechten Ecke des Dashboards **user\_joe** auf **Anpassen » Widget hinzufügen**.
- b. Klicken Sie auf **Metriken** und anschließend auf **Weiter**.
- c. Im Feld **Wie möchten Sie dieses Widget nennen?** geben Sie **Metrics display** ein.
- d. Im Feld **Welche Ressource interessiert Sie?** klicken Sie auf **demo16** für einen Datenbankserver, **MobiLinkServerSample** für einen MobiLink-Server bzw. die Relay Server-Farmressource für Relay Server.
- e. Im Feld **Welche Art von Anzeige möchten Sie?** klicken Sie auf **Diagramm**.
- f. Unter **Welche Metriken möchten Sie anzeigen?** klicken Sie auf eine der folgenden Optionen:

**Für Datenbanken** CPU-Nutzung, Verarbeitete Abfragen und Speichermetriken » Cachegröße.

**Für MobiLink** Synchronisationsmetriken

**Für Relay Server** CPU-Nutzung

- g. Klicken Sie auf **Erstellen**.

Ein Widget mit dem Namen **Metrics display** erscheint im Dashboard.

Um die Größe eines Widgets zu maximieren, klicken Sie im Widget-Fensterausschnitt auf den Pfeil am Dropdown-Menü und anschließend auf **Maximieren**.

Um Details im Diagramm anzuzeigen, positionieren Sie den Cursor über bestimmten Punkten.

## Ergebnisse

Sie haben ein Dashboard und ein Metriken-Widget für Ihre Ressource erstellt.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 6: Datenbankverbindungen schließen](#)“ auf Seite 1209.

## Siehe auch

- „[Dashboards verwalten](#)“ auf Seite 1126
- „[Widgets](#)“ auf Seite 1127

# Lektion 6: Datenbankverbindungen schließen

Schließen Sie eine Verbindung mit einer Datenbank.

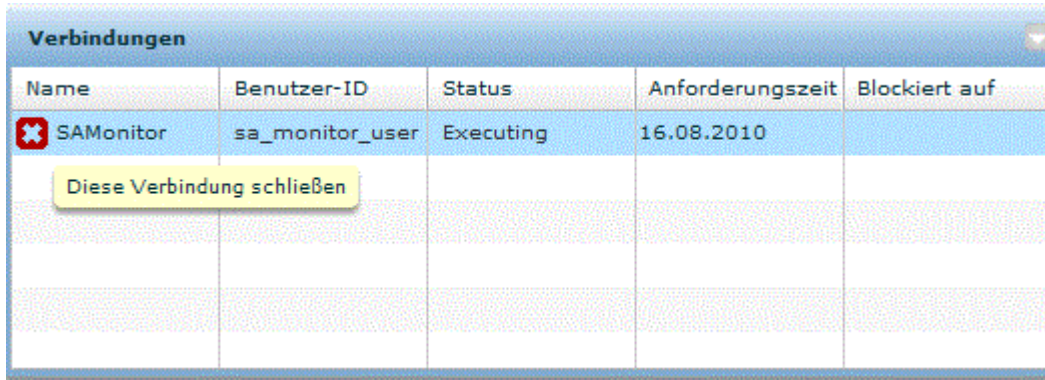
## Voraussetzungen


In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beim Monitor anmelden](#)“ auf Seite 1201.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Überwachen von Ressourcen mit dem Monitor“](#).

### Aufgabe

1. Öffnen Sie das **demo16**-Dashboard.
2. Klicken Sie im Widget **Connections** auf das **x** neben dem Namen der zu schließenden Verbindung.



Name	Benutzer-ID	Status	Anforderungszeit	Blockiert auf
 SAMonitor	sa_monitor_user	Executing	16.08.2010	
Diese Verbindung schließen				

3. Wenn Sie nach der erforderlichen Autorisierung gefragt werden, geben Sie im Feld **Benutzer-ID** den Wert **DBA** ein und im Feld **Kennwort** den Wert **sql**.

Der Monitor verwendet die Benutzer-ID und das Kennwort, um sich mit der Ressourcendatenbank zu verbinden und die Verbindung zu löschen. Diese Benutzer-ID muss das DROP CONNECTION-Systemprivileg haben. Die Benutzer-ID und das Kennwort werden nicht vom Monitor gespeichert.

4. Klicken Sie auf **OK**.

Die Verbindung wird aus dem Widget **Connections** entfernt.

### Ergebnisse

Die Verbindung wird geschlossen.

### Nächste Schritte

Gehen Sie weiter zu [„Lektion 7: Überwachung von Ressourcen stoppen“](#) auf Seite 1210.

## Lektion 7: Überwachung von Ressourcen stoppen

In dieser Lektion entfernen Sie die überwachte Ressource, wodurch die gesammelten Metriken gelöscht werden und das Sammeln der Daten gestoppt wird. Wenn Sie in einer Produktionsumgebung die Überwachung der Ressource fortsetzen möchten, lassen Sie einfach die Datenbank, den MobiLink-Server oder die Relay Server-Farm sowie den Monitor weiterlaufen.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Beim Monitor anmelden](#)“ auf Seite 1201.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

## Kontext und Bemerkungen

Sie können die Ressource **SQL Anywhere-Monitor** nicht löschen.

### Hinweis

Wenn Sie eine Datenbankressource entfernen, löscht der Monitor *nicht* die in der Datenbank installierten Überwachungsobjekte. Um diese Objekte zu löschen, müssen Sie sich als Benutzer mit **MANAGE ANY USER**-Systemprivileg mit der Datenbank verbinden und die folgende Anweisung ausführen:

```
DROP USER sa_monitor_user;
```

## Aufgabe

1. Entfernen Sie die Ressourcen, die Sie im Rahmen dieser praktischen Einführung hinzugefügt haben.
  - a. Klicken Sie auf **Extras » Administration**.
  - b. Klicken Sie auf **Ressourcen**.
  - c. Wählen Sie die Ressource **demo16**, die Ressource **MobiLinkServerSample** bzw. die Relay Server-Farmressource aus und klicken Sie auf **Stopp**.
  - d. Klicken Sie auf **Entfernen**.
  - e. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie die Ressource entfernen wollen.
  - f. Klicken Sie auf **Schließen**.
2. Klicken Sie auf **Abmelden**, um sich vom Monitor abzumelden, und schließen Sie das Browserfenster, in dem der Monitor angezeigt wird.
3. Fahren Sie den Monitor herunter und stoppen Sie die Überwachung.
  - Unter Windows rechtsklicken Sie in der Taskleiste auf das Monitor-Symbol und klicken auf **SQL Anywhere-Monitor beenden**.
  - Unter Linux: Führen Sie das Skript `samonitor.sh` im Verzeichnis `bin32` oder `bin64` im Monitor-Installationsverzeichnis aus:

```
./samonitor.sh stop
```

Der Monitor beendet das Erfassen von Metriken für alle Ressourcen.

4. Fahren Sie die Ressource herunter, die überwacht wurde. Wenn Sie beispielsweise die Datenbank herunterfahren möchten, doppelklicken Sie in der Taskleiste für den Datenbankserver auf das Symbol

des Netzwerkserver, klicken Sie im Meldungsfenster des Datenbankserver auf **Herunterfahren** und klicken Sie auf **Ja**, um die Aktion zu bestätigen.

### Ergebnisse

Der SQL Anywhere-Monitor wird heruntergefahren und beendet die Überwachung der Ressource, die ebenfalls heruntergefahren wird.

### Siehe auch

- [Monitor-Objekte löschen auf Seite 1194](#)
- [„Monitor-Benutzer“ auf Seite 1175](#)

## Lektion 8: Datenbankspiegelungssysteme überwachen

Verwenden Sie den Monitor zum Überwachen eines Datenbankspiegelungssystems.

### Voraussetzungen

In dieser praktischen Einführung wird davon ausgegangen, dass ein laufendes Scale-Out-System mit Schreibschutz vorhanden ist, wie unter [„Praktische Einführung: Datenbankspiegelungssysteme erstellen“](#) beschrieben.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Überwachen von Ressourcen mit dem Monitor“](#).

### Aufgabe

1. Fügen Sie ein Datenbankspiegelungssystem zur **Ressourcenliste** des Monitors hinzu.
  - a. Klicken Sie in der Seitenleiste **Extras** auf **Administration**.
  - b. Klicken Sie auf **Ressourcen** und klicken Sie dann auf **Hinzufügen**.
  - c. Klicken Sie auf **SQL Anywhere Server** und anschließend auf **Weiter**.
  - d. Im Feld **Name** geben Sie **mirror\_demo** ein und klicken dann auf **Weiter**.
  - e. Geben Sie im Feld **Host** die Hostnamen und Portnummern der Computer, auf denen Primär- und Spiegelservers ausgeführt werden, in eine kommasetrennte Liste ein. Geben Sie also z. B. **localhost:6871, localhost:6872** ein.
  - f. Geben Sie im Feld **Servername** den alternativen Namen für den Primärserver ein. Geben Sie also z. B. **mirror\_demo\_primary** ein.
  - g. Klicken Sie auf **Erstellen**.
  - h. Wenn Sie nach der erforderlichen Autorisierung gefragt werden, geben Sie **DBA** in das Feld **Benutzer-ID** ein und **sql** in das Feld **Kennwort**. Klicken Sie auf **OK**.  
Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch.
  - i. Klicken Sie zweimal auf **Schließen**.

2. Fügen Sie ein Widget für die Überwachung von *scaleoutdemo.db* hinzu:
  - a. Klicken Sie in der Seitenleiste **Dashboard** auf **mirror\_demo**.
  - b. Klicken Sie in der oberen rechten Ecke des mirrorsystemdemo-Dashboards auf **Anpassen » Widget hinzufügen**.
  - c. Wählen Sie die Option **Topologie des SQL Anywhere-Scale-Out** aus und klicken Sie auf **Weiter**.
  - d. Im Feld **Wie möchten Sie dieses Widget nennen?** geben Sie **mirror\_demowidget** ein.
  - e. Im Feld **Welche Ressource interessiert Sie?** wählen Sie **mirror\_demo** aus.
  - f. Klicken Sie auf **Erstellen**.

Das neue Widget erscheint im Dashboard:

Servename	Typ	Status	Verbindungen	Zuletzt aktualisiert
mirror_server1	partner - primary	connected	1	17.03.2011 12:56
mirror_server2	partner - mirror	connected	0	17.03.2011 12:56
demo_arbiter	arbiter	connected		

- **Servename** Zeigt die Namen der Datenbankserver im Spiegelungssystem an.
- **Typ** Zeigt den Servertyp und einen der folgenden Werte an:
  - Partner - Primärserver** Dieser Wert kennzeichnet den Server, der derzeit als Primärserver agiert.
  - Partner - Spiegelserver** Dieser Wert kennzeichnet den Server, der derzeit als Spiegelserver agiert.
  - Arbiter** Dieser Wert kennzeichnet den Arbiterserver.
- **Status** Dieser Wert zeigt den Verbindungsstatus der einzelnen Server an.
- **Verbindungen** Dieser Wert zeigt die Anzahl der aktuellen Verbindungen mit dem Server an.
- **Zuletzt aktualisiert** Dieser Wert zeigt an, wann der Serverstatus zuletzt aktualisiert wurde.

## Ergebnisse

Eine Datenbankspiegelungssystem-Ressource wird hinzugefügt und überwacht.

## Siehe auch

- „SQL Anywhere-Monitor“ auf Seite 1115
- „Datenbankressourcen hinzufügen“ auf Seite 1133
- „MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135
- „Dashboards“ auf Seite 1124
- „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129
- „Widgets“ auf Seite 1127

## Lektion 9: (Optional) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen

Starten Sie eine SQL Anywhere-Datenbank, die der Stammknoten in einem Scale-Out-System mit Schreibschutz ist, und fügen Sie diese Datenbank als vom SQL Anywhere-Monitor zu überwachende Ressource hinzu.

### Voraussetzungen

In dieser praktischen Einführung wird davon ausgegangen, dass ein laufendes Scale-Out-System mit Schreibschutz vorhanden ist, wie unter „[Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen](#)“ beschrieben.

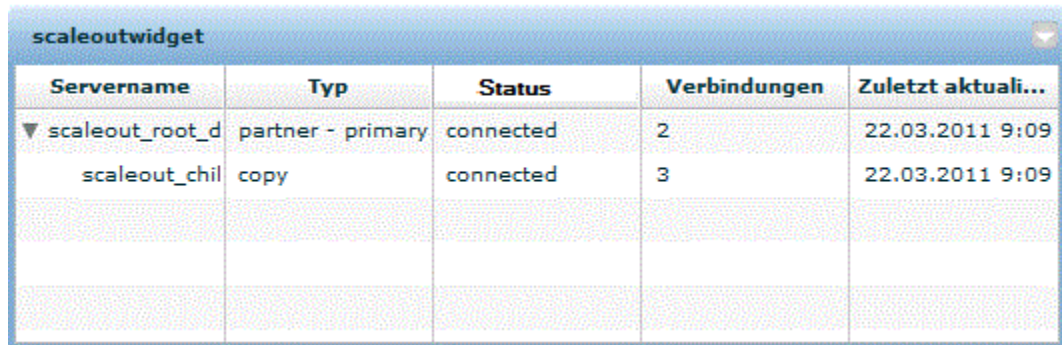
In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Überwachen von Ressourcen mit dem Monitor](#)“.

### Aufgabe

1. Starten Sie den SQL Anywhere-Monitor. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » SQL Anywhere-Monitor**.
2. Melden Sie sich beim Monitor als Standardadministrator an:
  - a. Im Feld **Benutzername** geben Sie **admin** ein.
  - b. Im Feld **Kennwort** geben Sie **admin** ein.
3. Fügen Sie *scaleoutdemo.db* als Ressource zum Monitor hinzu:
  - a. Klicken Sie in der Seitenleiste **Extras** auf **Administration**.
  - b. Klicken Sie auf **Ressourcen** und klicken Sie dann auf **Hinzufügen**.
  - c. Klicken Sie auf **SQL Anywhere Server** und anschließend auf **Weiter**.
  - d. Im Feld **Name** geben Sie **scaleoutdemo** ein und klicken dann auf **Weiter**.
  - e. Im Feld **Host** geben Sie **localhost** ein.
  - f. Im Feld **Server** geben Sie **scaleout\_root\_demo** ein.
  - g. Klicken Sie auf **Erstellen**.
  - h. Wenn Sie nach der erforderlichen Autorisierung gefragt werden, geben Sie **DBA** in das Feld **Benutzer-ID** ein und **sql** in das Feld **Kennwort**. Klicken Sie auf **OK**.  
Die Ressource wird hinzugefügt und die Überwachung der Ressource beginnt automatisch.
  - i. Klicken Sie zweimal auf **Schließen**.
4. Fügen Sie ein Widget für die Überwachung von *scaleoutdemo.db* hinzu:
  - a. Klicken Sie in der Seitenleiste **Dashboard** auf **scaleoutdemo**.
  - b. Klicken Sie in der oberen rechten Ecke des scaleoutdemo-Dashboards auf **Anpassen » Widget hinzufügen**.

- c. Wählen Sie die Option **Topologie des SQL Anywhere-Scale-Out** aus und klicken Sie auf **Weiter**.
- d. Im Feld **Wie möchten Sie dieses Widget nennen?** geben Sie **scaleoutwidget** ein.
- e. Im Feld **Welche Ressource interessiert Sie?** klicken Sie auf **scaleoutdemo**.
- f. Klicken Sie auf **Erstellen**.

Das neue Widget erscheint im Dashboard:



Servername	Typ	Status	Verbindungen	Zuletzt aktuali...
▼ scaleout_root_d	partner - primary	connected	2	22.03.2011 9:09
scaleout_chil	copy	connected	3	22.03.2011 9:09

Das Topologie-Widget zeigt die folgenden Spalten und ihre möglichen Werte:

- **Servername** Der Name des Knotens im Scale-Out-System.
- **Typ** Die Rolle des Datenbankservers. Der Typ ist entweder **Partner - Primärserver** oder **Kopie**, abhängig davon, wie der Server definiert wurde, als das Scale-Out-System mit Schreibschutz erstellt wurde.
- **Status** Der Verbindungsstatus des Knotens. Kann entweder **Verbunden** oder **Getrennt** sein.
- **Verbindungen** Die aktuelle Anzahl von Verbindungen mit diesem Knoten.
- **Zuletzt aktualisiert** Der Zeitpunkt, zu dem der Datenbankserver seinen Status zuletzt aktualisiert hat.

## Ergebnisse

Sie haben Ihr Scale-Out-System mit Schreibschutz als Ressource zum SQL Anywhere-Monitor hinzugefügt und ein Widget erstellt, mit dem dieses System überwacht wird und seine Metriken gesammelt werden.

## Siehe auch

- „SQL Anywhere-Monitor“ auf Seite 1115
- „Datenbankressourcen hinzufügen“ auf Seite 1133
- „MobiLink-Server oder Relay Server-Farmen als Ressourcen hinzufügen“ auf Seite 1135
- „Dashboards“ auf Seite 1124
- „Widget Topologie des SQL Anywhere-Scale-Out“ auf Seite 1129
- „Widgets“ auf Seite 1127

## Der SQL Anywhere SNMP-Erweiterungsagent

Wenn Sie SQL Anywhere unter Windows (32-Bit-Versionen) ausführen, können Sie den SQL Anywhere SNMP-Erweiterungsagenten zusammen mit SNMP-Managementanwendungen einsetzen, um Ihre SQL Anywhere-Datenbanken zu verwalten. Mit einem Agenten können mehrere Datenbanken überwacht werden, die auf verschiedenen Datenbankservern und unterschiedlichen Computern laufen.

Mit dem SQL Anywhere SNMP-Erweiterungsagenten können Sie Folgendes durchführen:

- Die Werte aller Server- und Datenbankstatistiken abfragen
- Die Werte aller Server- und Datenbankeigenschaften abfragen
- Die Werte aller PUBLIC-Datenbankoptionen abfragen
- Die Werte aller PUBLIC-Datenbankoptionen festlegen
- Gespeicherte Prozeduren ausführen
- Basierend auf Werten von Eigenschaften oder Statistiken Traps generieren

### Bereitgestellte Dateien

Die folgenden Dateien für den SQL Anywhere SNMP-Erweiterungsagenten sind in Ihrer SQL Anywhere Studio-Installation enthalten:

- ***dbsnmp16.dll*** Der SQL Anywhere SNMP-Erweiterungsagent. Diese Datei befindet sich im Verzeichnis `%SQLANY16%\bin32`.
- ***iAnywhere.mib*** Die SQL Anywhere MIB-Datenbank enthält alle OIDs für Datenbankserver- und Datenbankeigenschaften, Statistiken und Optionen, auf die mit dem SQL Anywhere SNMP-Erweiterungsagenten zugegriffen werden kann.
- ***RDBMS-MIB.mib*** Dies ist eine generische MIB-Datenbank für relationale Datenbankmanagementsysteme. Sie enthält OIDs, auf die mit dem SQL Anywhere SNMP-Erweiterungsagenten zugegriffen werden kann.
- ***SNMPv2-SMI.mib*** Diese MIB-Datenbank wird von den SQL Anywhere- und RDBMS-MIBs referenziert.
- ***SNMPv2-TC.mib*** Diese MIB-Datenbank wird von den SQL Anywhere- und RDBMS-MIBs referenziert.
- ***SYBASE-MIB.mib*** Die Sybase MIB-Datenbank. Diese MIB-Datenbank wird von der SQL Anywhere-MIB referenziert.
- ***sasnmp.ini*** Diese Datei listet die Datenbanken auf, die der SQL Anywhere SNMP-Erweiterungsagent überwacht. Diese Datei befindet sich im Verzeichnis `%SQLANY16%\bin32`.

## SNMP

Das **SNMP**-Protokoll (Simple Network Management Protocol) ist ein Standardprotokoll für die Netzwerkverwaltung. SNMP ermöglicht **Managern** und **Agenten** die Kommunikation: Manager senden Anfragen an Agenten und die Agenten beantworten Anfragen von Managern. Außerdem kann ein Agent den Manager mithilfe sogenannter **Traps** darauf hinweisen, wenn ein bestimmtes Ereignis eingetreten ist.

SNMP-Agenten bearbeiten Anforderungen zum Abfragen und Festlegen der Werte von Variablen für verwaltete Objekte. Jede Variable hat einen einzigen Wert. Werte sind gewöhnlich Zeichenfolgen oder Ganzzahlen, können aber auch andere Datentypen sein.

Variablen werden in einer globalen Hierarchie gespeichert und jede Variable hat eine eindeutige Nummer unter der ihr übergeordneten Variable. Der vollständige Name einer Variable (einschließlich aller ihrer übergeordneten Elemente) ist der Objektbezeichner (**Object Identifier** - **OID**). Alle OIDs von Sybase beginnen mit **1.3.6.1.4.1.897**.

Die Liste der von einem Agenten unterstützten OIDs, einschließlich ihrer Namen, Typen und anderer Informationen, wird in einer Datei gespeichert, die als Verwaltungsinformations-Datenbank oder **Management Information Base** (MIB) bezeichnet wird.

Eine MIB ist eine Datenbank, die Informationen über verwaltete Objekte zur Netzwerkverwaltung speichert. Die MIB-Datenbank ist von der SQL Anywhere-Datenbank getrennt, die mit dem SQL Anywhere SNMP-Erweiterungsagenten überwacht wird. Die Werte von MIB-Objekten können mit dem SNMP-Dienst geändert oder abgefragt werden. MIB-Objekte sind in einer Hierarchie organisiert, in der die allgemeinen Informationen in der Netzwerk-Hierarchie auf der obersten Ebene gespeichert sind. Der SQL Anywhere SNMP-Erweiterungsagent unterstützt die folgenden MIB-Datenbanken:

- **SQL Anywhere MIB-Datenbank** Eine MIB-Datenbank, die speziell für den SQL Anywhere SNMP-Erweiterungsagenten erstellt wurde. Alle OIDs in der SQL Anywhere MIB-Datenbank beginnen mit **1.3.6.1.4.1.897.2**. Die SQL Anywhere MIB-Datenbank listet die OIDs für die Statistiken, Eigenschaften und Optionswerte auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgefragt und in einigen Fällen festgelegt werden können.
- **RDBMS MIB-Datenbank.** Eine generische, herstellerunabhängige MIB-Datenbank für relationale Datenbanken. Diese MIB-Datenbank enthält Informationen über die Datenbankserver und Datenbanken in Ihrem System.

### Siehe auch

- „Die SQL Anywhere MIB-Datenbank“ auf Seite 1217
- „Die RDBMS MIB-Datenbank“ auf Seite 1220

## Die SQL Anywhere MIB-Datenbank

Die SQL Anywhere MIB wurde für den SQL Anywhere SNMP-Erweiterungsagenten erstellt. Sie enthält alle Statistiken und Eigenschaften des Datenbankservers sowie alle Statistiken, Eigenschaften und Optionen der Datenbank. Die Statistiken und Eigenschaften sind jeweils schreibgeschützt (mit wenigen Ausnahmen) und die Datenbankoptionen können angezeigt und geändert werden.

Standardmäßig befindet sich die SQL Anywhere MIB-Datenbank im Verzeichnis `%SQLANY16%\snmp\iAnywhere.mib`.

Die folgende Hierarchie beschreibt die SQL Anywhere MIB-Datenbank:

OID	Name	Beschreibung
1.3.6.1.4.897.2.1.1. <i>n.db</i>	saServer.saSrvStat	Gibt den Wert der Serverstatistik <i>n</i> für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.1.2. <i>n.db</i>	saServer.saSrvProp	Gibt den Wert der Servereigenschaft <i>n</i> für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.2.1. <i>n.db</i>	saDb.saDbStat	Gibt den Wert der Datenbankstatistik <i>n</i> für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.2.2. <i>n.db</i>	saDb.saDbProp	Gibt den Wert der Datenbankeigenschaft <i>n</i> für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.2.3. <i>n.db</i>	saDb.saDbOpt	Gibt den Wert der Datenbankoption <i>n</i> für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.3.1	saAgent.saVersion	Gibt die Version des SQL Anywhere-Erweiterungsagenten zurück.
1.3.6.1.4.897.2.3.2. <i>db</i>	saAgent.saDbConnStr	Gibt die Verbindungszeichenfolge für die Datenbank <i>db</i> zurück.
1.3.6.1.4.897.2.3.3. <i>db</i>	saAgent.saConnected	Gibt an, ob der SQL Anywhere-Erweiterungsagent mit der Datenbank <i>db</i> verbunden ist. Wenn dieser Wert auf "0" gesetzt wird, trennt der SQL Anywhere-Erweiterungsagent die Verbindung mit der Datenbank, während er beim Wert "1" versucht, sich mit der Datenbank zu verbinden.
1.3.6.1.4.897.2.3.4. <i>db</i>	saAgent.saStarted	Gibt zurück, ob die Datenbank <i>db</i> läuft. Wenn dieser Wert auf "0" gesetzt wird, fährt der SQL Anywhere-Erweiterungsagent die Datenbank herunter <sup>1</sup> , während er beim Wert "1" versucht, die Datenbank zu starten <sup>2</sup> .

OID	Name	Beschreibung
1.3.6.1.4.897.2.3.5.db	saAgent.saProc	Wenn dieser Wert auf eine <i>Prozedurname</i> -Zeichenfolge gesetzt wird, führt der SQL Anywhere-Erweiterungsagent die Prozedur <i>Prozedurname</i> in der Datenbank aus.  Argumente können angegeben werden (z.B. <code>proc_name("Zeichenfolge", 4)</code> ). Wenn keine Argumente angegeben werden, steht nach dem Namen eine leere Klammer (). Beim Abfragen des Werts wird "" zurückgegeben.
1.3.6.1.4.897.2.3.6	saAgent.saRestart	Das Einstellen des Werts dieser Variablen auf 1 bewirkt, dass sich der Agent selbst neu startet. (Er trennt die Verbindung zu allen Datenbanken und lädt die <i>.ini</i> -Datei neu.) Beim Abfragen des Werts wird 0 zurückgegeben.
1.3.6.1.4.897.2.3.7	saAgent.saInifile	Gibt den vollständig Pfad der Datei <i>sasnmplib.ini</i> zurück, die der SQL Anywhere-Erweiterungsagent verwendet.
1.3.6.1.4.897.2.4	saMetaData	Mehrere virtuelle Tabellen. Jede Zeile repräsentiert eine Variable, die von der SQL Anywhere MIB-Datenbank unterstützt wird.

<sup>1</sup> Wenn eine Datenbank durch das Setzen dieser Variablen heruntergefahren wird, kommt es zu einem unbedingten Herunterfahren, d.h. dass die Datenbank unabhängig davon heruntergefahren wird, ob aktive Verbindungen vorliegen.

<sup>2</sup> Damit eine Datenbank durch Setzen dieser Variable gestartet werden kann, muss in der Verbindungszeichenfolge der DBF-Parameter angegeben werden (einschließlich DBN sowie ggf. DBKEY) und es muss entweder das Feld **UtilDbPwd** in der Datei *sasnmplib.ini* festgelegt oder das START DATABASE-Privileg auf dem Server (festgelegt mit der Serveroption -gd) auf "all" gesetzt sein.

### saMetaData-Tabellen

Die SQL Anywhere MIB-Datenbank umfasst Metadatatabellen, über die aus dem SQL Anywhere-Erweiterungsagenten abgefragt werden kann, welche Variablen unterstützt werden.

- **saSrvMetaData.saSrvStatMetaDataTable** Listet die Datenbank-Serverstatistiken auf (Variable unter sa.saServer.saSrvStat)
- **saSrvMetaData.saSrvPropMetaDataTable** Listet die Eigenschaften des Datenbankservers auf (Variable unter sa.saServer.saSrv.Prop).
- **saDbMetaData.saDbStatMetaDataTable** Listet die Datenbankstatistiken auf (Variable unter sa.saDb.saDbStat).
- **saDbMetaData.saDbpropMetaDataTable** Listet die Datenbankeigenschaften auf (Variable unter sa.saDb.saDbProp).
- **saDbMetaData.saDbOptMetaDataTable** Listet die Datenbankoptionen auf (Variable unter sa.saDb.saDbOpt).

### Siehe auch

- [„SQL Anywhere MIB-Referenzhandbuch“ auf Seite 1230](#)
- [„Setzen von Werten mit dem SQL Anywhere SNMP-Erweiterungsagenten“ auf Seite 1226](#)
- [„saMetaData-Tabellen“ auf Seite 1231](#)

## Die RDBMS MIB-Datenbank

Die RDBMS MIB-Datenbank ist eine generische und herstellerunabhängige MIB-Datenbank (RFC 1697) für relationale Datenbank-Verwaltungssystemprodukte. Die RDBMS MIB-Datenbank verwendet **virtuelle Tabellen**, um Informationen über Server und Datenbanken zurückzugeben. Die Basis-OID ist **1.3.6.1.2.1.39** und diese MIB-Datenbank enthält 9 virtuelle Tabellen. Der SQL Anywhere SNMP-Erweiterungsagent unterstützt acht dieser virtuellen Tabellen.

Der SQL Anywhere-Erweiterungsagent stellt schreibgeschützten Zugriff auf alle unterstützten Variablen in der RDBMS MIB-Datenbank bereit. Keine dieser Variablen in der RDBMS MIB-Datenbank kann mit dem SQL Anywhere-Erweiterungsagenten geändert werden.

Eine virtuelle Tabelle enthält eine feste Anzahl von Attributen und eine beliebige Anzahl von Zeilen. Elemente in der Tabelle werden mithilfe von GET-Abfragen abgerufen, indem die Spalten- und die Zeilennummer an die OID der Tabelle angehängt werden. An die Tabellen-OID muss 1 angehängt werden, sodass die OID wie folgt aussieht:

```
table.1.column.rownum
```

Standardmäßig befindet sich die RDBMS MIB im Verzeichnis *%SQLANY16%\snmp\RDBMS-MIB.mib*.

### Siehe auch

- [„RDBMS MIB-Referenz“ auf Seite 1263](#)

## SQL Anywhere SNMP-Erweiterungsagent

Wenn Sie den SQL Anywhere SNMP-Erweiterungsagenten einsetzen wollen, muss auf Ihrem Computer der SNMP-Dienst installiert sein. Außerdem muss die Datei *sasnmp.ini* erstellt werden, die Informationen über die vom SQL Anywhere SNMP-Erweiterungsagenten überwachten Datenbanken enthält.

### SNMP-Installation

Um den SQL Anywhere-Erweiterungsagenten verwenden zu können, muss auf Ihrem Computer der SNMP-Dienst installiert sein. Standardmäßig ist SNMP nicht unter Windows installiert.

Hinweise zur Installation von SNMP finden Sie in Ihrer Dokumentation zum Betriebssystem.

Wenn Sie den SNMP-Dienst auf Ihrem Computer installieren, sollten folgende Dienste auf Ihrem Computer laufen: der "SNMP-Dienst" und der "SNMP-Trap-Dienst".

Wenn Sie den SNMP-Dienst vor der Installation von SQL Anywhere installiert haben, müssen Sie den Dienst stoppen und neu starten, damit er den SQL Anywhere SNMP-Erweiterungsagenten erkennt. Wenn Sie zuerst SQL Anywhere und anschließend den SNMP-Dienst installiert haben, erkennt der Dienst den SQL Anywhere SNMP-Erweiterungsagenten automatisch.

### SNMP-Dienst neu starten

Wenn Sie den SNMP-Dienst vor der Installation von SQL Anywhere installiert haben, müssen Sie den Dienst neu starten, damit er den SQL Anywhere SNMP-Erweiterungsagenten erkennt.

#### Voraussetzungen

Sie müssen auf Ihrem Computer Administrator sein.

#### Aufgabe

1. Führen Sie den folgenden Befehl aus, um den SNMP-Dienst zu stoppen:

```
net stop snmp
```

2. Führen Sie den folgenden Befehl aus, um den SNMP-Dienst zu starten:

```
net start snmp
```

#### Ergebnisse

Der SNMP-Dienst wird neu gestartet.

### SNMP-Erweiterungsagent neu starten

Wenn sich der Inhalt der Datei *sasnmp.ini* ändert, müssen Sie den SNMP-Erweiterungsagenten neu starten, damit die Änderungen wirksam werden.

## Voraussetzungen

Sie müssen auf Ihrem Computer Administrator sein.

## Aufgabe

- Ändern Sie mithilfe Ihres SNMP-Verwaltungstools den Wert der saAgent.saRestart-Eigenschaft von 1.3.6.1.4.1.897.2.3.6 in **1**.

## Ergebnisse

Die Änderungen am SNMP-Erweiterungsagenten werden wirksam.

## Nächste Schritte

Sie können den Inhalt der Datei *sasnmip.ini* mithilfe des Dienstprogramms zum Verschleiern von Dateien (dbfhide) mit einfacher Verschlüsselung verschleiern.

## Siehe auch

- [„Inhalte von .ini-Dateien verbergen“ auf Seite 489](#)

## Konfigurieren des SQL Anywhere SNMP-Erweiterungsagenten

Der SQL Anywhere-Erweiterungsagent kann eine oder mehrere Datenbanken überwachen. Die zu überwachenden Datenbanken sind in der Datei *sasnmip.ini* im folgenden Format gespeichert:

```
[SAAgent]
TrapPollTime=time-in-seconds

[DBn]
ConnStr=connection-string
UtilDbPwd=utility-database-password
CacheTime=time-in-seconds
DBSpaceCacheTime=time-in-seconds
TrapT=trap-information
Disabled=1 or 0
```

Standardmäßig wird vom SQL-Installationsprogramm die Datei *sasnmip.ini* im Verzeichnis *%SQLANYI6%\bin32* eingerichtet.

## Der SAAgent-Abschnitt

Der SAAgent-Abschnitt der *sasnmip.ini*-Datei enthält Informationen über den SQL Anywhere-Erweiterungsagenten. Wenn das Feld TrapPollTime nicht benötigt wird, können Sie den gesamten Abschnitt auslassen.

**TrapPollTime** Dieser Wert legt die Abrufhäufigkeit für dynamische Traps fest, sofern welche angegeben sind. Der SQL Anywhere SNMP-Erweiterungsagent fragt die Werte standardmäßig alle 5 Sekunden ab. Wenn dieser Wert 0 ist, sind dynamische Traps deaktiviert. Dieses Feld ist optional.

## Der DBn-Abschnitt

Jeder **DBn**-Abschnitt der Datei *sasnmplib.ini* beschreibt eine Datenbank, die Herstellung einer Verbindung zu ihr und die für die Datenbank vorhandenen dynamischen Traps. Die Felder in diesem Abschnitt unterscheiden zwischen Groß- und Kleinschreibung.

Der Wert für *n* ist eine Zahl, die die Datenbank kennzeichnet. Die Nummerierung muss mit 1 beginnen und es dürfen keine Zahlen ausgelassen werden. Wenn die Datei *sasnmplib.ini* z.B. die Einträge für [DB1], [DB2] und [DB4] enthält, wird der Eintrag [DB4] ignoriert, da der Eintrag [DB3] in der Datei fehlt.

- **ConnStr** Die Verbindungszeichenfolge für die Verbindung zur Datenbank. Sie müssen genügend Informationen bereitstellen, damit eine Verbindung mit der Datenbank hergestellt werden kann. Dieses Feld ist erforderlich.
  - Wenn Sie für die Verbindung mit der Datenbank eine ODBC-Datenquelle verwenden möchten, muss dies eine *System*-Datenquelle sein, keine *Benutzer*-Datenquelle.
  - Wenn Sie ein integriertes Login verwenden möchten, müssen Sie es dem SYSTEM-Konto zuordnen, weil der SNMP-Agent als Dienst ausgeführt wird. Danach können sich jedoch alle Komponenten, die als Dienst ausgeführt werden, ohne Kennwort mit der Datenbank verbinden. Alternativ dazu können Sie das Konto ändern, unter dem der Dienst ausgeführt wird, und dann für dieses Konto ein integriertes Login erstellen.
  - Die Zeichenfolge `ASTART=NO ; IDLE=0 ; CON=SNMP ; ASTOP=NO` wird der Verbindungszeichenfolge vorangestellt. Die Zeichenfolge hat folgende Konsequenzen:
    - Es wird verhindert, dass der SQL Anywhere SNMP-Erweiterungsagent versucht, einen Datenbankserver automatisch zu starten.
    - Das Inaktivitäts-Timeout wird deaktiviert, da der SQL Anywhere SNMP-Erweiterungsagent sehr wahrscheinlich für einen unbestimmten Zeitraum inaktiv sein wird.
    - Die Verbindung wird benannt, sodass sie identifiziert werden kann.
    - Es wird verhindert, dass die Datenbank heruntergefahren wird, wenn die Verbindung des SQL Anywhere SNMP-Erweiterungsagenten getrennt wird.

Wenn Sie einen dieser Werte in der Verbindungszeichenfolge in der Datei *sasnmplib.ini* verwenden, haben die Werte in der Datei *sasnmplib.ini* Vorrang vor den Standardeinstellungen.

- **UtilDbPwd** Wenn `sa.agent.saStarted` verwendet wird, um eine Datenbank zu starten, versucht der SQL Anywhere SNMP-Erweiterungsagent eine Verbindung zu der Datenbank mit dem Parameter `DBF` herzustellen, der den Datenbankserver anweist, wo die Datenbankdatei zu finden ist. Wenn jedoch zum Starten der Datenbank die DBA-Berechtigung erforderlich ist (was standardmäßig für den Netzwerkserver gilt bzw. mit der Option `-gd dba` sowohl für den Personal Server als auch für den Netzwerkserver festgelegt werden kann), lässt der Server die Verbindung nicht zu.

Um eine Datenbank auf einem solchen Server starten zu können, muss sich der SNMP-Erweiterungsagent als Benutzer mit `SERVER OPERATOR`-Systemprivileg mit einer Datenbank verbinden, die bereits auf demselben Server läuft. Hierzu kann eine Verbindung zur Dienstprogrammdateiabank hergestellt werden. Wenn Sie das Kennwort der

Dienstprogrammdatenbank (festgelegt durch die Serveroption -su) in der Datei *sasnmplib.ini* angeben, stellt der SQL Anywhere-Erweiterungsagent für den Start einer Datenbank eine Verbindung zu dem betreffenden Server her, führt die Anweisung START DATABASE aus und trennt die Verbindung dann. Dieses Feld ist optional.

- **CacheTime** Wenn Daten von der Datenbank abgerufen werden, können sie innerhalb des SQL Anywhere SNMP-Erweiterungsagenten im Cachespeicher zwischengespeichert werden, sodass für nachfolgende Abfragen des betreffenden Datentyps (z.B. Servereigenschaften oder Datenbankstatistiken) keine Kommunikation mit der Datenbank erforderlich ist. Durch das Caching der Daten werden Datenabfragen einerseits schneller ausgeführt, andererseits ist es jedoch möglich, dass die Daten nicht aktuell sind. Mit dem Feld CacheTime können Sie die Verweildauer im Cachespeicher ändern oder den Cachespeicher deaktivieren, indem Sie den Wert auf "0" setzen. Standardmäßig beträgt die Cachezeit 0 Sekunden. Wenn der Parameter CacheTime auf 0 gesetzt wird, sind die abgerufenen Daten immer aktuell, da die Daten für jede Abfrage aus der Datenbank abgerufen werden. Dieses Feld ist optional.
- **DBSpaceCacheTime** Die Tabelle rdbmsDbLimitedResourceTable in der RDBMS MIB-Datenbank enthält Informationen über DBSpaces. Wenn diese Informationen aus der Datenbank abgerufen werden, können sie auch innerhalb des SQL Anywhere-Erweiterungsagenten im Cachespeicher zwischengespeichert werden. Der Standardwert für das Caching von DBSpace-Informationen beträgt 600 Sekunden (10 Minuten). Mit diesem Feld können Sie die Verweildauer im Cachespeicher ändern (oder den Cachespeicher deaktivieren, indem Sie den Wert auf "0" setzen). Dieses Feld ist optional. Siehe „[rdbmsDbLimitedResourceTable](#)“ auf Seite 1265.
- **Trap t** Erstellt eine dynamische Trap. Der Wert *t* muss eine positive Ganzzahl sein, beginnend mit 1. Es dürfen keine Nummern übersprungen werden. Dieses Feld ist optional. Siehe „[Dynamische Traps](#)“ auf Seite 1228.
- **Deaktiviert** Wenn der Wert auf "1" gesetzt ist, wird dieser Datenbankeintrag vom SQL Anywhere SNMP-Erweiterungsagenten übersprungen. Dies ist sinnvoll, wenn eine Datenbank aus der Liste der Datenbanken, die vom SQL Anywhere SNMP-Erweiterungsagenten verwaltet werden, vorübergehend entfernt werden soll, ohne die übrigen Datenbanken neu zu nummerieren. Dieses Feld ist optional.

Wenn Sie diese Datei bearbeiten, müssen Sie den SNMP-Dienst oder den SQL Anywhere SNMP-Erweiterungsagenten neu starten, damit der Agent die neuen Einstellungen verwendet.

### sasnmplib.ini-Beispieldatei

Es folgt eine *sasnmplib.ini*-Beispielsdatei für den SQL Anywhere SNMP-Erweiterungsagenten.

```
[SAAgent]
[DB1]
ConnStr=UID=DBA;PWD=sql;DBN=sales;DBF=sales.db
Trap1=1.1.5 > 50000
UtilDbPwd=test
[DB2]
ConnStr=UID=DBA;PWD=sql;DBN=field;DBF=field.db
UtilDbPwd=test
Disabled=1
[DB3]
ConnStr=UID=DBA;PWD=sql;Host=host2;DBN=hq;DBF=hq.db
UtilDbPwd=test
```

Da im Abschnitt SAAgent keine Parameter angegeben sind, fragt der SQL Anywhere SNMP-Erweiterungsagent die Werte alle 5 Sekunden ab.

Der SQL Anywhere SNMP-Erweiterungsagent überwacht 3 verschiedene Datenbanken, die auf zwei unterschiedlichen Servern laufen. Datenbank 3 läuft auf einem anderen Computer, sodass der Host-Verbindungsparameter erforderlich ist. Für DB1 wird eine Trap festgelegt, die ausgelöst wird, wenn die Anzahl der vom Datenbankserver gesendeten Byte größer als 50000 ist.

## Rückgabewerte des SQL Anywhere SNMP-Erweiterungsagenten

Mit dem SQL Anywhere SNMP-Erweiterungsagenten können Sie folgende Werte abfragen:

- Datenbankservereigenschaften.
- Datenbankserverstatistiken.
- Datenbankoptionen.
- Datenbankeigenschaften.
- Datenbankstatistiken.

Wie diese Werte abgerufen werden, hängt von der jeweiligen SNMP-Managementsoftware ab.

### Beispiele

Die folgende Tabelle enthält eine Beschreibung und einen Beispielwert, der für die folgenden OIDs zurückgegeben werden könnte.

OID	Erklärung	Beispielwert
1.3.6.1.4.1.897.2.1.1.1.1	Serverstatistik ActiveReq für Datenbank 1	1
1.3.6.1.4.1.897.2.2.1.4.1	Datenbankstatistik CacheRead für Datenbank 1	11397
1.3.6.1.4.1.897.2.3.1	Agent-Version	16.0(2459)
1.3.6.1.4.1.897.2.3.2.1	Verbindungszeichenfolge für Datenbank 1	UID=DBA;PWD=sql; Host=host1; DBN=sales; DBF=sales.db

### Siehe auch

- „SQL Anywhere MIB-Servereigenschaften“ auf Seite 1237
- „SQL Anywhere MIB-Serverstatistiken“ auf Seite 1234
- „SQL Anywhere MIB-Datenbankoptionen“ auf Seite 1253
- „SQL Anywhere MIB-Datenbankeigenschaften“ auf Seite 1248
- „SQL Anywhere MIB-Datenbankstatistiken“ auf Seite 1244

## Setzen von Werten mit dem SQL Anywhere SNMP-Erweiterungsagenten

Der SQL Anywhere SNMP-Erweiterungsagent beantwortet get-, get-next- und set-Abfragen des SNMP-Diensts.

Sie können mit dem SQL Anywhere SNMP-Agenten beliebige Datenbankoptionen, einige Servereigenschaften und eine Datenbankeigenschaft festlegen.

Bei der Festlegung von Datenbankoptionen führt der SQL Anywhere SNMP-Agent folgende Anweisung aus:

```
SET OPTION PUBLIC.option-name = 'value'
```

Beim Festlegen von Datenbank- und Servereigenschaften wird die Systemprozedur `sa_server_option` verwendet.

Wie diese Werte festgelegt werden, hängt von der jeweiligen SNMP-Managementsoftware ab.

Weitere Hinweise über die Optionen und Eigenschaften, die mit dem SQL Anywhere SNMP-Erweiterungsagenten festgelegt werden können, finden Sie unter „[SQL Anywhere MIB-Referenzhandbuch](#)“ auf Seite 1230.

### Siehe auch

- „SET OPTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbankoptionen“ auf Seite 544
- „sa\_server\_option-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Gespeicherte Prozeduren und der SQL Anywhere SNMP-Erweiterungsagent

Die SQL Anywhere MIB-Datenbank enthält eine OID, mit der Sie eine gespeicherte Prozedur mithilfe des SQL Anywhere SNMP-Erweiterungsagenten ausführen können. Zur Ausführung einer gespeicherten Prozedur muss der Benutzer, der den SQL Anywhere SNMP-Erweiterungsagenten verwendet, eine der folgenden Voraussetzungen erfüllen:

- Er hat das EXECUTE-Privileg für die Prozedur.
- Er ist der Eigentümer der Prozedur.
- Er hat das EXECUTE ANY PROCEDURE-Systemprivileg

Alle von der Prozedur generierten Ergebnismengen oder Rückgabewerte werden ignoriert.

Wenn Sie eine gespeicherte Prozedur mit dem SQL Anywhere SNMP-Erweiterungsagenten ausführen möchten, setzen Sie den Wert von `saAgent.saProc` (OID 1.3.6.1.4.1.897.2.3.5.db, wobei *db* die Datenbanknummer in der Datei *sasnmplib.ini* ist) auf eine Zeichenfolge, die dem Namen einer gespeicherten Prozedur entspricht. Optional können Sie Argumente für die Prozedur angeben. Wenn keine Argumente vorhanden sind, werden an den Namen der Prozedur Klammern angehängt.

Beispiel: Wenn der Wert von `saAgent.saProc` auf die Zeichenfolge `"pchin.updatesales( 'param1', 2)"` gesetzt wird, wird die gespeicherte Prozedur `updatesales` aufgerufen, die dem Benutzer `pchin` gehört.

Wie der Wert dieser OID auf den Namen der Prozedur gesetzt wird, hängt von der verwendeten SNMP-Management-Software ab. Siehe „[Die SQL Anywhere MIB-Datenbank](#)“ auf Seite 1217.

## Traps

Eine **Trap** ist eine OID, die von einem SNMP-Agenten gesendet wird, wenn ein bestimmtes Ereignis eingetreten ist. Traps werden vom SNMP-Agenten initiiert und können von der SNMP-Managementsoftware erkannt werden. Diese kann direkt auf das Ereignis reagieren oder den SNMP-Agenten nach weiteren Informationen fragen.

Für den Empfang von Traps müssen Sie den SNMP-Dienst konfigurieren. Der SNMP-Dienst empfängt die Trap-Informationen und leitet sie dann an eine bestimmte Stelle weiter. Standardmäßig ist diese Stelle jedoch nicht festgelegt, sodass ein aktiver Trap-Listener keine Traps erkennt.

### Traps des SQL Anywhere SNMP-Erweiterungsagenten

Der SQL Anywhere SNMP-Erweiterungsagent sendet eine Trap, wenn eine Verbindung vom Datenbankserver unterbrochen wird. Die OID dieser Trap lautet `1.3.6.1.2.1.39.2.1`.

Wenn Sie eine Datenbankspiegelung verwenden und die Verbindung des SQL Anywhere SNMP-Erweiterungsagenten zum Datenbankserver unterbrochen wird, versucht der SQL Anywhere SNMP-Erweiterungsagent alle 30 Sekunden, erneut eine Verbindung zum Datenbankserver herzustellen. Wenn sich der Agent erneut verbindet und feststellt, dass er mit einem anderen Datenbankserver verbunden ist (von der `ServerName`-Eigenschaft festgestellt), sendet er eine Trap mit der OID `1.3.6.1.4.1.897.2.6.3` sowie die Datenbank-ID aus der `sasnmplib.ini`-Datei. In diesem Fall war der SQL Anywhere SNMP-Erweiterungsagent mit dem Primärdatenbankserver verbunden, der ausgefallen ist, und nun agiert der Spiegelserver als Primärserver.

Die einzigen anderen Traps, die vom SQL Anywhere SNMP-Erweiterungsagenten gesendet werden, sind dynamische Traps.

### Siehe auch

- „[Datenbankspiegelung](#)“ auf Seite 1467
- „[Dynamische Traps](#)“ auf Seite 1228

## SNMP-Dienst zum Senden von Traps an den Computer konfigurieren

Der SNMP-Dienst kann so konfiguriert werden, dass er Benachrichtigungen über Ereignisse mithilfe von Traps an Ihren Computer sendet.

### Voraussetzungen

Sie müssen auf Ihrem Computer Administrator sein.

## Aufgabe

1. Rechtsklicken Sie auf **Arbeitsplatz** und klicken Sie auf **Verwalten**.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Dienste und Anwendungen**.
3. Doppelklicken Sie im linken Fensterausschnitt auf **Dienste**.
4. Suchen Sie im rechten Fensterausschnitt in der Dienstliste nach dem SNMP-Dienst, rechtsklicken Sie darauf und klicken Sie auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Traps**.
6. Klicken Sie auf **Hinzufügen**.
7. Im Fenster **SNMP-Dienstkonfiguration** geben Sie in das Textfeld **localhost** ein und klicken dann auf **Hinzufügen**.
8. Klicken Sie auf **OK**.

## Ergebnisse

Eine Trap wird zum SNMP-Dienst hinzugefügt, damit er Benachrichtigungen an Ihren Computer sendet.

## Dynamische Traps

Eine **dynamische Trap** ist eine Trap, die vom SQL Anywhere-Erweiterungsagenten gesendet wird, wenn ein einfacher Ausdruck, der den Wert einer bestimmten Eigenschaft, Statistik oder Option einbezieht, TRUE ist. Dynamische Traps werden in der Datei *sasnmplib.ini* erstellt. Das Format der Trap-Informationen im Eintrag in der Datei *sasnmplib.ini* sieht wie folgt aus:

```
Traptrapnum=[1.3.6.1.4.1.897.2.]oid[.dbnum] op value
```

**trapnum** ist die dynamische Trap-Nummer. Die Nummerierung muss bei 1 beginnen und sequenziell sein.

**oid** ist die OID der Eigenschaft, Statistik oder Option. OIDs in der SQL Anywhere MIB-Datenbank oder der RDBMS MIB-Datenbank werden unterstützt. Wenn die betreffende OID eine ungültige SQL Anywhere- oder RDBMS-OID ist, wird das Präfix der SQL Anywhere MIB-Datenbank (1.3.6.1.4.1.897.2.) vorangestellt.

Weitere Informationen zu den OIDs in der SQL Anywhere MIB-Datenbank finden Sie unter „[SQL Anywhere MIB-Referenzhandbuch](#)“ auf Seite 1230.

Weitere Informationen zu den OIDs in der RDBMS MIB-Datenbank finden Sie unter „[RDBMS MIB-Referenz](#)“ auf Seite 1263.

### Hinweis

Sie können nur OIDs verwenden, die Datenbankserver- bzw. Datenbankeigenschaften, Statistiken oder Optionen in dynamischen Traps entsprechen.

**dbnum** ist die Datenbanknummer. Dieses Feld ist optional. Wenn es jedoch angegeben wird, muss sein Inhalt mit der Datenbanknummer aus dem Abschnitt [DBn] der Datei *sasnmplib.ini* übereinstimmen.

option muss einen der folgenden Werte haben:

- = oder == (gleich)
- !=, <> oder >< (ungleich)
- <= oder =< (kleiner oder gleich)
- >= oder => (größer oder gleich)
- < (kleiner als)
- > (größer als)

### op

#### Hinweis

Für Zeichenfolgenwerte wird nur die Gleichheit und Ungleichheit unterstützt.

**value** ist der im Ausdruck zu verwendende Wert. Zeichenfolgenwerte können zwischen Apostrophe oder Anführungszeichen gesetzt werden. Diese Apostrophe bzw. Anführungszeichen werden nicht in den Wert einbezogen. Wenn öffnende oder schließende Apostrophe oder Anführungszeichen als Teil der Zeichenfolge verwendet werden sollen, müssen sie verdoppelt werden. Apostrophe innerhalb der Zeichenfolge dürfen nicht verdoppelt werden.

Beim Festlegen von dynamischen Traps verwenden Sie k, m, g oder t um Einheiten von Kilobyte, Megabyte, Gigabyte oder Terabyte anzugeben. Sie können z.B. das Auslösen einer dynamischen Trap festlegen, wenn die aktuelle Cachegröße 200 MB überschreitet, indem Sie Folgendes verwenden:

```
Trap1=1.3.6.1.4.1.897.2.1.1.11.1 > 200M
```

Sie können beliebig viele Trap-Felder in der Datei *sasnmplib.ini* angeben. Die für die Trap verwendete OID lautet 1.3.6.1.4.1.897.2.4.1. Die mit der Trap gesendeten Daten enthalten folgende Angaben:

- Trap-Nummer (beginnt bei 1 für die erste dynamische Trap, die vom SQL Anywhere SNMP-Agenten gesendet wird)
- Datenbankindex
- Trap-Index des Datenbanknamens (aus der Datei *sasnmplib.ini*)
- Variablenname
- Variablenwert (dies ist der aktuelle Wert der Variablen, nicht unbedingt der Schwellenwert)

### Verhalten dynamischer Traps

Wenn eine dynamische Trap ausgelöst wurde, wird die Trap erst dann erneut gesendet, wenn sich die Bedingung, die sie ausgelöst hat, zu FALSE und dann zurück zu TRUE ändert.

Wenn Sie z.B. eine dynamische Trap mit 1.1.11.1 >= 51200K gesetzt haben, wird die Trap ausgelöst, sobald die Cachegröße des Servers 50 MB (= 51200 kB) erreicht. Danach wird die dynamische Trap deaktiviert, sodass keine weiteren Traps gesendet werden. Die Trap wird nur dann wieder aktiviert, wenn die Cachegröße anschließend unter 50 MB absinkt. Sie werden dann informiert, wenn die Cachegröße erneut über 50 MB anwächst.

### Beispiele für Traps

Trap-Informationen	Beschreibung
Trap1=1.1.5 > 10000	Die Trap wird gesendet, wenn die Anzahl der vom Server gesendeten Byte 10.000 übersteigt.
Trap2=1.3.6.1.2.1.39.1.4.1.4.14.1 >= 10485760	Die Trap wird gesendet, wenn die Transaktionslogdatei größer als 10 MB ist.

## SQL Anywhere MIB-Referenzhandbuch

Die Liste der von einem SNMP-Agenten unterstützten Objektbezeichner (Object Identifiers - OIDs), einschließlich ihrer Namen, Typen und anderer Informationen, wird in einer Datei gespeichert, die als Verwaltungsinformations-Datenbank oder Management Information Base (MIB) bezeichnet wird. Die folgenden Abschnitte listen die Statistiken, Eigenschaften und Optionen auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgefragt und gesetzt werden können.

### Siehe auch

- „SNMP“ auf Seite 1217

## Agent

Die Agent-Tabelle listet Informationen über den SQL Anywhere SNMP-Erweiterungsagenten auf.

Beschreibbare Eigenschaften sind mit einem Stern (\*) gekennzeichnet. Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.3.1	String	saVersion	Agent-Version
1.3.6.1.4.1.897.2.3.2. <i>n</i>	String	saDBConnStr	Verbindungszeichenfolge
1.3.6.1.4.1.897.2.3.3. <i>n</i>	Integer32	saConnected*	1, wenn der Agent verbunden ist, sonst 0
1.3.6.1.4.1.897.2.3.4. <i>n</i>	Integer32	saStarted*	1, wenn die Datenbank gestartet ist, sonst 0

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.3.5. <i>n</i>	String	saProc*	" "
1.3.6.1.4.1.897.2.3.6	String	saRestart*	0

## saMetaData-Tabellen

Die folgenden Metadaten tabellen sind in der SQL Anywhere MIB-Datenbank enthalten:

- saSrvMetaData.saSrvStatMetaDataTable
- saSrvMetaData.saSrvPropMetaDataTable
- saSrvMetaData.saDbStatMetaDataTable
- saSrvMetaData.saDbPropMetaDataTable
- saSrvMetaData.saDbOptMetaDataTable

### saSrvMetaData.saSrvStatMetaDataTable

Diese Tabelle enthält Metadaten über die Datenbankserver-Statistiken.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.4.1.1.1.1. <i>db</i>	Integer32	saSrvStatIndex	<i>db</i>
1.3.6.1.4.1.897.2.4.1.1.1.2. <i>db</i>	Integer32	saSrvStatObjType	1 <sup>1</sup>
1.3.6.1.4.1.897.2.4.1.1.1.3. <i>db</i>	Integer32	saSrvStatType	1 <sup>2</sup>
1.3.6.1.4.1.897.2.4.1.1.1.4. <i>db</i>	OID	saSrvStatOID	OID des SQL Anywhere MIB-Eintrags <sup>3</sup>
1.3.6.1.4.1.897.2.4.1.1.1.5. <i>db</i>	String	saSrvStatName	Statistikname

<sup>1</sup> Werte: 1=Server, 2=Datenbank

<sup>2</sup> Werte: 1=Statistik, 2=Eigenschaft, 3=Option

<sup>3</sup> Die zurückgegebene OID enthält nicht die Datenbanknummer. Sie müssen die Datenbanknummer an die OID anhängen, bevor sie in einer Abfrage verwendet werden kann.

### saSrvMetaData.saSrvPropMetaDataTable

Diese Tabelle enthält Metadaten über die Datenbankserver-Eigenschaften.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.4.1.2.1.1.db	Integer32	saSrvPropIndex	<i>db</i>
1.3.6.1.4.1.897.2.4.1.2.1.2.db	Integer32	saSrvPropObjType	1 <sup>1</sup>
1.3.6.1.4.1.897.2.4.1.2.1.3.db	Integer32	saSrvPropType	2 <sup>2</sup>
1.3.6.1.4.1.897.2.4.1.2.1.4.db	OID	saSrvPropOID	OID des SQL Anywhere MIB-Eintrags <sup>3</sup>
1.3.6.1.4.1.897.2.4.1.2.1.5.db	String	saSrvPropName	Eigenschaftsname

<sup>1</sup> Werte: 1=Server, 2=Datenbank

<sup>2</sup> Werte: 1=Statistik, 2=Eigenschaft, 3=Option

<sup>3</sup> Die zurückgegebene OID enthält nicht die Datenbanknummer. Sie müssen die Datenbanknummer an die OID anhängen, bevor sie in einer Abfrage verwendet werden kann.

## saDbMetaData.saDbStatMetaDataTable

Diese Tabelle enthält Metadaten über die Datenbank-Statistiken.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnm.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.4.2.1.1.1.db	Integer32	saDbStatIndex	<i>db</i>
1.3.6.1.4.1.897.2.4.2.1.1.2.db	Integer32	saDbStatObjType	2 <sup>1</sup>
1.3.6.1.4.1.897.2.4.2.1.1.3.db	Integer32	saDbStatType	1 <sup>2</sup>
1.3.6.1.4.1.897.2.4.2.1.1.4.db	OID	saDbStatOID	OID des SQL Anywhere MIB-Eintrags <sup>3</sup>
1.3.6.1.4.1.897.2.4.2.1.1.5.db	String	saDbStatName	Statistikname

<sup>1</sup> Werte: 1=Server, 2=Datenbank

<sup>2</sup> Werte: 1=Statistik, 2=Eigenschaft, 3=Option

<sup>3</sup> Die zurückgegebene OID enthält nicht die Datenbanknummer. Sie müssen die Datenbanknummer an die OID anhängen, bevor sie in einer Abfrage verwendet werden kann.

## saDbMetaData.saDbPropMetaDataTable

Diese Tabelle enthält Metadaten über die Datenbank-Eigenschaften.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.4.2.2.1.1. <i>db</i>	Integer32	saDbPropIndex	<i>db</i>
1.3.6.1.4.1.897.2.4.2.2.1.2. <i>db</i>	Integer32	saDbPropObjType	2 <sup>1</sup>
1.3.6.1.4.1.897.2.4.2.2.1.3. <i>db</i>	Integer32	saDbPropType	2 <sup>2</sup>
1.3.6.1.4.1.897.2.4.2.2.1.4. <i>db</i>	OID	saDbPropOID	OID des SQL Anywhere MIB-Eintrags <sup>3</sup>
1.3.6.1.4.1.897.2.4.2.2.1.5. <i>db</i>	String	saDbPropName	Eigenschaftsname

<sup>1</sup> Werte: 1=Server, 2=Datenbank

<sup>2</sup> Werte: 1=Statistik, 2=Eigenschaft, 3=Option

<sup>3</sup> Die zurückgegebene OID enthält nicht die Datenbanknummer. Sie müssen die Datenbanknummer an die OID anhängen, bevor sie in einer Abfrage verwendet werden kann.

## saDbMetaData.saDbOptMetaDataTable

Diese Tabelle enthält Metadaten über die Datenbankoptionen.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.4.1.897.2.4.2.1.1.1. <i>db</i>	Integer32	saDbOptIndex	<i>db</i>
1.3.6.1.4.1.897.2.4.2.1.1.2. <i>db</i>	Integer32	saDbOptObjType	2 <sup>1</sup>
1.3.6.1.4.1.897.2.4.2.1.1.3. <i>db</i>	Integer32	saDbOptType	3 <sup>2</sup>
1.3.6.1.4.1.897.2.4.2.1.1.4. <i>db</i>	OID	saDbOptOID	OID des SQL Anywhere MIB-Eintrags <sup>3</sup>
1.3.6.1.4.1.897.2.4.2.1.1.5. <i>db</i>	String	saDbOptName	Name der Option

<sup>1</sup> Werte: 1=Server, 2=Datenbank

<sup>2</sup> Werte: 1=Statistik, 2=Eigenschaft, 3=Option

<sup>3</sup> Die zurückgegebene OID enthält nicht die Datenbanknummer. Sie müssen die Datenbanknummer an die OID anhängen, bevor sie in einer Abfrage verwendet werden kann.

## SQL Anywhere MIB-Serverstatistiken

Diese Tabelle listet die OIDs und Namen der Datenbankserver-Statistiken auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgerufen werden können.

Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

### Beschreibungen

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatActiveReq	ActiveReq
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatAvailIO	AvailIO
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatBytesReceived	BytesReceived
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatBytesReceivedUncomp	BytesReceivedUncomp
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatBytesSent	BytesSent
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatBytesSentUncomp	BytesSentUncomp
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatCacheHits	CacheHits
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatCachePinned	CachePinned
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatCacheRead	CacheRead
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatCacheReplacements	CacheReplacements
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatCurrentCacheSize	CurrentCacheSize
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatDiskRead	DiskRead
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatFreeBuffers	FreeBuffers
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatInternal	Internal
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatUniqueClientAddresses	UniqueClientAddresses
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatLockedHeapPages	LockedHeapPages
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Counter64	srvStatMainHeapBytes	MainHeapBytes
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatMainHeapPages	MainHeapPages

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatMapPhysicalMemoryEng	MapPhysicalMemoryEng
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatMaxCacheSize	MaxCacheSize
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatMinCacheSize	MinCacheSize
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatMultiPacketsReceived	MultiPacketsReceived
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatMultiPacketsSent	MultiPacketsSent
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatPacketsReceived	PacketsReceived
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatPacketsReceivedUncomp	PacketsReceivedUncomp
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatPacketsSent	PacketsSent
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatPacketsSentUncomp	PacketsSentUncomp
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatPeakCacheSize	PeakCacheSize
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatRemoteputWait	RemoteputWait
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatReq	Req
1.3.6.1.4.1.897.2.1.1.n	Counter64	srvStatSendFail	SendFail
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatTotalBuffers	TotalBuffers
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatUnschReq	UnschReq
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatInternal	Internal
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheFile	CacheFile
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheFileDirty	CacheFileDirty
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheAllocated	CacheAllocated
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCachePanics	CachePanics
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheFree	CacheFree
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheScavenges	CacheScavenges
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCacheScavengeVisited	CacheScavengeVisited
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatLockedCursorPages	LockedCursorPages

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryHeapPages	QueryHeapPages
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCarverHeapPages	CarverHeapPages
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatHeapsRelocatable	HeapsRelocatable
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatHeapsLocked	HeapsLocked
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatHeapsQuery	HeapsQuery
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatHeapsCarver	HeapsCarver
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatMultiPageAllocs	MultiPageAllocs
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatRequestsReceived	RequestsReceived
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatExchangeTasks	ExchangeTasks
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatClientStmtCacheHits	ClientStmtCacheHits
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatClientStmtCacheMisses	ClientStmtCacheMisses
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemActiveCurr	QueryMemActiveCurr
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemActiveEst	QueryMemActiveEst
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemGrantWaiting	QueryMemGrantWaiting
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemGrantRequested	QueryMemGrantRequested
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemGrantWaited	QueryMemGrantWaited
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemGrantFailed	QueryMemGrantFailed
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemGrantGranted	QueryMemGrantGranted
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatQueryMemExtraAvail	QueryMemExtraAvail
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatThreadDeadlocksAvoided	ThreadDeadlocksAvoided
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatThreadDeadlocksReported	ThreadDeadlocksReported
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCommit	Commit
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCursor	Cursor
1.3.6.1.4.1.897.2.1.1.n	Integer32	srvStatCursorOpen	CursorOpen

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatRlbk	Rlbk
1.3.6.1.4.1.897.2.1.1. <i>n</i>	Integer32	srvStatPrepStmnt	PrepStmnt

**Siehe auch**

- „Liste der Datenbankserveigenschaften“ auf Seite 745
- „Liste der Datenbankeigenschaften“ auf Seite 767

**SQL Anywhere MIB-Serveigenschaften**

Die folgende Tabelle listet OIDs und Namen der Datenbankserver-Eigenschaften auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgerufen werden können.

Beschreibbare Eigenschaften sind mit einem Stern (\*) gekennzeichnet. Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

**Beschreibungen**

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.1. <i>n</i>	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.2. <i>n</i>	String	srvPropCharSet	CharSet
1.3.6.1.4.1.897.2.1.2.3. <i>n</i>	String	srvPropCommandLine	CommandLine
1.3.6.1.4.1.897.2.1.2.4. <i>n</i>	String	srvPropCompactPlatformVer	CompactPlatformVer
1.3.6.1.4.1.897.2.1.2.5. <i>n</i>	String	srvPropCompanyName	CompanyName
1.3.6.1.4.1.897.2.1.2.6. <i>n</i>	String	srvPropConnsDisabled*	ConnsDisabled
1.3.6.1.4.1.897.2.1.2.7. <i>n</i>	String	srvPropConsoleLogFile	ConsoleLogFile
1.3.6.1.4.1.897.2.1.2.8. <i>n</i>	String	srvPropDefaultCollation	DefaultCollation
1.3.6.1.4.1.897.2.1.2.9. <i>n</i>	String	srvPropIdleTimeout	IdleTimeout
1.3.6.1.4.1.897.2.1.2.10. <i>n</i>	String	srvPropIsIQ	IsIQ
1.3.6.1.4.1.897.2.1.2.11. <i>n</i>	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.12. <i>n</i>	String	srvPropIsNetworkServer	IsNetworkServer
1.3.6.1.4.1.897.2.1.2.13. <i>n</i>	String	srvPropIsRuntimeServer	IsRuntimeServer

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.14.n	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.15.n	String	srvPropLanguage	Language
1.3.6.1.4.1.897.2.1.2.16.n	String	srvPropLegalCopyright	LegalCopyright
1.3.6.1.4.1.897.2.1.2.17.n	String	srvPropLegalTrademarks	LegalTrademarks
1.3.6.1.4.1.897.2.1.2.18.n	String	srvPropLicenseCount	LicenseCount
1.3.6.1.4.1.897.2.1.2.19.n	String	srvPropLicensedCompany	LicensedCompany
1.3.6.1.4.1.897.2.1.2.20.n	String	srvPropLicensedUser	LicensedUser
1.3.6.1.4.1.897.2.1.2.21.n	String	srvPropLicenseType	LicenseType
1.3.6.1.4.1.897.2.1.2.22.n	String	srvPropLivenessTimeout*	LivenessTimeout
1.3.6.1.4.1.897.2.1.2.23.n	String	srvPropMachineName	MachineName
1.3.6.1.4.1.897.2.1.2.24.n	String	srvPropMaxMessage	MaxMessage
1.3.6.1.4.1.897.2.1.2.25.n	String	srvPropMessageWindowSize	MessageWindowSize
1.3.6.1.4.1.897.2.1.2.26.n	String	srvPropName	Name
1.3.6.1.4.1.897.2.1.2.27.n	String	srvPropNativeProcessorArchitecture	NativeProcessorArchitecture
1.3.6.1.4.1.897.2.1.2.28.n	String	srvPropNumPhysicalProcessors	NumPhysicalProcessors
1.3.6.1.4.1.897.2.1.2.29.n	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.30.n	String	srvPropOmniIdentifier	OmniIdentifier
1.3.6.1.4.1.897.2.1.2.31.n	String	srvPropPageSize	PageSize
1.3.6.1.4.1.897.2.1.2.32.n	String	srvPropPlatform	Platform
1.3.6.1.4.1.897.2.1.2.33.n	String	srvPropPlatformVer	PlatformVer
1.3.6.1.4.1.897.2.1.2.34.n	String	srvPropProcessCPU	ProcessCPU
1.3.6.1.4.1.897.2.1.2.35.n	String	srvPropProcessCPUSystem	ProcessCPUSystem
1.3.6.1.4.1.897.2.1.2.36.n	String	srvPropProcessCPUUser	ProcessCPUUser
1.3.6.1.4.1.897.2.1.2.37.n	String	srvPropProcessorArchitecture	ProcessorArchitecture

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.38.n	String	srvPropProductName	ProductName
1.3.6.1.4.1.897.2.1.2.39.n	String	srvPropProductVersion	ProductVersion
1.3.6.1.4.1.897.2.1.2.40.n	String	srvPropQuittingTime*	QuittingTime
1.3.6.1.4.1.897.2.1.2.41.n	String	srvPropRememberLastStatement*	RememberLastStatement
1.3.6.1.4.1.897.2.1.2.42.n	String	srvPropRequestFilterConn	RequestFilterConn
1.3.6.1.4.1.897.2.1.2.43.n	String	srvPropRequestFilterDB	RequestFilterDB
1.3.6.1.4.1.897.2.1.2.44.n	String	srvPropRequestLogFile*	RequestLogFile
1.3.6.1.4.1.897.2.1.2.45.n	String	srvPropRequestLogging*	RequestLogging
1.3.6.1.4.1.897.2.1.2.46.n	String	srvPropRequestLogMaxSize	RequestLogMaxSize
1.3.6.1.4.1.897.2.1.2.47.n	String	srvPropStartTime	StartTime
1.3.6.1.4.1.897.2.1.2.48.n	String	srvPropTempDir	TempDir
1.3.6.1.4.1.897.2.1.2.49.n	String	srvPropMultiProgrammingLevel	MultiProgrammingLevel
1.3.6.1.4.1.897.2.1.2.50.n	String	srvPropTimeZoneAdjustment	TimeZoneAdjustment
1.3.6.1.4.1.897.2.1.2.51.n	String	srvPropHttpPorts	HttpPorts
1.3.6.1.4.1.897.2.1.2.52.n	String	srvPropHttpsPorts	HttpsPorts
1.3.6.1.4.1.897.2.1.2.53.n	String	srvPropProfileFilterConn	ProfileFilterConn
1.3.6.1.4.1.897.2.1.2.54.n	String	srvPropProfileFilterUser	ProfileFilterUser
1.3.6.1.4.1.897.2.1.2.55.n	String	srvPropRequestLogNumFiles	RequestLogNumFiles
1.3.6.1.4.1.897.2.1.2.56.n	String	srvPropIsFipsAvailable	IsFipsAvailable
1.3.6.1.4.1.897.2.1.2.57.n	String	srvPropFipsMode	FipsMode
1.3.6.1.4.1.897.2.1.2.58.n	String	srvPropStartDBPermission	StartDBPermission
1.3.6.1.4.1.897.2.1.2.59.n	String	srvPropServerName	ServerName
1.3.6.1.4.1.897.2.1.2.60.n	String	srvPropRememberLastPlan	RememberLastPlan
1.3.6.1.4.1.897.2.1.2.61.n	String	srvPropInternal	Internal

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.62.n	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.63.n	String	srvPropRequestTiming	RequestTiming
1.3.6.1.4.1.897.2.1.2.64.n	String	srvPropCacheSizingStatistics	CacheSizingStatistics
1.3.6.1.4.1.897.2.1.2.65.n	String	srvPropConsoleLogMaxSize	ConsoleLogMaxSize
1.3.6.1.4.1.897.2.1.2.66.n	String	srvPropDebuggingInformation	DebuggingInformation
1.3.6.1.4.1.897.2.1.2.67.n	String	srvPropMessage	Message
1.3.6.1.4.1.897.2.1.2.68.n	String	srvPropMessageText	MessageText
1.3.6.1.4.1.897.2.1.2.69.n	String	srvPropMessageTime	MessageTime
1.3.6.1.4.1.897.2.1.2.70.n	String	srvPropIsRsaAvailable	IsRsaAvailable
1.3.6.1.4.1.897.2.1.2.71.n	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.72.n	String	srvPropMaxConnections	MaxConnections
1.3.6.1.4.1.897.2.1.2.73.n	String	srvPropNumLogicalProcessors	NumLogicalProcessors
1.3.6.1.4.1.897.2.1.2.74.n	String	srvPropNumLogicalProcessorsUsed	NumLogicalProcessorsUsed
1.3.6.1.4.1.897.2.1.2.75.n	String	srvPropNumPhysicalProcessorsUsed	NumPhysicalProcessorsUsed
1.3.6.1.4.1.897.2.1.2.76.n	String	srvPropDefaultNcharCollation	DefaultNcharCollation
1.3.6.1.4.1.897.2.1.2.77.n	String	srvPropCollectStatistics	CollectStatistics
1.3.6.1.4.1.897.2.1.2.78.n	String	srvPropFirstOption	FirstOption
1.3.6.1.4.1.897.2.1.2.79.n	String	srvPropLastOption	LastOption
1.3.6.1.4.1.897.2.1.2.80.n	String	srvPropLastConnectionProperty	LastConnectionProperty
1.3.6.1.4.1.897.2.1.2.81.n	String	srvPropLastDatabaseProperty	LastDatabaseProperty
1.3.6.1.4.1.897.2.1.2.82.n	String	srvPropLastServerProperty	LastServerProperty
1.3.6.1.4.1.897.2.1.2.83.n	String	srvPropWebClientLogging	WebClientLogging
1.3.6.1.4.1.897.2.1.2.84.n	String	srvPropWebClientLogFile	WebClientLogFile

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.85. <i>n</i>	String	srvPropHttpNumConnections	HttpNumConnections
1.3.6.1.4.1.897.2.1.2.86. <i>n</i>	String	srvPropHttpsNumConnections	HttpsNumConnections
1.3.6.1.4.1.897.2.1.2.87. <i>n</i>	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.88. <i>n</i>	String	srvPropHttpNumActiveReq	HttpNumActiveReq
1.3.6.1.4.1.897.2.1.2.89. <i>n</i>	String	srvPropHttpsNumActiveReq	HttpsNumActiveReq
1.3.6.1.4.1.897.2.1.2.90. <i>n</i>	String	srvPropHttpNumSessions	HttpNumSessions
1.3.6.1.4.1.897.2.1.2.91. <i>n</i>	String	srvPropQueryMemPages	QueryMemPages
1.3.6.1.4.1.897.2.1.2.92. <i>n</i>	String	srvPropQueryMemGrantBase	QueryMemGrantBase
1.3.6.1.4.1.897.2.1.2.93. <i>n</i>	String	srvPropQueryMemGrantBaseMI	QueryMemGrantBaseMI
1.3.6.1.4.1.897.2.1.2.94. <i>n</i>	String	srvPropQueryMemGrantExtra	QueryMemGrantExtra
1.3.6.1.4.1.897.2.1.2.95. <i>n</i>	String	srvPropQueryMemActiveMax	QueryMemActiveMax
1.3.6.1.4.1.897.2.1.2.96. <i>n</i>	String	srvPropQueryMemPercentOfCache	QueryMemPercentOfCache
1.3.6.1.4.1.897.2.1.2.97. <i>n</i>	String	srvPropMessageCategoryLimit	MessageCategoryLimit
1.3.6.1.4.1.897.2.1.2.98. <i>n</i>	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.99. <i>n</i>	String	srvPropInternal	Internal
1.3.6.1.4.1.897.2.1.2.100. <i>n</i>	String	srvPropIsService	IsService
1.3.6.1.4.1.897.2.1.2.101. <i>n</i>	String	srvPropTcpIpAddresses	TcpIpAddresses
1.3.6.1.4.1.897.2.1.2.102. <i>n</i>	String	srvPropHttpAddresses	HttpAddresses
1.3.6.1.4.1.897.2.1.2.103. <i>n</i>	String	srvPropHttpsAddresses	HttpsAddresses
1.3.6.1.4.1.897.2.1.2.104. <i>n</i>	String	srvPropProcessID	ProcessID

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.105. <i>n</i>	String	srvPropRemoteCapability	RemoteCapability
1.3.6.1.4.1.897.2.1.2.106. <i>n</i>	String	srvPropMaxRemoteCapability	MaxRemoteCapability
1.3.6.1.4.1.897.2.1.2.107. <i>n</i>	String	srvPropEventTypeName	EventTypeName
1.3.6.1.4.1.897.2.1.2.108. <i>n</i>	String	srvPropEventTypeDesc	EventTypeDesc
1.3.6.1.4.1.897.2.1.2.109. <i>n</i>	String	srvPropMaxEventType	MaxEventType
1.3.6.1.4.1.897.2.1.2.110. <i>n</i>	String	srvPropIsPortableDevice	IsPortableDevice
1.3.6.1.4.1.897.2.1.2.111. <i>n</i>	String	srvPropIPAddressMonitorPeriod	IPAddressMonitorPeriod
1.3.6.1.4.1.897.2.1.2.112. <i>n</i>	String	srvPropServerEdition	ServerEdition
1.3.6.1.4.1.897.2.1.2.113. <i>n</i>	String	srvPropObjectType	ObjectType
1.3.6.1.4.1.897.2.1.2.114. <i>n</i>	String	srvPropCurrentMultiProgram- mingLevel	CurrentMultiProgramming- Level
1.3.6.1.4.1.897.2.1.2.115. <i>n</i>	String	srvPropMinMultiProgrammingLe- vel	MinMultiProgrammingLe- vel
1.3.6.1.4.1.897.2.1.2.116. <i>n</i>	String	srvPropMaxMultiProgrammingLe- vel	MaxMultiProgrammingLe- vel
1.3.6.1.4.1.897.2.1.2.117. <i>n</i>	String	srvPropAutoMultiProgramming- Level	AutoMultiProgrammingLe- vel
1.3.6.1.4.1.897.2.1.2.118. <i>n</i>	String	srvPropAutoMultiProgramming- LevelStatistics	AutoMultiProgrammingLe- velStatistics
1.3.6.1.4.1.897.2.1.2.119. <i>n</i>	String	srvPropApproximateCPUTime	ApproximateCPUTime
1.3.6.1.4.1.897.2.1.2.120. <i>n</i>	String	srvPropConnectedTime	ConnectedTime

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.1.2.121. <i>n</i>	String	srvPropReqCountUnscheduled	ReqCountUnscheduled
1.3.6.1.4.1.897.2.1.2.122. <i>n</i>	String	srvPropReqCountActive	ReqCountActive
1.3.6.1.4.1.897.2.1.2.123. <i>n</i>	String	srvPropReqCountBlockIO	ReqCountBlockIO
1.3.6.1.4.1.897.2.1.2.124. <i>n</i>	String	srvPropReqCountBlockLock	ReqCountBlockLock
1.3.6.1.4.1.897.2.1.2.125. <i>n</i>	String	srvPropReqCountBlockContention	ReqCountBlockContention
1.3.6.1.4.1.897.2.1.2.126. <i>n</i>	String	srvPropReqTimeUnscheduled	ReqTimeUnscheduled
1.3.6.1.4.1.897.2.1.2.127. <i>n</i>	String	srvPropReqTimeActive	ReqTimeActive
1.3.6.1.4.1.897.2.1.2.128. <i>n</i>	String	srvPropReqTimeBlockIO	ReqTimeBlockIO
1.3.6.1.4.1.897.2.1.2.129. <i>n</i>	String	srvPropReqTimeBlockLock	ReqTimeBlockLock
1.3.6.1.4.1.897.2.1.2.130. <i>n</i>	String	srvPropReqTimeBlockContention	ReqTimeBlockContention
1.3.6.1.4.1.897.2.1.2.131. <i>n</i>	String	srvPropLicenseKey	LicenseKey
1.3.6.1.4.1.897.2.1.2.132. <i>n</i>	String	srvPropDiskSandbox	DiskSandbox
1.3.6.1.4.1.897.2.1.2.133. <i>n</i>	String	srvPropProcessorAffinity	ProcessorAffinity
1.3.6.1.4.1.897.2.1.2.134. <i>n</i>	String	srvPropIsAesniAvailable	IsAesniAvailable

**Siehe auch**

- [„Liste der Datenbankseigenschaft“ auf Seite 745](#)

## SQL Anywhere MIB-Datenbankstatistiken

Die folgende Tabelle listet die OIDs und Namen der Datenbankstatistiken auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgerufen werden können.

Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

### Beschreibungen

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Counter64	dbStatCacheHits	CacheHits
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCacheReadIndInt	CacheReadIndInt
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCacheReadIndLeaf	CacheReadIndLeaf
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Counter64	dbStatCacheRead	CacheRead
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCacheReadTable	CacheReadTable
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatChkpt	Chkpt
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatChkptFlush	ChkptFlush
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatChkptPage	ChkptPage
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointUrgency	CheckpointUrgency
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatInternal	Internal
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatInternal	Internal
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogCommitTo-Disk	CheckpointLogCommit-ToDisk
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogPagesInUse	CheckpointLogPagesInUse
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogPagesRelocated	CheckpointLogPagesRelocated
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogSavePre-image	CheckpointLogSavePre-image
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogSize	CheckpointLogSize
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatCheckpointLogWrites	CheckpointLogWrites

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCheckpointLogPagesWritten	CheckpointLogPagesWritten
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCommitFile	CommitFile
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatConnCount	ConnCount
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCurrIO	CurrIO
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCurrRead	CurrRead
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCurrWrite	CurrWrite
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatDiskReadIndInt	DiskReadIndInt
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatDiskReadIndLeaf	DiskReadIndLeaf
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatDiskRead	DiskRead
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatDiskReadTable	DiskReadTable
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatDiskWrite	DiskWrite
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatExtendDB	ExtendDB
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatExtendTempWrite	ExtendTempWrite
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatFullCompare	FullCompare
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatGetData	GetData
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIdleCheck	IdleCheck
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIdleChkpt	IdleChkpt
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIdleChkTime	IdleChkTime
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIdleWrite	IdleWrite
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIndAdd	IndAdd
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIndLookup	IndLookup
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatIOToRecover	IOToRecover
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatInternal	Internal
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatInternal	Internal

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatLockTablePages	LockTablePages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatInternal	Internal
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatMaxIO	MaxIO
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatMaxRead	MaxRead
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatMaxWrite	MaxWrite
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatPageRelocations	PageRelocations
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatProcedurePages	ProcedurePages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatQueryCachePages	QueryCachePages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatQueryLowMemoryStrategy	QueryLowMemoryStrategy
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatQueryRowsMaterialized	QueryRowsMaterialized
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatRecoveryUrgency	RecoveryUrgency
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatLogFreeCommit	LogFreeCommit
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatLogWrite	LogWrite
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatRelocatableHeapPages	RelocatableHeapPages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatRollbackLogPages	RollbackLogPages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatTempTablePages	TempTablePages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatTriggerPages	TriggerPages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatViewPages	ViewPages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatVersionStorePages	VersionStorePages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatSnapshotCount	SnapshotCount
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatLockCount	LockCount
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCacheReadWorkTable	CacheReadWorkTable
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatDiskReadWorkTable	DiskReadWorkTable
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatPrepares	Prepares

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatConnPoolCachedCount	ConnPoolCachedCount
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatConnPoolHits	ConnPoolHits
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatConnPoolMisses	ConnPoolMisses
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHttpConnPoolCachedCount	HttpConnPoolCached-Count
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHttpConnPoolHits	HttpConnPoolHits
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHttpConnPoolMisses	HttpConnPoolMisses
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHttpConnPoolSteals	HttpConnPoolSteals
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatMirrorServerWaits	MirrorServerWaits
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatBytesReceived	BytesReceived
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatBytesReceivedUncomp	BytesReceivedUncomp
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatBytesSent	BytesSent
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatBytesSentUncomp	BytesSentUncomp
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCarverHeapPages	CarverHeapPages
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatClientStmtCacheHits	ClientStmtCacheHits
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatClientStmtCacheMisses	ClientStmtCacheMisses
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCommit	Commit
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCursor	Cursor
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHeapsCarver	HeapsCarver
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHeapsLocked	HeapsLocked
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHeapsQuery	HeapsQuery
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatHeapsRelocatable	HeapsRelocatable
1.3.6.1.4.1.897.2.2.1.n	Integer32	dbStatCursorOpen	CursorOpen
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatPacketsReceived	PacketsReceived
1.3.6.1.4.1.897.2.2.1.n	Counter64	dbStatPacketsReceivedUncomp	PacketsReceivedUncomp

OID	Typ	Name	Statistik
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Counter64	dbStatPacketsSent	PacketsSent
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Counter64	dbStatPacketsSentUncomp	PacketsSentUncomp
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryHeapPages	QueryHeapPages
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemActiveCurr	QueryMemActiveCurr
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemGrantFailed	QueryMemGrantFailed
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemGrantGranted	QueryMemGrantGranted
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemGrantRequested	QueryMemGrantRequested
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemGrantWaited	QueryMemGrantWaited
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatQueryMemGrantWaiting	QueryMemGrantWaiting
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatRequestsReceived	RequestsReceived
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatRlbk	Rlbk
1.3.6.1.4.1.897.2.2.1. <i>n</i>	Integer32	dbStatPrepStmt	PrepStmt

**Siehe auch**

- „Liste der Datenbankservereigenschaften“ auf Seite 745
- „Liste der Datenbankeigenschaften“ auf Seite 767

**SQL Anywhere MIB-Datenbankeigenschaften**

Die folgende Tabelle listet die OIDs und Namen der Datenbankeigenschaften auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgerufen werden können.

Beschreibbare Eigenschaften sind mit einem Stern (\*) gekennzeichnet. Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

**Beschreibungen**

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.1. <i>n</i>	String	dbPropAlias	Alias
1.3.6.1.4.1.897.2.2.2.2. <i>n</i>	String	dbPropAuditingTypes	AuditingTypes
1.3.6.1.4.1.897.2.2.2.3. <i>n</i>	String	dbPropBlankPadding	BlankPadding

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.4.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.5.n	String	dbPropCapabilities	Capabilities
1.3.6.1.4.1.897.2.2.2.6.n	String	dbPropCaseSensitive	CaseSensitive
1.3.6.1.4.1.897.2.2.2.7.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.8.n	String	dbPropCharSet	CharSet
1.3.6.1.4.1.897.2.2.2.9.n	String	dbPropChecksum	Checksum
1.3.6.1.4.1.897.2.2.2.10.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.11.n	String	dbPropCollation	Collation
1.3.6.1.4.1.897.2.2.2.12.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.13.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.14.n	String	dbPropCurrentRedoPos	CurrentRedoPos
1.3.6.1.4.1.897.2.2.2.15.n	String	dbPropDBFileFragments	DBFileFragments
1.3.6.1.4.1.897.2.2.2.16.n	String	dbPropDriveType	DriveType
1.3.6.1.4.1.897.2.2.2.17.n	String	dbPropEncryption	Encryption
1.3.6.1.4.1.897.2.2.2.18.n	String	dbPropFile	File
1.3.6.1.4.1.897.2.2.2.19.n	String	dbPropFileSize	FileSize
1.3.6.1.4.1.897.2.2.2.20.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.21.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.22.n	String	dbPropFreePages	FreePages
1.3.6.1.4.1.897.2.2.2.23.n	String	dbPropGlobalDBID	GlobalDBID
1.3.6.1.4.1.897.2.2.2.24.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.25.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.26.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.27.n	String	dbPropIQStore	IQStore

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.28.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.29.n	String	dbPropLanguage	Language
1.3.6.1.4.1.897.2.2.2.30.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.31.n	String	dbPropLogFileFragments	LogFileFragments
1.3.6.1.4.1.897.2.2.2.32.n	String	dbPropLogMirrorName	LogMirrorName
1.3.6.1.4.1.897.2.2.2.33.n	String	dbPropLogName	LogName
1.3.6.1.4.1.897.2.2.2.34.n	String	dbPropLTMGeneration	LTMGeneration
1.3.6.1.4.1.897.2.2.2.35.n	String	dbPropLTMTrunc	LTMTrunc
1.3.6.1.4.1.897.2.2.2.36.n	String	dbPropMultiByteCharSet	MultiByteCharSet
1.3.6.1.4.1.897.2.2.2.37.n	String	dbPropName	Name
1.3.6.1.4.1.897.2.2.2.38.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.39.n	String	dbPropPageSize	PageSize
1.3.6.1.4.1.897.2.2.2.40.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.41.n	String	dbPropProcedureProfiling*	ProcedureProfiling
1.3.6.1.4.1.897.2.2.2.42.n	String	dbPropReadOnly	ReadOnly
1.3.6.1.4.1.897.2.2.2.43.n	String	dbPropRemoteTrunc	RemoteTrunc
1.3.6.1.4.1.897.2.2.2.44.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.45.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.46.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.47.n	String	dbPropSyncTrunc	SyncTrunc
1.3.6.1.4.1.897.2.2.2.48.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.49.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.50.n	String	dbPropTempFileName	TempFileName
1.3.6.1.4.1.897.2.2.2.51.n	String	dbPropInternal	Internal

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.52.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.53.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.54.n	String	dbPropNextScheduleTime	NextScheduleTime
1.3.6.1.4.1.897.2.2.2.55.n	String	dbPropIdentitySignature	IdentitySignature
1.3.6.1.4.1.897.2.2.2.56.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.57.n	String	dbPropSnapshotIsolationState	SnapshotIsolationState
1.3.6.1.4.1.897.2.2.2.58.n	String	dbPropConnsDisabled	ConnsDisabled
1.3.6.1.4.1.897.2.2.2.59.n	String	dbPropPartnerState	PartnerState
1.3.6.1.4.1.897.2.2.2.60.n	String	dbPropArbiterState	ArbiterState
1.3.6.1.4.1.897.2.2.2.61.n	String	dbPropMirrorState	MirrorState
1.3.6.1.4.1.897.2.2.2.62.n	String	dbPropAlternateServerName	AlternateServerName
1.3.6.1.4.1.897.2.2.2.63.n	String	dbPropEncryptionScope	EncryptionScope
1.3.6.1.4.1.897.2.2.2.64.n	String	dbPropNcharCharSet	NcharCharSet
1.3.6.1.4.1.897.2.2.2.65.n	String	dbPropNcharCollation	NcharCollation
1.3.6.1.4.1.897.2.2.2.66.n	String	dbPropAccentSensitive	AccentSensitive
1.3.6.1.4.1.897.2.2.2.67.n	String	dbPropSendingTracingTo	SendingTracingTo
1.3.6.1.4.1.897.2.2.2.68.n	String	dbPropReceivingTracingFrom	ReceivingTracingFrom
1.3.6.1.4.1.897.2.2.2.69.n	String	dbPropIOParallelism	IOParallelism
1.3.6.1.4.1.897.2.2.2.70.n	String	dbPropJavaVM	JavaVM
1.3.6.1.4.1.897.2.2.2.71.n	String	dbPropDatabaseCleaner	DatabaseCleaner
1.3.6.1.4.1.897.2.2.2.72.n	String	dbPropHasCollationTailoring	HasCollationTailoring
1.3.6.1.4.1.897.2.2.2.73.n	String	dbPropCatalogCollation	CatalogCollation
1.3.6.1.4.1.897.2.2.2.74.n	String	dbPropHasEndianSwapFix	HasEndianSwapFix
1.3.6.1.4.1.897.2.2.2.75.n	String	dbPropAlternateMirrorServerName	AlternateMirrorServerName

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.76.n	String	dbPropOptionWatchList	OptionWatchList
1.3.6.1.4.1.897.2.2.2.77.n	String	dbPropOptionWatchAction	OptionWatchAction
1.3.6.1.4.1.897.2.2.2.78.n	String	dbPropMirrorMode	MirrorMode
1.3.6.1.4.1.897.2.2.2.79.n	String	dbPropHasNCHARLegacyCollationFix	HasNCHARLegacyCollationFix
1.3.6.1.4.1.897.2.2.2.80.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.81.n	String	dbPropAuthenticated	Authenticated
1.3.6.1.4.1.897.2.2.2.82.n	String	dbPropSynchronizationSchemaChangeActive	SynchronizationSchemaChangeActive
1.3.6.1.4.1.897.2.2.2.83.n	String	dbPropLastCheckpointTime	LastCheckpointTime
1.3.6.1.4.1.897.2.2.2.84.n	String	dbPropMirrorServerState	MirrorServerState
1.3.6.1.4.1.897.2.2.2.85.n	String	dbPropDriveBus	DriveBus
1.3.6.1.4.1.897.2.2.2.86.n	String	dbPropDriveModel	DriveModel
1.3.6.1.4.1.897.2.2.2.87.n	String	dbPropInternal	Internal
1.3.6.1.4.1.897.2.2.2.88.n	String	dbPropMirrorRole	MirrorRole
1.3.6.1.4.1.897.2.2.2.89.n	String	dbPropWriteChecksum	WriteChecksum
1.3.6.1.4.1.897.2.2.2.90.n	String	dbPropApproximateCPUTime	ApproximateCPUTime
1.3.6.1.4.1.897.2.2.2.91.n	String	dbPropConnectedTime	ConnectedTime
1.3.6.1.4.1.897.2.2.2.92.n	String	dbPropReqCountUnscheduled	ReqCountUnscheduled
1.3.6.1.4.1.897.2.2.2.93.n	String	dbPropReqCountActive	ReqCountActive
1.3.6.1.4.1.897.2.2.2.94.n	String	dbPropReqCountBlockIO	ReqCountBlockIO
1.3.6.1.4.1.897.2.2.2.95.n	String	dbPropReqCountBlockLock	ReqCountBlockLock
1.3.6.1.4.1.897.2.2.2.96.n	String	dbPropReqCountBlockContention	ReqCountBlockContention
1.3.6.1.4.1.897.2.2.2.97.n	String	dbPropReqTimeUnscheduled	ReqTimeUnscheduled
1.3.6.1.4.1.897.2.2.2.98.n	String	dbPropReqTimeActive	ReqTimeActive

OID	Typ	Name	Eigenschaft
1.3.6.1.4.1.897.2.2.2.99. <i>n</i>	String	dbPropReqTimeBlockIO	ReqTimeBlockIO
1.3.6.1.4.1.897.2.2.2.100. <i>n</i>	String	dbPropReqTimeBlockLock	ReqTimeBlockLock
1.3.6.1.4.1.897.2.2.2.101. <i>n</i>	String	dbPropReqTimeBlockContention	ReqTimeBlockContention
1.3.6.1.4.1.897.2.2.2.102. <i>n</i>	String	dbPropCopyNodeParent	CopyNodeParent
1.3.6.1.4.1.897.2.2.2.103. <i>n</i>	String	dbPropLastCommitRedoPos	LastCommitRedoPos
1.3.6.1.4.1.897.2.2.2.104. <i>n</i>	String	dbPropLastWrittenRedoPos	LastWrittenRedoPos
1.3.6.1.4.1.897.2.2.2.105. <i>n</i>	String	dbPropLastSyncedRedoPos	LastSyncedRedoPos
1.3.6.1.4.1.897.2.2.2.106. <i>n</i>	String	dbPropUTCTimestampCatalog	UTCTimestampCatalog
1.3.6.1.4.1.897.2.2.2.107. <i>n</i>	String	dbPropDiskSandbox	DiskSandbox

**Siehe auch**

- „Liste der Datenbankeigenschaften“ auf Seite 767

**SQL Anywhere MIB-Datenbankoptionen**

Die folgende Tabelle listet die OIDs und Namen der Datenbankoptionen auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgerufen werden können.

Beschreibbare Optionen sind mit einem Stern (\*) gekennzeichnet. Der Wert *n* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

**Beschreibungen**

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.1. <i>n</i>	String	dbOptAllowNullsByDefault*	allow_nulls_by_default
1.3.6.1.4.1.897.2.2.3.2. <i>n</i>	String	dbOptAnsinull*	ansinull

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.3.n	String	dbOptAnsiBlanks*	ansi_blanks
1.3.6.1.4.1.897.2.2.3.4.n	String	dbOptAnsiCloseCursorsOnRollback*	ansi_close_cursors_on_rollback
1.3.6.1.4.1.897.2.2.3.5.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.6.n	String	dbOptAnsiPermissions*	ansi_permissions
1.3.6.1.4.1.897.2.2.3.7.n	String	dbOptAnsiUpdateConstraints*	ansi_update_constraints
1.3.6.1.4.1.897.2.2.3.8.n	String	dbOptAuditing*	auditing
1.3.6.1.4.1.897.2.2.3.9.n	String	dbOptAuditingOptions*	auditing_options
1.3.6.1.4.1.897.2.2.3.10.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.11.n	String	dbOptBackgroundPriority*	background_priority
1.3.6.1.4.1.897.2.2.3.12.n	String	dbOptBlocking*	blocking
1.3.6.1.4.1.897.2.2.3.13.n	Integer32	dbOptBlockingTimeout*	blocking_timeout
1.3.6.1.4.1.897.2.2.3.14.n	String	dbOptChained*	chained
1.3.6.1.4.1.897.2.2.3.15.n	Integer32	dbOptCheckpointTime*	checkpoint_time
1.3.6.1.4.1.897.2.2.3.16.n	Integer32	dbOptCisOption*	cis_option
1.3.6.1.4.1.897.2.2.3.17.n	Integer32	dbOptCisRowsetSize*	cis_rowset_size
1.3.6.1.4.1.897.2.2.3.18.n	String	dbOptCloseOnEndtrans*	close_on_endtrans
1.3.6.1.4.1.897.2.2.3.19.n	String	dbOptConnectionAuthentication*	connection_authentication
1.3.6.1.4.1.897.2.2.3.20.n	String	dbOptContinueAfterRaiseError*	continue_after_raiseerror
1.3.6.1.4.1.897.2.2.3.21.n	String	dbOptConversionError*	conversion_error
1.3.6.1.4.1.897.2.2.3.22.n	String	dbOptCooperativeCommits*	cooperative_commits

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.23.n	Integer32	dbOptCooperativeCommitTimeout*	cooperative_commit_timeout
1.3.6.1.4.1.897.2.2.3.24.n	String	dbOptDatabaseAuthentication*	database_authentication
1.3.6.1.4.1.897.2.2.3.25.n	String	dbOptDateFormat*	date_format
1.3.6.1.4.1.897.2.2.3.26.n	String	dbOptDateOrder*	date_order
1.3.6.1.4.1.897.2.2.3.27.n	String	dbOptDebugMessages*	debug_messages
1.3.6.1.4.1.897.2.2.3.28.n	String	dbOptDedicatedTask*	dedicated_task
1.3.6.1.4.1.897.2.2.3.29.n	Integer32	dbOptDefaultTimestampIncrement*	default_timestamp_increment
1.3.6.1.4.1.897.2.2.3.30.n	String	dbOptDelayedCommits*	delayed_commits
1.3.6.1.4.1.897.2.2.3.31.n	Integer32	dbOptDelayedCommitTimeout*	delayed_commit_timeout
1.3.6.1.4.1.897.2.2.3.32.n	String	dbOptDivideByZeroError*	divide_by_zero_error
1.3.6.1.4.1.897.2.2.3.33.n	String	dbOptEscapeCharacter*	escape_character
1.3.6.1.4.1.897.2.2.3.34.n	String	dbOptExcludeOperators*	exclude_operators
1.3.6.1.4.1.897.2.2.3.35.n	String	dbOptExtendedJoinSyntax*	extended_join_syntax
1.3.6.1.4.1.897.2.2.3.36.n	String	dbOptFireTriggers*	fire_triggers
1.3.6.1.4.1.897.2.2.3.37.n	Integer32	dbOptFirstDayOfWeek*	first_day_of_week
1.3.6.1.4.1.897.2.2.3.38.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.39.n	String	dbOptForceViewCreation*	force_view_creation
1.3.6.1.4.1.897.2.2.3.40.n	String	dbOptForXmlNullTreatment*	for_xml_null_treatment
1.3.6.1.4.1.897.2.2.3.41.n	Integer32	dbOptGlobalDatabaseId*	global_database_id
1.3.6.1.4.1.897.2.2.3.42.n	Integer32	dbOptIsolationLevel*	isolation_level

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.43.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.44.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.45.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.46.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.47.n	String	dbOptLockRejected-Rows*	lock_rejected_rows
1.3.6.1.4.1.897.2.2.3.48.n	String	dbOptLoginMode*	login_mode
1.3.6.1.4.1.897.2.2.3.49.n	String	dbOptLoginProcedure*	login_procedure
1.3.6.1.4.1.897.2.2.3.50.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.51.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.52.n	Integer32	dbOptMaxCursorCount*	max_cursor_count
1.3.6.1.4.1.897.2.2.3.53.n	Integer32	dbOptMaxHashSize*	max_hash_size
1.3.6.1.4.1.897.2.2.3.54.n	Integer32	dbOptMaxPlansCached*	max_plans_cached
1.3.6.1.4.1.897.2.2.3.55.n	Integer32	dbOptMaxRecursiveIterations*	max_recursive_iterations
1.3.6.1.4.1.897.2.2.3.56.n	Integer32	dbOptMaxStatement-Count*	max_statement_count
1.3.6.1.4.1.897.2.2.3.57.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.58.n	Integer32	dbOptMinPassword-Length*	min_password_length
1.3.6.1.4.1.897.2.2.3.59.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.60.n	Integer32	dbOptNearestCentury*	nearest_century
1.3.6.1.4.1.897.2.2.3.61.n	String	dbOptNonKeywords*	non_keywords
1.3.6.1.4.1.897.2.2.3.62.n	String	dbOptOdbcDistinguish-CharAndVarchar*	odbc_distinguish_char_and_varchar
1.3.6.1.4.1.897.2.2.3.63.n	String	dbOptOnCharsetConversionFailure*	on_charset_conversion_failure

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.64.n	String	dbOptOnTsqlError*	on_tsql_error
1.3.6.1.4.1.897.2.2.3.65.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.66.n	String	dbOptOptimizationGoal*	optimization_goal
1.3.6.1.4.1.897.2.2.3.67.n	Integer32	dbOptOptimizationLevel*	optimization_level
1.3.6.1.4.1.897.2.2.3.68.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.69.n	String	dbOptOptimizationWorkload*	optimization_workload
1.3.6.1.4.1.897.2.2.3.70.n	Integer32	dbOptPinnedCursorPercentOfCache*	pinned_cursor_percent_of_cache
1.3.6.1.4.1.897.2.2.3.71.n	Integer32	dbOptPrecision*	precision
1.3.6.1.4.1.897.2.2.3.72.n	String	dbOptPrefetch*	prefetch
1.3.6.1.4.1.897.2.2.3.73.n	String	dbOptPreserveSourceFormat*	preserve_source_format
1.3.6.1.4.1.897.2.2.3.74.n	String	dbOptPreventArticlePrimaryKeyUpdate*	prevent_article_pkey_update
1.3.6.1.4.1.897.2.2.3.75.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.76.n	String	dbOptQuotedIdentifier*	quoted_identifier
1.3.6.1.4.1.897.2.2.3.77.n	String	dbOptReadPastDeleted*	read_past_deleted
1.3.6.1.4.1.897.2.2.3.78.n	Integer32	dbOptRecoveryTime*	recovery_time
1.3.6.1.4.1.897.2.2.3.79.n	String	dbOptReplicateAll*	replicate_all
1.3.6.1.4.1.897.2.2.3.80.n	String	dbOptReturnDateTimeAsString*	return_date_time_as_string
1.3.6.1.4.1.897.2.2.3.81.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.82.n	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.83.n	String	dbOptRowCounts*	row_counts
1.3.6.1.4.1.897.2.2.3.84.n	Integer32	dbOptScale*	scale

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.85. <i>n</i>	String	dbOptSortCollation*	sort_collation
1.3.6.1.4.1.897.2.2.3.86. <i>n</i>	String	dbOptSqlFlaggerErrorLevel*	sql_flagger_error_level
1.3.6.1.4.1.897.2.2.3.87. <i>n</i>	String	dbOptSqlFlaggerWarningLevel*	sql_flagger_warning_level
1.3.6.1.4.1.897.2.2.3.88. <i>n</i>	String	dbOptStringRtruncation*	string_rtruncation
1.3.6.1.4.1.897.2.2.3.89. <i>n</i>	String	dbOptSubsumeRowLocks*	subsume_row_locks
1.3.6.1.4.1.897.2.2.3.90. <i>n</i>	String	dbOptSuppressTdsDebugging*	suppress_tds_debugging
1.3.6.1.4.1.897.2.2.3.91. <i>n</i>	String	dbOptTdsEmptyStringIsNull*	tds_empty_string_is_null
1.3.6.1.4.1.897.2.2.3.92. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.93. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.94. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.95. <i>n</i>	String	dbOptTimestampFormat*	timestamp_format
1.3.6.1.4.1.897.2.2.3.96. <i>n</i>	String	dbOptTimeFormat*	time_format
1.3.6.1.4.1.897.2.2.3.97. <i>n</i>	Integer32	dbOptTimeZoneAdjustment*	time_zone_adjustment
1.3.6.1.4.1.897.2.2.3.98. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.99. <i>n</i>	String	dbOptTruncateTimestampValues*	truncate_timestamp_values
1.3.6.1.4.1.897.2.2.3.100. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.101. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.102. <i>n</i>	String	dbOptTsqlVariables*	tsql_variables

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.103. <i>n</i>	String	dbOptUpdateStatistics*	update_statistics
1.3.6.1.4.1.897.2.2.3.104. <i>n</i>	String	dbOptUpgradeDatabase-Capability*	upgrade_database_capability
1.3.6.1.4.1.897.2.2.3.105. <i>n</i>	String	dbOptUserEstimates*	user_estimates
1.3.6.1.4.1.897.2.2.3.106. <i>n</i>	String	dbOptWaitForCommit*	wait_for_commit
1.3.6.1.4.1.897.2.2.3.107. <i>n</i>	String	dbOptTempSpaceLimit-Check*	temp_space_limit_check
1.3.6.1.4.1.897.2.2.3.108. <i>n</i>	Integer32	dbOptRemoteIdleTimeout*	remote_idle_timeout
1.3.6.1.4.1.897.2.2.3.109. <i>n</i>	String	dbOptAnsiSubstring*	ansi_substring
1.3.6.1.4.1.897.2.2.3.110. <i>n</i>	String	dbOptOdbcDescribeBinaryAsVarbinary*	odbc_describe_binary_as_varbinary
1.3.6.1.4.1.897.2.2.3.111. <i>n</i>	String	dbOptRollbackOnDeadlock*	rollback_on_deadlock
1.3.6.1.4.1.897.2.2.3.112. <i>n</i>	String	dbOptIntegratedServer-Name*	integrated_server_name
1.3.6.1.4.1.897.2.2.3.113. <i>n</i>	String	dbOptLogDeadlocks*	log_deadlocks
1.3.6.1.4.1.897.2.2.3.114. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.115. <i>n</i>	String	dbOptWebserviceNamespaceHost*	webservice_namespace_host
1.3.6.1.4.1.897.2.2.3.116. <i>n</i>	Integer32	dbOptMaxQueryTasks*	max_query_tasks
1.3.6.1.4.1.897.2.2.3.117. <i>n</i>	Integer32	dbOptRequestTimeout*	request_timeout
1.3.6.1.4.1.897.2.2.3.118. <i>n</i>	String	dbOptSynchronizeMirrorOnCommit*	synchronize_mirror_on_commit

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.119. <i>n</i>	Integer32	dbOptHttpSessionTimeout*	http_session_timeout
1.3.6.1.4.1.897.2.2.3.120. <i>n</i>	String	dbOptUuidHasHyphens*	uuid_has_hyphens
1.3.6.1.4.1.897.2.2.3.121. <i>n</i>	String	dbOptAllowSnapshotIsolation*	allow_snapshot_isolation
1.3.6.1.4.1.897.2.2.3.122. <i>n</i>	String	dbOptVerifyPasswordFunction*	verify_password_function
1.3.6.1.4.1.897.2.2.3.123. <i>n</i>	String	dbOptDefaultDbSpace*	default_dbspace
1.3.6.1.4.1.897.2.2.3.124. <i>n</i>	String	dbOptCollectStatisticsOnDmlUpdates*	collect_statistics_on_dml_updates
1.3.6.1.4.1.897.2.2.3.125. <i>n</i>	String	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.126. <i>n</i>	String	dbOptJavaLocation*	java_location
1.3.6.1.4.1.897.2.2.3.127. <i>n</i>	String	dbOptOemString*	oem_string
1.3.6.1.4.1.897.2.2.3.128. <i>n</i>	Integer32	dbOptMaxTempSpace*	max_temp_space
1.3.6.1.4.1.897.2.2.3.129. <i>n</i>	String	dbOptSecureFeatureKey*	secure_feature_key
1.3.6.1.4.1.897.2.2.3.130. <i>n</i>	String	dbOptMaterializedViewOptimization*	materialized_view_optimization
1.3.6.1.4.1.897.2.2.3.131. <i>n</i>	Integer32	dbOptUpdatableStatementIsolation*	updatable_statement_isolation
1.3.6.1.4.1.897.2.2.3.132. <i>n</i>	String	dbOptTsqlOuterJoins*	tsql_outer_joins
1.3.6.1.4.1.897.2.2.3.133. <i>n</i>	String	dbOptPostLoginProcedure*	post_login_procedure
1.3.6.1.4.1.897.2.2.3.134. <i>n</i>	String	dbOptConnAuditing*	conn_auditing

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.135. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.136. <i>n</i>	String	dbOptJavaVmOptions*	java_vm_options
1.3.6.1.4.1.897.2.2.3.137. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.138. <i>n</i>	Integer32	dbOptMaxClientState- mentsCached*	max_client_statements_cached
1.3.6.1.4.1.897.2.2.3.139. <i>n</i>	String	dbOptQueryMemTi- meout*	query_mem_timeout
1.3.6.1.4.1.897.2.2.3.140. <i>n</i>	String	dbOptAllowReadClient- File*	allow_read_client_file
1.3.6.1.4.1.897.2.2.3.141. <i>n</i>	String	dbOptAllowWriteClient- File*	allow_write_client_file
1.3.6.1.4.1.897.2.2.3.142. <i>n</i>	String	dbOptPriority*	priority
1.3.6.1.4.1.897.2.2.3.143. <i>n</i>	String	dbOptMaxPriority*	max_priority
1.3.6.1.4.1.897.2.2.3.144. <i>n</i>	String	dbOptProgressMessages*	progress_messages
1.3.6.1.4.1.897.2.2.3.145. <i>n</i>	Integer32	dbOptBlockingOthersTi- meout*	blocking_others_timeout
1.3.6.1.4.1.897.2.2.3.146. <i>n</i>	Integer32	dbOptInternal	Internal
1.3.6.1.4.1.897.2.2.3.147. <i>n</i>	String	dbOptTimestampWithTi- meZoneFormat*	timestamp_with_time_zone_for- mat
1.3.6.1.4.1.897.2.2.3.148. <i>n</i>	Integer32	dbOptHttpConnection- PoolTimeout*	http_connection_pool_timeout
1.3.6.1.4.1.897.2.2.3.149. <i>n</i>	Integer32	dbOptHttpConnection- PoolBasesize*	http_connection_pool_basesize
1.3.6.1.4.1.897.2.2.3.150. <i>n</i>	String	dbOptStGeometryDescri- beType*	st_geometry_describe_type

OID	Typ	Name	Option
1.3.6.1.4.1.897.2.2.3.151. <i>n</i>	String	dbOptStGeometryAtext- Format*	st_geometry_astext_format
1.3.6.1.4.1.897.2.2.3.152. <i>n</i>	String	dbOptStGeometryAsbi- naryFormat*	st_geometry_asbinary_format
1.3.6.1.4.1.897.2.2.3.153. <i>n</i>	String	dbOptStGeometryAsxml- Format*	st_geometry_asxml_format
1.3.6.1.4.1.897.2.2.3.154. <i>n</i>	String	dbOptReservedKey- words*	reserved_keywords
1.3.6.1.4.1.897.2.2.3.155. <i>n</i>	String	dbOptStGeometryOnIn- valid*	st_geometry_on_invalid
1.3.6.1.4.1.897.2.2.3.156. <i>n</i>	Integer32	dbOptMinRoleAdmins*	min_role_admins
1.3.6.1.4.1.897.2.2.3.157. <i>n</i>	String	dbOptTrustedCertifica- tesFile*	trusted_certificates_file
1.3.6.1.4.1.897.2.2.3.158. <i>n</i>	String	dbOptJavaClassPath*	java_class_path
1.3.6.1.4.1.897.2.2.3.159. <i>n</i>	String	dbOptStGeometryInter- polation*	st_geometry_interpolation
1.3.6.1.4.1.897.2.2.3.160. <i>n</i>	String	dbOptExternLoginCre- dentials*	extern_login_credentials
1.3.6.1.4.1.897.2.2.3.161. <i>n</i>	String	dbOptWebserviceSessio- nidName*	webservice_sessionid_name
1.3.6.1.4.1.897.2.2.3.162. <i>n</i>	String	dbOptDbPublisher*	db_publisher
1.3.6.1.4.1.897.2.2.3.163. <i>n</i>	String	dbOptAutoCommitOnC- reateLocalTempIndex*	auto_commit_on_crea- te_local_temp_index
1.3.6.1.4.1.897.2.2.3.164. <i>n</i>	String	dbOptDiskSandbox*	disk_sandbox
1.3.6.1.4.1.897.2.2.3.165. <i>n</i>	String	dbOptBaseTablesInRlv- Store*	base_tables_in_rlv_store

**Siehe auch**

- „Alphabetische Liste der Datenbankoptionen“ auf Seite 572

## RDBMS MIB-Referenz

Die folgenden Abschnitte listen die OIDs der Werte auf, die mit dem SQL Anywhere SNMP-Erweiterungsagenten abgefragt werden können. Standardmäßig befindet sich die RDBMS MIB im Verzeichnis *C:\Program Files\SQL Anywhere 16\snmp\RDBMS-MIB.mib*.

### rdbmsDbTable

Diese Tabelle listet Informationen über die Datenbanken auf, die in einem System installiert sind.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.1.1.1. <i>db</i>	Integer	rdbmsDbIndex	<i>db</i>
1.3.6.1.2.1.39.1.1.1.2. <i>db</i>	OID	rdbmsDbPrivateMibOID	1.3.6.1.4.1.897.2
1.3.6.1.2.1.39.1.1.1.3. <i>db</i>	String	rdbmsDbVendorName	PROPERTY( 'CompanyNa-me' )
1.3.6.1.2.1.39.1.1.1.4. <i>db</i>	String	rdbmsDbName	DB_PROPERTY( 'Name' )
1.3.6.1.2.1.39.1.1.1.5. <i>db</i>	String	rdbmsDbContact	PROPERTY( 'LicensedUser' )

### rdbmsDbInfoTable

Diese Tabelle enthält weitere Informationen über die Datenbanken im System.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.2.1.1. <i>db</i>	String	rdbmsDbInfoProduct-Name	PROPERTY("ProductName")
1.3.6.1.2.1.39.1.2.1.2. <i>db</i>	String	rdbmsDbInfoVersion	PROPERTY("ProductVersion")

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.2.1.3.db	Integer	rdbsmsDbInfoSizeUnits	Berechnet basierend auf dbInfoSizeAllocated und dbInfoSizeUsed.  <ul style="list-style-type: none"> <li>• 1=Byte</li> <li>• 2=kB</li> <li>• 3=MB</li> <li>• 4=GB</li> <li>• 5=TByte</li> </ul> (Jede Einheit ist 1024 Mal größer als die vorherige.)
1.3.6.1.2.1.39.1.2.1.4.db	Integer	rdbsmsDbInfoSizeAllocated	DB_PROPERTY("PageSize") * DB_PROPERTY("FileSize")
1.3.6.1.2.1.39.1.2.1.5.db	Integer	rdbsmsDbInfoSizeUsed	DB_PROPERTY("PageSize") * (DB_PROPERTY("FileSize") - DB_PROPERTY("FreePages"))
1.3.6.1.2.1.39.1.2.1.6.db	String	rdbsmsDbInfoLastBackup	NULL <sup>1</sup>

<sup>1</sup> Diese OID wird vom SQL Anywhere SNMP-Erweiterungsagenten nicht unterstützt.

## rdbsmsDbParamTable

Diese Tabelle listet die Konfigurationsparameter für die Datenbanken im System auf.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini* und *n* ist der Index der Option in der Unterstruktur *sa.2.3*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.3.1.1.db	String	rdbsmsDbParamName	Name der Option
1.3.6.1.2.1.39.1.3.1.2.db	Integer	rdbsmsDbParamSubIndex	<i>n</i>
1.3.6.1.2.1.39.1.3.1.3.db	OID	rdbsmsDbParamID	OID in SQL Anywhere MIB-Datenbank, die dieser Option entspricht
1.3.6.1.2.1.39.1.3.1.4.db	String	rdbsmsDbParamCurrValue	Optionswert

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.3.1.5. <i>db</i>	String	rdbmsDbParamComment	NULL <sup>1</sup>

<sup>1</sup> Diese OID wird vom SQL Anywhere SNMP-Erweiterungsagenten nicht unterstützt.

## rdbmsDbLimitedResourceTable

In dieser Tabelle werden Informationen über freien Speicherplatz in jedem DBSpace aufgelistet. Der Wert *n* stellt dabei jeden DBSpace folgendermaßen dar:

- 1-13 sind normale DBSpaces (in der Datenbank nummeriert mit 0-12)
- 14 ist die Transaktionslogdatei.
- 15 ist die Transaktionslog-Spiegeldatei.
- 16 ist die temporäre Datei.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.4.1.1. <i>n.db</i>	String	rdbmsDbLimitedResource-Name	Name des DBSpaces, des Transaktionslogs, des Transaktionslogspiegels oder der temporären Datei
1.3.6.1.2.1.39.1.4.1.2. <i>n.db</i>	OID	rdbmsDbLimitedResourceID	1.3.6.1.4.1.897.2
1.3.6.1.2.1.39.1.4.1.3. <i>n.db</i>	Integer	rdbmsDbLimitedResource-Limit	Auf der Festplatte verfügbarer Speicherplatz + aktuelle Dateigröße
1.3.6.1.2.1.39.1.4.1.4. <i>n.db</i>	Integer	rdbmsDbLimitedResource-Current	Aktuelle Dateigröße
1.3.6.1.2.1.39.1.4.1.5. <i>n.db</i>	Integer	rdbmsDbLimitedResource-Highwater	Aktuelle Größe
1.3.6.1.2.1.39.1.4.1.6. <i>n.db</i>	Integer	rdbmsDbLimitedResource-Failure	0 <sup>1</sup>
1.3.6.1.2.1.39.1.4.1.7. <i>n.db</i>	String	rdbmsDbLimitedResource-Description	Byte, kB, MB, GB oder TByte

<sup>1</sup> Diese OID wird vom SQL Anywhere SNMP-Erweiterungsagenten nicht unterstützt.

## rdbmsSrvTable

Diese Tabelle listet die im System laufenden oder installierten Datenbankserver auf.

Der Wert *db* ist die Datenbanknummer in der Datei *sasmp.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.5.1.1. <i>db</i>	OID	rdbmsSrvPrivateMibOID	1.3.6.1.4.1.897.2
1.3.6.1.2.1.39.1.5.1.2. <i>db</i>	String	rdbmsSrvVendorName	PROPERTY( 'CompanyName' )
1.3.6.1.2.1.39.1.5.1.3. <i>db</i>	String	rdbmsSrvProductName	PROPERTY( 'ProductName' )
1.3.6.1.2.1.39.1.5.1.4. <i>db</i>	String	rdbmsSrvContact	PROPERTY( 'LicensedCompany' )

## rdbmsSrvInfoTable

Diese Tabelle enthält weitere Informationen über die Datenbankserver im System.

Der Wert *db* ist die Datenbanknummer in der Datei *sasmp.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.6.1.1. <i>db</i>	Integer	rdbmsSrvInfoStartupTime	PROPERTY( 'StartTime' )
1.3.6.1.2.1.39.1.6.1.2. <i>db</i>	Integer	rdbmsSrvInfoFinishedTransactions	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.3. <i>db</i>	Integer	rdbmsSrvInfoDiskReads	PROPERTY( 'DiskReadEng' )
1.3.6.1.2.1.39.1.6.1.4. <i>db</i>	Integer	rdbmsSrvInfoLogicalReads	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.5. <i>db</i>	Integer	rdbmsSrvInfoDiskWrites	PROPERTY( 'DiskWriteEng' )
1.3.6.1.2.1.39.1.6.1.6. <i>db</i>	Integer	rdbmsSrvInfoLogicalWrites	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.7. <i>db</i>	Integer	rdbmsSrvInfoPageReads	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.8. <i>db</i>	Integer	rdbmsSrvInfoPageDiskOutOfWrites	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.9. <i>db</i>	Integer	rdbmsSrvInfoSpaces	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.10. <i>db</i>	Integer	rdbmsSrvInfoHandledRequests	PROPERTY( 'Req' )

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.6.1.11.db	Integer	rdbmsSrvInfoRequestRecvs	PROPERTY( 'Packets-ReceivedUncomp' )
1.3.6.1.2.1.39.1.6.1.12.db	Integer	rdbmsSrvInfoRequestSends	PROPERTY( 'Packets-SentUncomp' )
1.3.6.1.2.1.39.1.6.1.13.db	Integer	rdbmsSrvInfoHighwaterInboundAssociations	0 <sup>1</sup>
1.3.6.1.2.1.39.1.6.1.14.db	Integer	rdbmsSrvInfoMaxInboundAssociations	0 <sup>1</sup>

<sup>1</sup> Diese OID wird vom SQL Anywhere SNMP-Erweiterungsagenten nicht unterstützt.

## rdbmsSrvParamTable

In dieser Tabelle werden die Serveroptionen aufgelistet, die vom SQL Anywhere SNMP-Erweiterungsagenten über die SQL Anywhere MIB-Datenbank festgelegt werden können. *n* ist dabei der Index:

<i>n</i>	Serveroption
1	ConnsDisabled
2	LivenessTimeout (Standardwert)
3	QuittingTime
4	RememberLastStatement
5	RequestLogFile
6	RequestLogging

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmplib.ini*.

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.7.1.1.n.db	String	rdbmsDbSrvParamName	Name der Option <i>n</i>
1.3.6.1.2.1.39.1.7.1.2.n.db	Integer	rdbmsDbSrvParamSubIndex	<i>n</i>
1.3.6.1.2.1.39.1.7.1.3.n.db	OID	rdbmsDbSrvParamID	1.3.6.1.4.1.897.2

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.7.1.4. <i>n.db</i>	String	rdbsDbSrvParamCurrValue	Aktueller Wert der Option <i>n</i>
1.3.6.1.2.1.39.1.7.1.5. <i>n.db</i>	String	rdbsDbSrvParamComment	Vollständiger Name der Option <i>n</i>

## rdbsSrvLimitedResourceTable

Diese Tabelle enthält Informationen über Parameter für die Serverkonfiguration.

Der Wert *db* ist die Datenbanknummer in der Datei *sasnmp.ini* und *n* ist der Index der Ressource, der folgende Werte haben kann:

<i>n</i>	Name	Ressource	Ressourcengrenze
1	Connections	PROPERTY( "UniqueClientAddresses" )	PROPERTY("LicenseCount")
2	Processors	PROPERTY("NumLogicalProcessorsUsed")	PROPERTY("NumLogicalProcessorsUsed")

OID	Typ	Name	Zurückgegebener Wert
1.3.6.1.2.1.39.1.8.1.1. <i>db</i>	String	rdbsSrvLimitedResourceName	Name der Ressource <i>n</i>
1.3.6.1.2.1.39.1.8.1.2. <i>db</i>	OID	rdbsSrvLimitedResourceID	OID in SQL Anywhere MIB-Datenbank, die dieser Option entspricht
1.3.6.1.2.1.39.1.8.1.3. <i>db</i>	Integer	rdbsSrvLimitedResourceLimit	Obergrenze der Ressource <i>n</i>
1.3.6.1.2.1.39.1.8.1.4. <i>db</i>	Integer	rdbsSrvLimitedResourceCurrent	Aktueller Wert der Ressource <i>n</i>
1.3.6.1.2.1.39.1.8.1.5. <i>db</i>	Integer	rdbsSrvLimitedResourceHighwater	Aktueller Wert der Ressource <i>n</i>
1.3.6.1.2.1.39.1.8.1.6. <i>db</i>	Integer	rdbsSrvLimitedResourceFailures	0 <sup>1</sup>
1.3.6.1.2.1.39.1.8.1.7. <i>db</i>	String	rdbsSrvLimitedResourceDescription	Name der Ressource <i>n</i>

<sup>1</sup> Diese OID wird vom SQL Anywhere SNMP-Erweiterungsagenten nicht unterstützt.



---

# Benutzer- und Datenbanksicherheit

Dieser Abschnitt beschreibt Sicherheitsfunktionen in SQL Anywhere.

## Benutzersicherheit (Rollen und Privilegien)

SQL Anywhere bietet ein **rollenbasiertes Zugriffssteuerungsmodell** für die Ausführung von mit Privilegien verbundenen Vorgängen. Ein rollenbasiertes Zugriffssteuerungsmodell ermöglicht vollständige Kontrolle und Granularität für die Privilegien, die Sie Benutzern erteilen möchten. Jeder mit Privilegien verbundene Vorgang, den ein Benutzer in der Datenbank ausführen kann, erfordert ein oder mehrere Systemprivilegien oder Privilegien auf Objektebene.

Ein **Systemprivileg** ist ein Recht, eine autorisierte Datenbankaufgabe auszuführen. Mit dem CREATE TABLE-Systemprivileg kann ein Benutzer beispielsweise im eigenen Eigentum stehende Tabellen erstellen.

Ein **Privileg auf Objektebene** ist ein Recht, eine autorisierte Aufgabe für ein angegebenes Objekt auszuführen. Mit ALTER-Privilegien für eine bestimmte Tabelle kann ein Benutzer beispielsweise diese Tabelle ändern, jedoch keine anderen Tabellen.

Eine **Rolle** ist eine Sammlung aus Systemprivilegien, Privilegien auf Objektebene oder anderen Rollen. Sie können Rollen anderen Rollen erteilen, um eine Rollenhierarchie zu erstellen. Wenn einem Benutzer eine Rolle erteilt wird, entspricht dies dem Erteilen aller der Rolle zugrunde liegenden Systemprivilegien.

Jede neue oder migrierte SQL Anywhere-Datenbank enthält vordefinierte Rollen, die Sie für Ihre ersten Schritte nutzen können. Diese Systemrollen dienen als Ausgangspunkt für die Implementierung der rollenbasierten Sicherheit.

### Hinweis

Wenn Sie schon vor Version 16.0 SQL Anywhere-Kunde waren, sollten Sie sich diese Abschnitte durchlesen, in denen beschrieben wird, wie das Sicherheitsmodell vom Modell Berechtigung/Gruppe zum Modell Rolle/Privileg/benutzererweiterte Rolle geändert hat: „[Upgrade auf rollenbasierte Sicherheit](#)“ auf Seite 1385.

### Siehe auch

- „[Rollen](#)“ auf Seite 1271

## Rollen

Im rollenbasierten Sicherheitsmodell gibt es drei Arten von Rollen: **Systemrollen**, **benutzerdefinierte Rollen** (einschließlich der benutzererweiterten Rollen) und **Kompatibilitätsrollen**.

Sie können die Rollen und Privilegien, die ein Benutzer hat, in Sybase Central anzeigen, indem Sie auf den Benutzer klicken und die angezeigten Details durchgehen. Sie können die Details auch mit der sp\_displayroles-Systemprozedur abrufen. Siehe „[sp\\_displayroles-Systemprozedur](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

**Siehe auch**

- [„Upgrade auf rollenbasierte Sicherheit“ auf Seite 1385](#)

## Systemrollen

Systemrollen sind permanente Rollen, die in jede neue Datenbank integriert werden. Sie enthalten in der Regel die Privilegien, die für komplexere Vorgänge erforderlich sind. Die folgenden Punkte sind bei Systemrollen zu beachten:

- Systemrollen können Sie nicht löschen.
- Sie können beim Erteilen von Systemrollen keine Administrationsrechte (WITH ADMIN OPTION oder WITH ADMIN ONLY OPTION) erteilen. Administrationsrechte für diese Systemrollen liegen ausschließlich beim MANAGE ROLES-Systemprivileg.
- Wenn eine Systemrolle einer benutzererweiterten Rolle erteilt wird, erben Benutzer, denen die benutzererweiterte Rolle erteilt wird, auch die Systemrolle.
- Mit Ausnahme der SYS-Rolle können Sie einer Systemrolle zusätzliche Privilegien und Rollen erteilen und entziehen, sofern Sie Administrationsrechte für die zu erteilenden bzw. zu entziehenden Privilegien und Rollen haben.
- Mit Ausnahme der Rollen SYS, dbo und rs\_systabgroup sind Systemrollen keine Eigentümerinnen von Objekten.

Systemrolle	Beschreibung
DBO	Diese Rolle ist Eigentümerin vieler gespeicherter Systemprozeduren und -ansichten sowie der für UltraLite und MobiLink verwendeten Tabellen. Sie ist Berechtigungsempfängerin der SYS-Rolle. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.
DIAGNOSTICS	Diese Rolle erteilt die Privilegien SELECT, INSERT, UPDATE, DELETE und ALTER für Diagnosetabellen und -ansichten. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.
PUBLIC	Diese Rolle hat das SELECT-Privileg für die Systemtabellen. Die Rolle PUBLIC ist außerdem Berechtigungsempfängerin der Rollen SYS und DBO und hat Schreibzugriff auf einige der Systemtabellen und -ansichten, damit Benutzer Informationen zum Datenbankschema ermitteln können.
rs_systabgroup	Diese Rolle ist Eigentümerin der Tabellen und Systemprozeduren, die für Replication Server erforderlich sind. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.

Systemrolle	Beschreibung
SA_DEBUG	Diese Rolle ist für den SQL Anywhere-Debugger erforderlich. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.
SYS	Diese Rolle ist Eigentümerin des Katalogs, der die vollständige Beschreibung des Datenbankschemas einschließlich aller Datenbankobjekte und aller Benutzer-IDs enthält. Sie können dieser Rolle keine zusätzlichen Privilegien erteilen oder entziehen. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.
SYS_REPLICATION_ADMIN_ROLE	Diese Rolle ist zum Ausführen von Administrationsaufgaben im Zusammenhang mit der Replikation erforderlich, z.B. Erteilen von Replikationsrollen, Verwalten von Publikationen, Subskriptionen, Synchronisationsbenutzern und Profilen, Verwalten von Nachrichtentypen, Festlegen von Optionen für die Replikation usw. Nur Benutzer mit dem MANAGE REPLICATION-Systemprivileg können diese Rolle verwalten. Siehe <a href="#">„Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273</a> .
SYS_RUN_REPLICATION_ROLE	Diese Rolle ist für die Replikation mithilfe des Dienstprogramms dbremote und für die Synchronisation mithilfe des Dienstprogramms dbmlsync erforderlich. Nur Benutzer mit der SYS_REPLICATION_ADMIN_ROLE-Systemrolle können diese Rolle verwalten.  Siehe <a href="#">„Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273</a> .
SYS_SAMONITOR_ADMIN_ROLE	Diese Rolle ist für den SQL Anywhere-Monitor erforderlich.
SYS_SPATIAL_ADMIN_ROLE	Diese Rolle ermöglicht es Benutzern, räumliche Bezugssysteme und räumliche Maßeinheiten zu erstellen, zu ändern oder zu löschen. Nur Benutzer mit dem MANAGE ROLES-Systemprivileg können diese Rolle verwalten.

**Siehe auch**

- [„Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273](#)

**Systemrollen im Zusammenhang mit der Replikation**

Es gibt zwei Systemrollen im Zusammenhang mit der Replikation: SYS\_RUN\_REPLICATION\_ROLE und SYS\_REPLICATION\_ADMIN\_ROLE.

Die Systemrolle **SYS\_RUN\_REPLICATION\_ROLE** ist für die Replikation mithilfe des Dienstprogramms dbremote und für die Synchronisation mithilfe des Dienstprogramms dbmlsync erforderlich. **SYS\_RUN\_REPLICATION\_ROLE** werden die folgenden Systemprivilegien erteilt:

- MONITOR
- BACKUP DATABASE
- DROP CONNECTION
- SELECT ANY TABLE
- SET ANY SYSTEM OPTION
- SET ANY USER DEFINED OPTION

Neben den mit den oben genannten Privilegien verbundenen Anweisungen können Benutzer mit der **SYS\_RUN\_REPLICATION\_ROLE**-Systemrolle auch die folgende Anweisung ausführen:

- SYNCHRONIZE PROFILE-Anweisung

Die Systemrolle **SYS\_REPLICATION\_ADMIN\_ROLE** ist zum Ausführen von Administrationsaufgaben im Zusammenhang mit der Replikation erforderlich, z.B. Erteilen von Replikationsrollen, Verwalten von Publikationen, Subskriptionen, Synchronisationsbenutzern und Profilen, Verwalten von Nachrichtentypen, Festlegen von Optionen für die Replikation usw. **SYS\_REPLICATION\_ADMIN\_ROLE** werden die folgenden Systemprivilegien erteilt:

- MANAGE REPLICATION
- SET ANY SYSTEM OPTION
- SET ANY PUBLIC OPTION
- SET ANY USER DEFINED OPTION
- SELECT ANY TABLE
- CREATE ANY PROCEDURE
- DROP ANY PROCEDURE
- MANAGE ANY WEB SERVICE
- CREATE ANY TABLE
- DROP ANY TABLE
- SERVER OPERATOR
- MANAGE ANY USER
- MANAGE ROLES
- MANAGE ANY OBJECT PRIVILEGE

Dies sind die minimalen (und unwiderruflichen) Privilegien, die für diese beiden Rollen erforderlich sind. Sie können jedoch auch zusätzliche Berechtigungen erteilen.

Neben den mit den oben genannten Privilegien verbundenen Anweisungen können Benutzer mit der **SYS\_REPLICATION\_ADMIN\_ROLE**-Systemrolle auch die folgenden Anweisungen ausführen:

- SYNCHRONIZE PROFILE-Anweisung
- REMOTE RESET-Anweisung
- LOCK FEATURE-Anweisung

**Siehe auch**

- „sp\_has\_role-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT ROLE SYS\_RUN\_REPLICATION\_ROLE-Anweisung [[MobiLink](#)] [[SQL Remote](#)]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT ROLE SYS\_REPLICATION\_ADMIN\_ROLE-Anweisung [[MobiLink](#)] [[SQL Remote](#)]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**Kompatibilitätsrollen**

Kompatibilitätsrollen sind mit Startrollen vergleichbar, die logische Gruppen von Privilegien enthalten. Außerdem dienen sie dazu, die Abwärtskompatibilität mit früheren Versionen von SQL Anywhere zu gewährleisten, die berechtigungsbasierte Sicherheit unterstützen.

Sie können weiterhin Berechtigungen erteilen und entziehen, indem Sie die nicht mehr empfohlene GRANT- und REVOKE-Syntax verwenden. Der Datenbankserver konvertiert jedoch die Erteilung bzw. Entziehung in den äquivalenten Vorgang für Kompatibilitätsrollen. Außerdem gilt für die Berechtigungen vor Version 16.0, die nicht vererbbar waren (DBA, REMOTE DBA, BACKUP, RESOURCE und VALIDATE), dass die äquivalente Kompatibilitätsrolle standardmäßig vererbbar ist.

Sie können nicht die zugrunde liegenden Privilegien von Kompatibilitätsrollen ändern. Sie können jedoch Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren und anschließend die Privilegien ändern. Beim Migrieren einer Kompatibilitätsrolle wird allen Berechtigungsempfängern der Kompatibilitätsrolle stattdessen automatisch die benutzerdefinierte Rolle erteilt. Durch Migrieren einer Kompatibilitätsrolle in eine benutzerdefinierte Rolle wird die Kompatibilitätsrolle automatisch gelöscht. Sie können jedoch die Kompatibilitätsrolle jederzeit wiederherstellen.

Die folgende Tabelle enthält Beschreibungen aller Kompatibilitätsrollen, einschließlich der jeweils äquivalenten Berechtigung vor Version 16.0.

Kompatibilitätsrolle	Beschreibung	Berechtigung vor Version 16.0
SYS_AUTH_DBA_ROLE	Diese Rolle umfasst alle erteilbaren Privilegien in der Software, weil ihr die Kompatibilitätsrollen SYS_AUTH_DBA_ROLE und SYS_AUTH_SA_ROLE erteilt werden.	DBA

Kompatibilitätsrolle	Beschreibung	Berechtigung vor Version 16.0
SYS_AUTH_SA_ROLE	<p>Diese Rolle umfasst alle Privilegien für die <b>Datenbankadministration</b> aus der SYS_AUTH_DBA_ROLE-Systemrolle und ist mit dieser Rolle verknüpft. Diese Rolle und SYS_AUTH_SSO_ROLE ergeben zusammen alle Privilegien in der SYS_AUTH_DBA_ROLE-Systemrolle.</p> <p>Diese Rolle kann migriert, gelöscht und wiederhergestellt werden, aber nur im Rahmen der Ausführung dieser Vorgänge mit SYS_AUTH_DBA_ROLE.</p>	-
SYS_AUTH_SSO_ROLE	<p>Diese Rolle umfasst alle <b>sicherheits- und zugriffs-bezogenen Privilegien</b> aus der SYS_AUTH_DBA_ROLE-Systemrolle. Diese Rolle und SYS_AUTH_SA_ROLE ergeben zusammen alle Privilegien in der SYS_AUTH_DBA_ROLE-Systemrolle.</p> <p>Diese Rolle kann migriert, gelöscht und wiederhergestellt werden, aber nur im Rahmen der Ausführung dieser Vorgänge mit SYS_AUTH_DBA_ROLE.</p>	-
SYS_AUTH_BACKUP_ROLE	Diese Rolle ermöglicht es einem Benutzer, mithilfe der BACKUP-Anweisung oder des Dienstprogramms dbbackup Datenbanken und Transaktionslogs mit Archiv- oder Sicherungskopien zu sichern.	BACKUP
SYS_AUTH_PROFILE_ROLE	Diese Rolle ermöglicht es einem Benutzer, Profilerstellungs-, Protokollierungs- und Diagnosevorgänge auszuführen.	PROFILE
SYS_AUTH_READCLIENTFILE_ROLE	Diese Rolle ermöglicht es einem Benutzer, Dateien auf dem Clientcomputer zu lesen, z.B. wenn Daten aus einer Datei auf einem Clientcomputer geladen werden.	READCLIENTFILE
SYS_AUTH_READFILE_ROLE	Diese Rolle ermöglicht es einem Benutzer, die OPENSTRING-Klausel in einer SELECT-Anweisung zum Lesen einer Datei zu verwenden.	READFILE
SYS_AUTH_RESOURCE_ROLE	Diese Rolle ermöglicht es einem Benutzer, Datenbankobjekte wie Tabellen, Ansichten, gespeicherte Prozeduren und Trigger zu erstellen.	RESOURCE

Kompatibilitätsrolle	Beschreibung	Berechtigung vor Version 16.0
SYS_AUTH_VALIDATE_ROLE	Diese Rolle ermöglicht es einem Benutzer, mithilfe der VALIDATE-Anweisung oder des Dienstprogramms dbvalid Datenbanken, Tabellen, Indizes und Prüfsummen zu validieren.	VALIDATE
SYS_AUTH_WRITEFILE_ROLE	Diese Rolle ermöglicht es einem Benutzer, die xp_write_file-Systemprozedur auszuführen.	WRITEFILE
SYS_AUTH_WRITECLIENTFILE_ROLE	Diese Rolle ermöglicht es einem Benutzer, in Dateien auf einem Clientcomputer zu schreiben, z.B. wenn die UNLOAD TABLE-Anweisung verwendet wird, um Daten auf einen Clientcomputer zu schreiben.	WRITECLIENTFILE

**Siehe auch**

- „Berechtigungen auf Datenbankebene werden zu Kompatibilitätsrollen“ auf Seite 1386
- „Änderungen des Vererbungsverhaltens für einige Berechtigungen, die zu Rollen geworden sind“ auf Seite 1400
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)“ auf Seite 1278
- „Kompatibilitätsrollen wiederherstellen (SQL)“ auf Seite 1284
- „Kompatibilitätsrollen wiederherstellen (Sybase Central)“ auf Seite 1283
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)**

Migrieren Sie eine Kompatibilitätsrolle in eine benutzerdefinierte Rolle und erteilen Sie anschließend die neue Rolle anderen Rollen und Benutzern. Beim Migrieren einer Kompatibilitätsrolle wird allen Berechtigungsempfängern der Kompatibilitätsrolle automatisch die benutzerdefinierte Rolle erteilt und die Kompatibilitätsrolle wird gelöscht.

**Voraussetzungen**

Sie benötigen das MANAGE ANY USER-Systemprivileg, das MANAGE ROLES-Systemprivileg und Administrationsrechte für die zu migrierende Rolle.

**Kontext und Bemerkungen**

Kompatibilitätsrollen sind mit Startrollen vergleichbar. Sie können nicht die zugrunde liegenden Privilegien von Kompatibilitätsrollen ändern. Sie können jedoch Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren und anschließend die Privilegien ändern.

Der Name, den Sie der neuen Rolle zuordnen, darf weder mit dem Präfix SYS\_ beginnen noch mit dem Suffix \_ROLE enden. SYS\_MyBackup\_ROLE kann beispielsweise nicht als Name einer

benutzerdefinierten Rolle verwendet werden. Der Name, den Sie der neuen Rolle geben, ist permanent und Sie können ihn nicht zu einem späteren Zeitpunkt ändern.

Die Systemrollen SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE können nicht einzeln migriert werden. Wenn jedoch die SYS\_AUTH\_DBA\_ROLE-Systemrolle migriert wird, werden die Systemrollen SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE automatisch ebenfalls in neue benutzerdefinierte Rollen migriert (standardmäßig sa\_role und sso\_role).

Wenn Sie eine Rolle migrieren, bei der die Vererbung von Systemprivilegien deaktiviert wurde (z.B. SYS\_AUTH\_VALIDATE\_ROLE), werden die Privilegien der neu erstellten benutzerdefinierten Rolle allen Berechtigungsempfängern in der Vererbungsstruktur erteilt.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Rollen** und wählen Sie die Kompatibilitätsrolle aus.
3. Rechtsklicken Sie auf die Kompatibilitätsrolle und klicken Sie dann auf **Zur benutzerdefinierten Rolle migrieren**
4. Im Feld **Name** können Sie einen neuen Namen für die neue benutzerdefinierte Rolle angeben oder den Standardnamen akzeptieren.
5. Klicken Sie auf **OK**.

### Ergebnisse

Allen Berechtigungsempfängern der Kompatibilitätsrolle wird automatisch die benutzerdefinierte Rolle erteilt. Die Kompatibilitätsrolle wird gelöscht.

### Nächste Schritte

Ändern Sie die Systemprivilegien der benutzerdefinierten Rolle und erteilen Sie die Rolle anderen Benutzern.

### Siehe auch

- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)“ auf Seite 1278
- „Kompatibilitätsrollen wiederherstellen (SQL)“ auf Seite 1284
- „Kompatibilitätsrollen“ auf Seite 1275
- „Rollen und Privilegien für Rollen konfigurieren (Sybase Central)“ auf Seite 1296

## Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)

Migrieren Sie eine Kompatibilitätsrolle in eine benutzerdefinierte Rolle und erteilen Sie anschließend die neue Rolle anderen Rollen und Benutzern. Beim Migrieren einer Kompatibilitätsrolle wird allen

Berechtigungsempfängern der Kompatibilitätsrolle automatisch die benutzerdefinierte Rolle erteilt und die Kompatibilitätsrolle wird gelöscht.

### Voraussetzungen

Sie benötigen das `MANAGE ROLES`-Systemprivileg und Administrationsrechte für die zu migrierende Rolle.

### Kontext und Bemerkungen

Kompatibilitätsrollen sind mit Startrollen vergleichbar. Sie können nicht die zugrunde liegenden Privilegien von Kompatibilitätsrollen ändern. Sie können jedoch Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren und anschließend die Privilegien ändern.

Der Name, den Sie der neuen Rolle zuordnen, darf weder mit dem Präfix `SYS_` beginnen noch mit dem Suffix `_ROLE` enden. `SYS_MyBackup_ROLE` kann beispielsweise nicht als Name einer benutzerdefinierten Rolle verwendet werden. Der Name, den Sie der neuen Rolle geben, ist permanent und Sie können ihn nicht zu einem späteren Zeitpunkt ändern.

Wenn Sie eine Rolle migrieren, bei der die Vererbung von Systemprivilegien deaktiviert wurde (z.B. `SYS_AUTH_VALIDATE_ROLE`), werden die Privilegien der neu erstellten benutzerdefinierten Rolle allen Berechtigungsempfängern in der Vererbungsstruktur erteilt.

Die Systemrollen `SYS_AUTH_SA_ROLE` und `SYS_AUTH_SSO_ROLE` können nicht einzeln migriert werden. Wenn jedoch die `SYS_AUTH_DBA_ROLE`-Systemrolle migriert wird, werden die Systemrollen `SYS_AUTH_SA_ROLE` und `SYS_AUTH_SSO_ROLE` automatisch in die neue benutzerdefinierte Rolle einbezogen.

### Aufgabe

- Wenn Sie eine Kompatibilitätsrolle migrieren möchten, führen Sie eine `ALTER ROLE`-Anweisung ähnlich der folgenden aus:

```
ALTER ROLE compatibility-role MIGRATE TO new-role-name;
```

Wenn Sie die `SYS_AUTH_DBA_ROLE`-Systemrolle migrieren, vergessen Sie nicht, Namen für die Systemrollen `SYS_AUTH_SA_ROLE` und `SYS_AUTH_SSO_ROLE` einzubeziehen, die automatisch migriert werden (d.h. `MIGRATE TO neuer_Rollenname, neuer_sa-Rollenname, neuer_sso-Rollenname`).

### Ergebnisse

Allen Berechtigungsempfänger der Kompatibilitätsrolle wird automatisch die benutzerdefinierte Rolle erteilt. Die Kompatibilitätsrolle wird gelöscht.

### Nächste Schritte

Ändern Sie die Systemprivilegien der neuen benutzerdefinierten Rolle und erteilen Sie die Rolle anderen Benutzern.

Obwohl Kompatibilitätsrollen nach dem Migrieren automatisch gelöscht werden, können Sie sie mit der CREATE ROLE-Anweisung für zukünftige Zwecke wiederherstellen. Siehe „[Kompatibilitätsrollen wiederherstellen \(SQL\)](#)“ auf Seite 1284.

### Beispiel

Die folgende Anweisung migriert die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle in die neue benutzerdefinierte Rolle my\_BACKUP. Allen Benutzern, denen zuvor die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle erteilt wurde, wird nun die my\_BACKUP-Rolle erteilt, einschließlich der Administrationsrechte, die sie für die Kompatibilitätsrolle hatten.

```
ALTER ROLE SYS_AUTH_BACKUP_ROLE MIGRATE TO my_BACKUP;
```

Die folgende Anweisung migriert die Systemrollen SYS\_AUTH\_DBA\_ROLE, SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE in die benutzerdefinierten Rollen my\_DBA, my\_DBA\_Administration bzw. my\_DBA\_Security. Alle Benutzer, zugrunde liegenden Privilegien und der ursprünglichen Rolle erteilten Rollen werden automatisch in die neuen Rollen migriert. Abschließend werden die Systemrollen SYS\_AUTH\_DBA\_ROLE, SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE gelöscht.

```
ALTER ROLE SYS_AUTH_DBA_ROLE  
MIGRATE TO my_DBA, my_DBA_Administration, my_DBA_Security;
```

### Siehe auch

- „ALTER ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277
- „Kompatibilitätsrollen“ auf Seite 1275

## Kompatibilitätsrollen erteilen (Sybase Central)

Erteilen Sie eine Kompatibilitätsrolle einem Benutzer oder einer Rolle. Normalerweise erteilen Sie Kompatibilitätsrollen, um die Abwärtskompatibilität aufrechtzuerhalten.

### Voraussetzungen

Sie benötigen Administrationsrechte für die zu erteilende Kompatibilitätsrolle.

### Kontext und Bemerkungen

Wenn Sie eine Kompatibilitätsrolle einer Rolle erteilen, sind die Systemprivilegien der Kompatibilitätsrolle sowohl für die Rolle als auch für deren Berechtigungsempfänger verfügbar. Sie können jedoch die Vererbung der Systemprivilegien für die folgenden Kompatibilitätsrollen deaktivieren:

- SYS\_AUTH\_DBA\_ROLE
- SYS\_AUTH\_RESOURCE\_ROLE
- SYS\_AUTH\_BACKUP\_ROLE
- SYS\_AUTH\_VALIDATE\_ROLE

Wenn Sie in Sybase Central eine dieser Kompatibilitätsrollen einer benutzererweiterten Rolle oder einer Systemrolle erteilen, wird die Vererbung der Systemprivilegien standardmäßig deaktiviert. Das

Deaktivieren der Vererbung von Systemprivilegien für eine Kompatibilitätsrolle entspricht dem Verhalten der nicht vererbten Berechtigungen in Datenbanken bis Version 12.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im Rollenordner auf die Kompatibilitätsrolle, die Sie erteilen möchten.
3. Klicken Sie im rechten Fensterausschnitt auf **Berechtigungsempfänger**.
4. Rechtsklicken Sie in den rechten Fensterausschnitt und wählen Sie **Neu » Berechtigungsempfänger**.
5. Klicken Sie auf den Benutzer bzw. die Rolle, dem bzw. der Sie die Kompatibilitätsrolle erteilen möchten, und anschließend auf **OK**.

Unter **Berechtigungsempfänger** wird eine neue Zeile hinzugefügt.

Wenn die Vererbung der Systemprivilegien für die Kompatibilitätsrolle deaktiviert ist, enthält die Spalte **Optionen** den Eintrag **Vererbung deaktiviert**. Wenn Sie die Vererbung der Systemprivilegien aktivieren möchten, rechtsklicken Sie auf die Zeile, klicken Sie auf **Optionen festlegen** und wählen Sie **Vererbung von Systemprivilegien aktivieren**.

Mit Ausnahme der Erteilung der SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle können Sie keine Administrationsrechte erteilen, wenn **Vererbung deaktiviert** ausgewählt ist.

6. Klicken Sie auf **Datei » Speichern**.

### Ergebnisse

Die Kompatibilitätsrolle wird dem Benutzer bzw. der Rolle erteilt.

### Siehe auch

- „Kompatibilitätsrollen“ auf Seite 1275
- „Berechtigungen auf Datenbankebene werden zu Kompatibilitätsrollen“ auf Seite 1386
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277

## Kompatibilitätsrollen erteilen (SQL)

Erteilen Sie eine Kompatibilitätsrolle einem Benutzer oder einer benutzererweiterten Rolle. Sie können Kompatibilitätsrollen nur benutzerdefinierten Rollen erteilen, die benutzererweiterte Rollen sind.

### Voraussetzungen

Sie benötigen Administrationsrechte für die zu erteilende Rolle.

Kontext und Bemerkungen

Normalerweise erteilen Sie Benutzern oder Rollen Kompatibilitätsrollen, um die Abwärtskompatibilität aufrechtzuerhalten.

Wenn Sie eine Kompatibilitätsrolle einer Rolle erteilen, sind die Systemprivilegien der Kompatibilitätsrolle sowohl für die Rolle als auch für deren Berechtigungsempfänger verfügbar. Sie können jedoch die Vererbung der Systemprivilegien für die folgenden Kompatibilitätsrollen deaktivieren:

- SYS\_AUTH\_DBA\_ROLE
- SYS\_AUTH\_RESOURCE\_ROLE
- SYS\_AUTH\_BACKUP\_ROLE
- SYS\_AUTH\_VALIDATE\_ROLE

Wenn Sie die Vererbung der Systemprivilegien für eine Kompatibilitätsrolle deaktivieren, sind die Systemprivilegien nur für die Rolle verfügbar, aber nicht für ihre Berechtigungsempfänger. Das Deaktivieren der Vererbung von Systemprivilegien für eine Kompatibilitätsrolle entspricht dem Verhalten der nicht vererbten Berechtigungen in Datenbanken bis Version 12.

Aufgabe

- Führen Sie eine GRANT ROLE-Anweisung aus:

Option	Beispielanweisung
Gewähren der Möglichkeit, die Rolle auszuüben, zusammen mit der Möglichkeit, sie anderen Benutzern oder Rollen zu erteilen und zu entziehen:	<pre>GRANT ROLE SYS_AUTH_DBA_ROLE TO user- or-role-name WITH ADMIN OPTION;</pre>
Gewähren der Möglichkeit, die Rolle anderen Benutzern oder Rollen zu erteilen und zu entziehen, aber nicht der Möglichkeit, sie auszuüben:	<pre>GRANT ROLE SYS_AUTH_DBA_ROLE TO user- or-role-name WITH ADMIN ONLY OPTION;</pre>
Gewähren der Möglichkeit, die Rolle auszuüben, aber nicht der Möglichkeit, sie anderen Benutzern oder Rollen zu erteilen und zu entziehen:	<pre>GRANT ROLE SYS_AUTH_DBA_ROLE TO user- or-role-name WITH NO ADMIN OPTION;</pre>
Gewähren der Möglichkeit, eine Kompatibilitätsrolle auszuüben und die Vererbung von Systemprivilegien der Rolle zu deaktivieren:	<pre>GRANT ROLE SYS_AUTH_DBA_ROLE TO role- name WITH NO SYSTEM PRIVILEGE INHERITANCE;</pre>

Ergebnisse

Die Kompatibilitätsrolle wird dem Benutzer bzw. der Rolle erteilt.

Beispiel

In diesem Beispiel wird SYS\_AUTH\_BACKUP\_ROLE der R\_HumanResources-Rolle erteilt.

```
GRANT ROLE SYS_AUTH_BACKUP_ROLE TO R_HumanResources
WITH NO SYSTEM PRIVILEGE INHERITANCE;
```

### Siehe auch

- „Kompatibilitätsrollen“ auf Seite 1275
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)“ auf Seite 1278
- „Berechtigungen auf Datenbankebene werden zu Kompatibilitätsrollen“ auf Seite 1386

## Kompatibilitätsrollen wiederherstellen (Sybase Central)

Stellt eine Kompatibilitätsrolle wieder her, die migriert oder gelöscht wurde. Diese Methode kann nicht verwendet werden, um andere Arten von Rollen wiederherzustellen.

### Voraussetzungen

Sie benötigen das MANAGE ROLES-Systemprivileg und Administrationsrechte für alle Systemprivilegien, die der wiederherzustellenden Rolle erteilt werden. Um beispielsweise die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle wiederherzustellen, benötigen Sie das MANAGE ROLES-Systemprivileg und Administrationsrechte für das BACKUP DATABASE-Systemprivileg.

### Kontext und Bemerkungen

Sie können Kompatibilitätsrollen wiederherstellen, die sich nicht mehr in der Datenbank befinden. Das Wiederherstellen einer solchen Rolle kann hilfreich sein, um die Privilegien, die die ursprüngliche Rolle hatte, abzurufen oder in benutzerdefinierte Rollen zu migrieren.

Wenn Sie die Kompatibilitätsrolle migriert haben (sodass sie gelöscht wurde), wurde Berechtigungsempfängern der Rolle automatisch die neue benutzerdefinierte Rolle erteilt, in die Sie migriert haben. Beim Wiederherstellen einer Kompatibilitätsrolle wird die Kompatibilitätsrolle nicht automatisch wieder ihren Berechtigungsempfängern erteilt. Diese bleiben Berechtigungsempfänger der benutzerdefinierten Rolle, die Sie erstellt haben.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Rollen**.
3. Rechtsklicken Sie in den rechten Fensterausschnitt und klicken Sie auf **Neu » Rollen**.
4. Klicken Sie auf die Option **Kompatibilitätsrollen wiederherstellen** des **Assistenten zum Erstellen einer Rolle** und befolgen Sie die Anweisungen.

### Ergebnisse

Die Rolle wird wiederhergestellt. Administratorprivilegien für die wiederhergestellte Rolle werden automatisch der SYS\_AUTH\_DBA\_ROLE-Systemrolle erteilt, sofern diese immer noch in der Datenbank vorhanden ist.

Wenn Sie die SYS\_AUTH\_DBA\_ROLE-Systemrolle wiederherstellen, werden die Systemrollen SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE automatisch ebenfalls wiederhergestellt.

### Siehe auch

- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsrollen“ auf Seite 1275
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277
- „Rollen löschen (Sybase Central)“ auf Seite 1303

## Kompatibilitätsrollen wiederherstellen (SQL)

Stellt eine Kompatibilitätsrolle wieder her, die migriert oder gelöscht wurde. Diese Methode kann nicht verwendet werden, um andere Arten von Rollen wiederherzustellen.

### Voraussetzungen

Sie benötigen das MANAGE ROLES-Systemprivileg und Administrationsrechte für alle Systemprivilegien, die der wiederherzustellenden Rolle erteilt werden. Um beispielsweise die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle wiederherzustellen, benötigen Sie das MANAGE ROLES-Systemprivileg und Administrationsrechte für das BACKUP DATABASE-Systemprivileg.

### Kontext und Bemerkungen

Sie können Kompatibilitätsrollen wiederherstellen, die sich nicht mehr in der Datenbank befinden. Das Wiederherstellen einer solchen Rolle kann hilfreich sein, um die Privilegien, die die ursprüngliche Rolle hatte, abzurufen oder in benutzerdefinierte Rollen zu migrieren.

Wenn Sie die Kompatibilitätsrolle migriert haben (sodass sie gelöscht wurde), wurde Berechtigungsempfängern der Rolle automatisch die neue benutzerdefinierte Rolle erteilt, in die Sie migriert haben. Beim Wiederherstellen einer Kompatibilitätsrolle wird die Kompatibilitätsrolle nicht automatisch wieder ihren Berechtigungsempfängern erteilt. Diese bleiben Berechtigungsempfänger der benutzerdefinierten Rolle, die Sie erstellt haben.

### Aufgabe

- Führen Sie eine CREATE ROLE-Anweisung ähnlich der folgenden aus, wobei *Rollenname* der Name der Rolle ist:

```
CREATE ROLE role-name;
```

### Ergebnisse

Die Rolle wird wiederhergestellt. Administratorprivilegien für die wiederhergestellte Rolle werden automatisch der SYS\_AUTH\_DBA\_ROLE-Systemrolle erteilt, sofern diese immer noch in der Datenbank vorhanden ist.

Wenn Sie die SYS\_AUTH\_DBA\_ROLE-Systemrolle wiederherstellen, werden die Systemrollen SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE automatisch ebenfalls wiederhergestellt.

## Beispiel

Im folgenden Beispiel wird die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle wiederhergestellt und dem Benutzer "TomW" (nur) als Administrator erteilt:

```
CREATE ROLE SYS_AUTH_BACKUP_ROLE;
```

Im folgenden Beispiel werden die Systemrollen SYS\_AUTH\_DBA\_ROLE, SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE wiederhergestellt:

```
CREATE ROLE SYS_AUTH_DBA_ROLE;
```

## Siehe auch

- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kompatibilitätsrollen“ auf Seite 1275
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)“ auf Seite 1278

## Benutzerdefinierte Rollen

Eine benutzerdefinierte Rolle ist eine benutzerdefinierte Sammlung von Systemprivilegien, Privilegien auf Objektebene und Rollen, die in der Regel erstellt wird, um Privilegien zu gruppieren, die mit einer bestimmten Aufgabe oder Aufgabengruppe zusammenhängen. Sie können benutzerdefinierte Rollen erstellen, die an die Anforderungen Ihrer Organisation angepasst sind.

Benutzerdefinierte Rollen können Eigentümerinnen von Objekten sein.

Wenn eine benutzerdefinierte Rolle mit Administrationsrechten erteilt wird, kann ein Benutzer die Rolle verwalten (erteilen, entziehen und löschen) sowie die zugrunde liegenden Systemprivilegien der Rolle nutzen. Wenn die Rolle nur mit Administrationsrechten erteilt wird, kann der Benutzer die Rolle verwalten, aber nicht die zugrunde liegenden Systemprivilegien nutzen. Wenn die Rolle ohne Administrationsrechte erteilt wird, kann der Benutzer nur die zugrunde liegenden Systemprivilegien nutzen.

Eine spezielle Form der benutzerdefinierten Rolle ist die **benutzererweiterte Rolle**. Dies ist ein Benutzer, der zu einer Rolle erweitert wurde, die wiederum anderen erteilt werden kann.

## Siehe auch

- „Benutzererweiterte Rollen“ auf Seite 1287
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (SQL)“ auf Seite 1278

## Benutzerdefinierte Rollen erstellen (Sybase Central)

Erstellen Sie eine Rolle und erteilen Sie ihr Rollen und Privilegien.

### Voraussetzungen

Sie müssen das MANAGE ROLES-Systemprivileg haben.

Der Name, den Sie der neuen Rolle zuordnen, darf weder mit dem Präfix **SYS\_** beginnen noch mit dem Suffix **\_ROLE** enden. **SYS\_MyBackup\_ROLE** kann beispielsweise nicht als Name einer benutzerdefinierten Rolle verwendet werden.

### Kontext und Bemerkungen

Sie können auch einen vorhandenen Benutzer in eine benutzererweiterte Rolle konvertieren und anschließend die benutzererweiterte Rolle anderen Benutzern erteilen.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Rollen** und klicken Sie auf **Neu » Rolle**.
3. Befolgen Sie die Anweisungen des Assistenten.

### Ergebnisse

Eine neue Rolle wird erstellt. Standardmäßig sind Sie Eigentümer der Rolle und die Rolle wird dem **MANAGE ROLES**-Systemprivileg erteilt.

### Nächste Schritte

Erteilen Sie dieser Rolle Systemprivilegien und erteilen Sie diese Rolle anderen Benutzern.

### Siehe auch

- „Rollen erteilen (Sybase Central)“ auf Seite 1298
- „Rollen“ auf Seite 1271
- „Rollenadministratoren“ auf Seite 1293
- „Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)“ auf Seite 1289
- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Vererbung von Rollen und Privilegien“ auf Seite 1348

## Benutzerdefinierte Rollen erstellen (SQL)

Erstellen Sie eine Rolle und erteilen Sie ihr Privilegien und Rollen.

### Voraussetzungen

Sie müssen das **MANAGE ROLES**-Systemprivileg haben.

Der Name, den Sie der neuen Rolle zuordnen, darf weder mit dem Präfix **SYS\_** beginnen noch mit dem Suffix **\_ROLE** enden. **SYS\_MyBackup\_ROLE** kann beispielsweise nicht als Name einer benutzerdefinierten Rolle verwendet werden.

## Kontext und Bemerkungen

Sie können auch einen vorhandenen Benutzer in eine benutzererweiterte Rolle konvertieren und anschließend die benutzererweiterte Rolle anderen Benutzern erteilen.

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine CREATE ROLE-Anweisung aus. Zum Beispiel:

```
CREATE ROLE role-name
```

3. Erteilen Sie mithilfe der GRANT-Anweisung der neuen Rolle Systemprivilegien und Rollen.

## Ergebnisse

Die neue Rolle wird erstellt.

## Nächste Schritte

Erteilen Sie dieser Rolle Systemprivilegien und erteilen Sie diese Rolle anderen Benutzern.

## Beispiel

Die folgende Anweisung erstellt eine Rolle namens Sales. Da kein Administrator angegeben wurde, können globale Administratoren (Benutzer mit dem MANAGE ROLES-Systemprivileg) die Rolle verwalten.

```
CREATE ROLE Sales;  
GRANT SELECT, UPDATE ON GROUP0.SalesOrders TO Sales;  
GRANT SELECT, UPDATE ON GROUP0.SalesOrderItems TO Sales;
```

## Siehe auch

- „CREATE ROLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Benutzerdefinierte Rollen erstellen (Sybase Central)“ auf Seite 1285
- „Rollen“ auf Seite 1271
- „Rollenadministratoren“ auf Seite 1293
- „Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)“ auf Seite 1289
- „Rollen erteilen (Sybase Central)“ auf Seite 1298
- „Vererbung von Rollen und Privilegien“ auf Seite 1348

## Benutzererweiterte Rollen

Eine **benutzererweiterte Rolle** ist ein Typ der benutzerdefinierten Rolle. Es handelt sich um eine Benutzer-ID, die zu einer Rolle erweitert wurde, die wiederum anderen erteilt werden kann.

Benutzererweiterte Rollen sind das Äquivalent von **Gruppen** in Versionen von SQL Anywhere vor 16.0.

Wenn Sie eine benutzererweiterte Rolle einem Benutzer oder einer anderen Rolle erteilen, erbt der Berechtigungsempfänger alle Systemprivilegien und Privilegien auf Objektebene, die die benutzererweiterte Rolle hat, einschließlich etwaiger Administrationsrechte.

Da das Eigentum an Datenbankobjekten einer einzelnen Benutzer-ID zugeordnet ist, wird im Fall einer benutzererweiterten Rolle als Eigentümerin das Eigentum am Datenbankobjekt nicht von deren Berechtigungsempfängern geerbt. Nur erteilte Privilegien werden geerbt.

Benutzererweiterte Rollen sind sinnvoll, wenn Sie einen Benutzer mit Systemprivilegien haben, die Sie einem anderen Benutzer erteilen möchten. Der Benutzer, der zu einer benutzererweiterten Rolle wird, kann anschließend die neue Rolle verwalten (anderen erteilen und entziehen), es sei denn, dieses Privileg wird explizit entfernt.

Beim Erstellen einer benutzererweiterten Rolle wird der Rolle automatisch das `MANAGE ROLES`-Systemprivileg nur mit Administrationsrechten erteilt.

Sie können die Erweiterung einer Rolle widerrufen und steuern, welche Privilegien den Berechtigungsempfängern entzogen werden.

Ein Benutzer kann sich weiterhin mit seiner Benutzer-ID anmelden, auch wenn er als benutzererweiterte Rolle fungiert.

Wenn Sie einen Benutzer in eine benutzererweiterte Rolle konvertieren möchten, verwenden Sie die `CREATE ROLE`-Anweisung. Wenn Sie eine benutzererweiterte Rolle in einen Benutzer zurückkonvertieren möchten, verwenden Sie die `DROP ROLE`-Anweisung.

### Siehe auch

- „`sp_has_role`-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`CREATE ROLE`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`DROP ROLE`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`GRANT`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`REVOKE`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Namen von Datenbankobjekten und Präfixe“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

### Beispiel

- Die folgenden Anweisungen erstellen Benutzer1, erteilen Benutzer1 das `BACKUP DATABASE`-Privileg, erweitern Benutzer1 als Rolle und erteilen anschließend an Benutzer2 und Benutzer3 die Rolle Benutzer1:

```
CREATE USER "user1" IDENTIFIED BY 'sql';
GRANT BACKUP DATABASE TO "user1";
CREATE ROLE FOR USER "user1";
GRANT ROLE "user1" TO "user2";
GRANT ROLE "user1" TO "user3";
```

Die folgende Anweisung entzieht Benutzer2 die Rolle Benutzer1:

```
REVOKE ROLE "user1" FROM "user2";
```

Die folgende Anweisung ändert die Rolle Benutzer1 in einen Benutzer. Als Folge davon wird Benutzer3 die Rolle Benutzer1 entzogen:

```
DROP ROLE FROM USER "user1" WITH REVOKE;
```

## Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)

Ändern Sie einen Benutzer in eine benutzererweiterte Rolle, die anschließend anderen Benutzern und Rollen erteilt werden kann. Benutzererweiterte Rollen sind sinnvoll, wenn Sie einen Benutzer mit den gewünschten Systemprivilegien und Rollen haben, die Sie auch einem anderen Benutzer erteilen möchten.

### Voraussetzungen

Sie müssen das `MANAGE ROLES`-Privileg haben.

### Kontext und Bemerkungen

Der Benutzer, der zu einer benutzererweiterten Rolle wird, kann anschließend die neue Rolle verwalten (anderen erteilen und entziehen), es sei denn, dieses Privileg wird explizit entfernt. Außerdem können Benutzer mit `MANAGE ROLES`-Systemprivileg die Rolle verwalten.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Benutzer** und wählen Sie den Benutzer aus.
3. Rechtsklicken Sie auf den Benutzer und klicken Sie dann auf **In benutzererweiterte Rolle ändern**.

### Ergebnisse

Der Benutzer wird zu einer Rolle erweitert. Im rechten Fensterausschnitt wird die zusätzliche Registerkarte **Berechtigungsempfänger** angezeigt und im linken Fensterausschnitt erscheint die neue Rolle in der Liste der Rollen.

### Nächste Schritte

Sie können die neue Rolle anderen Benutzern und Rollen erteilen. Wenn Sie eine benutzererweiterte Rolle einem Benutzer oder einer anderen Rolle erteilen, erbt der Berechtigungsempfänger alle Systemprivilegien und Privilegien auf Objektebene, die die benutzererweiterte Rolle hat, einschließlich etwaiger Administrationsrechte.

### Siehe auch

- „[CREATE ROLE-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „[Benutzererweiterte Rollen in Benutzer zurückkonvertieren \(Sybase Central\)](#)“ auf Seite 1291
- „[Benutzer in benutzererweiterte Rollen konvertieren \(SQL\)](#)“ auf Seite 1290
- „[Benutzererweiterte Rollen](#)“ auf Seite 1287

# Benutzer in benutzererweiterte Rollen konvertieren (SQL)

Ändern Sie einen Benutzer in eine benutzererweiterte Rolle, die anschließend anderen Benutzern und Rollen erteilt werden kann. Benutzererweiterte Rollen sind sinnvoll, wenn Sie einen Benutzer mit den gewünschten Systemprivilegien und Rollen haben, die Sie auch einem anderen Benutzer erteilen möchten.

## Voraussetzungen

Sie müssen das `MANAGE ROLES`-Systemprivileg haben.

## Kontext und Bemerkungen

Sie können während der Konvertierung Administratoren für die Rolle angeben. Wenn Sie keine Administratoren angeben, kann standardmäßig jeder Benutzer mit `MANAGE ROLE`-Systemprivileg die Rolle verwalten.

Der Benutzer, der zu einer benutzererweiterten Rolle erweitert wird, kann nicht als Administrator angegeben werden und ihm können nach Abschluss der Konvertierung keine Administrationsrechte für die Rolle erteilt werden. Wenn jedoch der zu erweiternde Benutzer das `MANAGE ROLES`-Systemprivileg hat und zum Zeitpunkt der Konvertierung keine Administratoren angegeben werden, kann der Benutzer die Rolle verwalten.

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine `CREATE ROLE`-Anweisung ähnlich der folgenden aus:

Beschreibung	Anweisung
Der Benutzer wird zu einer Rolle erweitert, die jeder Benutzer mit <code>MANAGE ROLES</code> -Systemprivileg verwalten kann.	<code>CREATE ROLE FOR USER userid;</code>
Der Benutzer wird zu einer Rolle erweitert, die jeder Benutzer in der <i>Liste_der_Administrator-IDs</i> verwalten kann.	<code>CREATE ROLE FOR USER userid WITH ADMIN list-of- administrator-ids;</code>

## Ergebnisse

Der Benutzer wird zu einer Rolle erweitert.

## Nächste Schritte

Sie können die neue Rolle anderen Benutzern und Rollen erteilen. Wenn Sie eine benutzererweiterte Rolle einem Benutzer oder einer anderen Rolle erteilen, erbt der Berechtigungsempfänger alle Systemprivilegien und Privilegien auf Objektebene, die die benutzererweiterte Rolle hat, einschließlich etwaiger Administrationsrechte.

## Beispiel

Die folgende Anweisung erweitert den Benutzer JaneSmith zu einer Rolle, die anderen zugeordnet werden kann.

```
CREATE ROLE FOR USER JaneSmith;
```

## Siehe auch

- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Benutzererweiterte Rollen in Benutzer zurückkonvertieren (SQL)“ auf Seite 1292
- „Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)“ auf Seite 1289
- „Benutzererweiterte Rollen“ auf Seite 1287

## Benutzererweiterte Rollen in Benutzer zurückkonvertieren (Sybase Central)

Ändern Sie eine benutzererweiterte Rolle in einen normalen Benutzer zurück.

### Voraussetzungen

Sie benötigen das MANAGE ROLES-Systemprivileg oder Administrationsrechte für die Rolle.

### Kontext und Bemerkungen

Eine benutzererweiterte Rolle kann in einen normalen Benutzer zurückkonvertiert werden, solange alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die min\_role\_admin-Datenbankoption festgelegt ist.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Rollen** und wählen Sie die benutzererweiterte Rolle aus.
3. Rechtsklicken Sie auf die benutzererweiterte Rolle und klicken Sie dann auf **Auf Benutzer ändern**.

### Ergebnisse

Die Rolle wird in einen Benutzer zurückkonvertiert. Im rechten Fensterausschnitt wird die Registerkarte **Berechtigungsempfänger** nicht mehr angezeigt und im linken Fensterausschnitt verschwindet die Rolle aus der Liste der Rollen. Alle Objekte, die Eigentum der benutzererweiterten Rolle waren, verbleiben beim konvertierten Benutzer. Benutzer oder Rollen, die vorher die benutzererweiterte Rolle hatten, verfügen nicht mehr über die Privilegien, die der konvertierte Benutzer hat.

### Nächste Schritte

Wenn Sie die benutzererweiterte Rolle in einen Benutzer ändern möchten, um die Rolle zu löschen, können Sie den Benutzer löschen.

**Siehe auch**

- „Benutzererweiterte Rollen“ auf Seite 1287
- „DROP ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „min\_role\_admins-Option“ auf Seite 638

**Benutzererweiterte Rollen in Benutzer zurückkonvertieren (SQL)**

Ändern Sie eine benutzererweiterte Rolle in einen normalen Benutzer zurück.

**Voraussetzungen**

Sie benötigen das MANAGE ROLES-Systemprivileg oder Administrationsrechte für die Rolle.

**Kontext und Bemerkungen**

Eine benutzererweiterte Rolle kann in einen normalen Benutzer zurückkonvertiert werden, solange alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die min\_role\_admin-Datenbankoption festgelegt ist.

**Aufgabe**

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine Anweisung ähnlich der folgenden aus:

Option	Anweisung
Die Rolle in einen Benutzer zurückkonvertieren, sofern sie keinen anderen Rollen oder Benutzern erteilt wurde	<pre>DROP ROLE FROM USER userid;</pre>
Die Rolle in einen Benutzer zurückkonvertieren und die zugrunde liegenden Privilegien allen entziehen, denen die benutzererweiterte Rolle erteilt wurde	<pre>DROP ROLE FROM USER userid WITH REVOKE;</pre>

**Ergebnisse**

Die Rolle wird in einen Benutzer zurückkonvertiert. Alle Objekte, die Eigentum der benutzererweiterten Rolle waren, verbleiben beim konvertierten Benutzer. Benutzer oder Rollen, die vorher die benutzererweiterte Rolle hatten, verfügen nicht mehr über die Privilegien, die der konvertierte Benutzer hat.

**Nächste Schritte**

Wenn Sie die benutzererweiterte Rolle in einen Benutzer ändern möchten, um den Benutzer zu löschen, können Sie nun den Benutzer löschen.

**Beispiel**

Die folgende Anweisung konvertiert eine benutzererweiterte Rolle namens Joe in einen normalen Benutzer zurück. Objekte, die Eigentum der benutzererweiterten Rolle waren, gehören nun dem normalen

Benutzer Joe. Benutzer oder Rollen, denen die Rolle Joe erteilt war, behalten die der Rolle zugrunde liegenden Privilegien.

```
DROP ROLE FROM USER Joe;
```

Die folgende Anweisung konvertiert eine benutzererweiterte Rolle namens Sam in einen normalen Benutzer zurück. Benutzer oder Rollen, denen die Rolle Sam erteilt war, werden die Privilegien von Jack entzogen.

```
DROP ROLE FROM USER Sam WITH REVOKE;
```

Die folgende Anweisung löscht eine Rolle namens Marketing2, löscht die Objekte, deren Eigentümerin sie war, und entzieht die zugrunde liegenden Privilegien denjenigen, denen die Rolle erteilt war.

```
DROP ROLE Marketing2 WITH REVOKE WITH DROP OBJECTS;
```

### Siehe auch

- „Benutzererweiterte Rollen in Benutzer zurückkonvertieren (Sybase Central)“ auf Seite 1291
- „Benutzer in benutzererweiterte Rollen konvertieren (SQL)“ auf Seite 1290
- „Benutzererweiterte Rollen“ auf Seite 1287
- „DROP ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „min\_role\_admins-Option“ auf Seite 638

## Rollenadministratoren

Rollenadministratoren sind dafür verantwortlich, benutzerdefinierte Rollen Benutzern und anderen Rollen zu erteilen und zu entziehen. Sie können Rollenadministratoren nach Bedarf hinzufügen und entfernen. Es gibt keine maximale Anzahl von Rollenadministratoren, die einer einzelnen Rolle erteilt werden können. Es gibt jedoch eine Mindestzahl, wie durch die min\_role\_admins-Datenbankoption festgelegt.

Außerdem werden Benutzer mit MANAGE ROLES-Systemprivileg als **globale Rollenadministratoren** bezeichnet. Globale Rollenadministratoren können benutzerdefinierte Rollen verwalten, für die kein Administrator angegeben wurde.

Globale Rollenadministratoren sind die einzigen Administratoren der Systemrollen.

### Administratoren angeben

Sie können Rollenadministratoren bei der Rollenerstellung angeben oder nach dem Erstellen der Rolle.

In diesem Beispiel wird die Rolle myRole erstellt sowie den Benutzern MaryM und TomS mit Administrationsrechten erteilt. Nach der Erstellung können nur MaryM und TomS die Rolle erteilen oder entziehen.

```
CREATE ROLE myRole WITH ADMIN MaryM, TomS;
```

In diesem Beispiel wird die Rolle myRole erstellt, ihr wird ein Privileg hinzugefügt und anschließend wird die Benutzer-ID PeriW als Administrator hinzugefügt.

```
CREATE USER PeriW IDENTIFIED BY PeriW;
CREATE ROLE myRole;
```

```
GRANT SELECT ANY TABLE to myRole;  
GRANT ROLE myRole to PeriW WITH ADMIN ONLY OPTION;
```

### Globale Administratoren und das MANAGE ROLES-Systemprivileg

Wenn Sie eine Rolle erstellen, aber bei der Erstellung keinen Administrator angeben, werden dem MANAGE ROLES-Systemprivileg automatisch (nur) Administrationsrechte für die neue Rolle erteilt. Dadurch kann jeder Benutzer mit MANAGE ROLES-Systemprivileg die Rolle verwalten.

MANAGE ROLES ist in dieser Hinsicht einmalig: Es ist das einzige Systemprivileg, dem Rollen erteilt (WITH ADMIN ONLY OPTION) und entzogen werden können.

Wenn bei der Rollenerstellung kein Administrator angegeben wird (sodass die Rolle automatisch MANAGE ROLES erteilt wird) und später Administratoren für die Rollen angegeben werden, können sowohl diese Administratoren als auch alle Benutzer mit MANAGE ROLES-Systemprivileg die Rolle verwalten.

Wenn Sie eine Rolle erstellen und während der Erstellung Administratoren angeben, können nur diese Administratoren die Rolle verwalten, und globale Administratoren können es nur, wenn MANAGE ROLES einer der angegebenen Administratoren ist. Wenn Sie eine Rolle erstellen und MANAGE ROLES als einen der Administratoren einbeziehen möchten, führen Sie eine Anweisung ähnlich der folgenden aus. Beim Angeben des MANAGE ROLES-Systemprivilegs müssen Sie die interne Darstellung verwenden: SYS\_MANAGE\_ROLES\_ROLE. Wenn Sie dem MANAGE ROLES-Systemprivileg eine Rolle erteilen möchten, müssen Sie sie nur mit Administrationsrechten (WITH ADMIN ONLY) erteilen. Andernfalls wird ein Fehler zurückgegeben.

```
CREATE ROLE myRole WITH ADMIN ONLY MaryM, TomS, SYS_MANAGE_ROLES_ROLE;
```

MaryM, TomS und jeder Benutzer mit MANAGE ROLES-Systemprivileg können die Rolle verwalten. MaryM und TomS können jedoch die Rolle nicht ausüben.

#### Hinweis

Beim Erstellen einer Rolle sind folgende Optionen im Zusammenhang mit Administrationsrechten verfügbar: WITH ADMIN und WITH ADMIN ONLY. Beim Erteilen einer Rolle sind folgende Optionen im Zusammenhang mit Administrationsrechten verfügbar: WITH ADMIN OPTION, WITH NO ADMIN OPTION und WITH ADMIN ONLY OPTION.

Sie können auch nach dem Erstellen einer Rolle dem MANAGE ROLES-Systemprivileg Administrationsrechte erteilen, indem Sie eine Anweisung ähnlich der folgenden ausführen. Auch hier müssen Sie daran denken, WITH ADMIN ONLY OPTION anzugeben:

```
GRANT ROLE myRole TO SYS_MANAGE_ROLES_ROLE WITH ADMIN ONLY OPTION;
```

Wenn Sie eine Rolle erstellt haben und die Möglichkeit für den globalen Administrator entfernen möchten, diese zu verwalten, können Sie MANAGE ROLES die Rolle entziehen, indem Sie eine Anweisung ähnlich der folgenden ausführen:

```
REVOKE ROLE myRole FROM SYS_MANAGE_ROLES_ROLE;
```

## Rollenadministratoren nach Erstellung ändern oder löschen

Wenn einer Rolle bereits ein Administrator zugewiesen ist und Sie diesen in eine andere Benutzer-ID ändern möchten, erteilen Sie die Rolle dem neuen Administrator (unter Angabe von WITH ADMIN oder WITH ADMIN ONLY) und entziehen Sie dann dem ersten Administrator die Administratorprivilegien.

### Hinweis

Wenn Sie nur Rollenadministratoren zu einer Rolle hinzufügen möchten, verwenden Sie die GRANT ROLE-Anweisung mit der WITH ADMIN [ONLY] OPTION-Klausel statt der CREATE OR REPLACE ROLE-Anweisung.

Die min\_role\_admins-Datenbankoption steuert die Mindestanzahl von Administratoren, die eine Rolle haben muss. Die Anweisung, einem Benutzer Administrationsrechte zu entziehen, kann fehlschlagen, wenn ihre Ausführung dazu führen würde, dass die Anzahl der Administratoren unter den durch die min\_role\_admins-Option festgelegten Wert fällt. Dies ist jedoch kein Problem, solange andere Benutzer globale Rollenadministrationsrechte haben (MANAGE ROLE-Systemprivileg), da diese globalen Rollenadministratoren Rollen verwalten können, für die keine Administratoren angegeben wurden.

## Administratoren während der Rollenerstellung angeben

Legen Sie beim Erstellen einer Rolle die Administratoren im Rahmen der CREATE ROLE-Anweisung fest. Ziehen Sie in diesem Fall die Möglichkeit in Betracht, den Administratoren das MANAGE ROLES-Systemprivileg zu erteilen.

Die folgende Anweisung erstellt beispielsweise die Rolle myRole und legt die Benutzerinnen SallyG und IrisM als Administratorinnen fest:

```
CREATE ROLE myRole WITH ADMIN SallyG, IrisM, SYS_MANAGE_ROLES_ROLE;
```

### Siehe auch

- „CREATE ROLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „min\_role\_admins-Option“ auf Seite 638

## Superuser

Superuser sind Benutzer, die jedes Systemprivileg ausüben und jede Rolle verwalten dürfen. Sie können alle mit Privilegien verbundenen Vorgänge im System ausführen. Wenn eine neue Datenbank erstellt wird, ist der Standardbenutzer (DBA) der Superuser mit vollen Administrationsrechten. Der Benutzer DBA kann alle mit Privilegien verbundenen Vorgänge in einer neu erstellten Datenbank ausführen. Wenn allerdings eine neue Rolle erstellt wird und bei der Erstellung ein Rollenadministrator angegeben wurde, kann der Benutzer DBA nicht standardmäßig die Rolle verwalten. In diesem Fall müssen Sie daran denken, DBA die Rolle mit Administrationsrechten zu erteilen. Außerdem können Sie den Benutzer DBA löschen und einen eigenen Superuser erstellen.

Wenn Sie einen Superuser erstellen möchten, müssen Sie einen Benutzer erstellen und diesem die SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle erteilen. Wenn Sie SYS\_AUTH\_DBA\_ROLE migriert haben, müssen Sie dem Superuser manuell die gewünschten Rollen und Privilegien (mit

Administrationsrechten) erteilen. Ab diesem Zeitpunkt müssen Sie daran denken, dem Superuser alle neuen Rollen mit Administrationsrechten zu erteilen.

**Siehe auch**

- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen“ auf Seite 1275
- „Rollenadministratoren“ auf Seite 1293

## Rollen und Privilegien für Rollen konfigurieren (Sybase Central)

Für jede Rolle können Sie Rollen oder Privilegien erteilen, Rollen oder Privilegien entziehen sowie die Administrationsrechte festlegen, die die Rolle für die ihr erteilten Rollen und Privilegien haben soll.

**Voraussetzungen**

Wenn Sie eine Systemrolle erteilen oder entziehen möchten, benötigen Sie das **MANAGE ROLES**-Systemprivileg.

Wenn Sie eine Kompatibilitätsrolle erteilen oder entziehen möchten, benötigen Sie Administrationsrechte für die Rolle.

Wenn Sie **SYS\_RUN\_REPLICATION\_ROLE** erteilen oder entziehen möchten, benötigen Sie die **SYS\_REPLICATION\_ADMIN\_ROLE**-Systemrolle.

**Aufgabe**

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Rollen** und wählen Sie die zu ändernde Rolle aus.

Administratoroption	Aktion
Privilegien erteilen	<div>a. Klicken Sie im rechten Fensterausschnitt auf die relevante Privilegien-Registerkarte.</div> <div>b. Rechtsklicken Sie in den rechten Fensterausschnitt und wählen Sie <b>Neu » Privilegien</b>.</div> <div>c. Wählen Sie ein oder mehrere Privilegien aus der Liste und klicken Sie auf <b>OK</b>.</div>
Privilegien entziehen	<div>a. Klicken Sie im rechten Fensterausschnitt auf die relevante Privilegien-Registerkarte.</div> <div>b. Rechtsklicken Sie auf das zu entziehende Privileg und klicken Sie auf <b>Löschen</b>.</div>

Administratoroption	Aktion
Rollen erteilen	a. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte <b>Rollen</b> . b. Rechtsklicken Sie in den rechten Fensterausschnitt und wählen Sie <b>Neu » Erteilte Rollen</b> . c. Wählen Sie eine oder mehrere zu erteilende Rollen und klicken Sie auf <b>OK</b> .
Rollen entziehen	a. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte <b>Rollen</b> . b. Rechtsklicken Sie auf die zu entziehende Rolle und klicken Sie auf <b>Löschen</b> .

3. Klicken Sie auf **Datei » Speichern**.

### Ergebnisse

Die Rolle wird konfiguriert.

### Siehe auch

- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343

## Rollen und Privilegien für Rollen konfigurieren (SQL)

Für jede Rolle können Sie Rollen oder Privilegien erteilen, Rollen oder Privilegien entziehen sowie die Administrationsrechte festlegen, die die Rolle für die ihr erteilten Rollen und Privilegien haben soll.

### Voraussetzungen

Wenn Sie eine Systemrolle erteilen oder entziehen möchten, benötigen Sie das **MANAGE ROLES**-Systemprivileg.

Wenn Sie eine Kompatibilitätsrolle erteilen oder entziehen möchten, benötigen Sie Administrationsrechte für die Rolle.

Wenn Sie **SYS\_RUN\_REPLICATION\_ROLE** erteilen oder entziehen möchten, benötigen Sie die **SYS\_REPLICATION\_ADMIN\_ROLE**-Systemrolle.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie Anweisungen ähnlich den folgenden aus, je nachdem, welche Änderung Sie vornehmen möchten:

Option	Aktion
Privilegien erteilen	<code>GRANT privilege-name TO target-role-name;</code>
Privilegien entziehen	<code>REVOKE privilege-name FROM target-role-name;</code>
Rollen erteilen	<code>GRANT ROLE role-name TO target-role-name;</code>
Rollen entziehen	<code>REVOKE ROLE role-name FROM target-role-name;</code>

## Ergebnisse

Die Rolle wird konfiguriert.

## Beispiel

Wenn Sie der Rolle RolleA das CREATE ANY OBJECT-Systemprivileg erteilen möchten, ohne ihr Administrationsrechte zu geben, führen Sie die folgende Anweisung aus:

```
GRANT CREATE ANY OBJECT TO RoleA;
```

Wenn Sie der Rolle RolleA das CREATE ANY OBJECT-Systemprivileg erteilen möchten, zusammen mit der Möglichkeit, Benutzern und anderen Rollen das Systemprivileg zu erteilen oder zu entziehen, führen Sie die folgende Anweisung aus:

```
GRANT CREATE ANY OBJECT TO RoleA WITH ADMIN OPTION;
```

Wenn Sie der Benutzerin Jane die Rolle RolleB einschließlich der dazugehörigen Administrationsrechte erteilen möchten, führen Sie die folgende Anweisung aus:

```
GRANT ROLE RoleB TO Jane WITH ADMIN OPTION;
```

Wenn Sie dem Benutzer John die Administrationsrechte für RolleB erteilen möchten, jedoch ohne die Möglichkeit, diese Rolle zu nutzen, führen Sie die folgende Anweisung aus:

```
GRANT ROLE RoleB TO John WITH ADMIN ONLY OPTION;
```

## Siehe auch

- „Rollen und Privilegien für Rollen konfigurieren (Sybase Central)“ auf Seite 1296
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Rollen erteilen (Sybase Central)

Erteilen Sie eine Rolle einem Benutzer oder einer anderen Rolle.

### Voraussetzungen

Sie benötigen Administrationsrechte für die zu erteilende Rolle.

## Kontext und Bemerkungen

Sie können keine Administrationsrechte für Systemrollen erteilen. Nur Benutzer mit MANAGE ROLES-Systemprivileg haben Administrationsrechte für Systemrollen.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie auf **Benutzer** oder **Rollen** und wählen Sie einen Benutzer bzw. eine Rolle, dem bzw. der Sie die Rolle(n) erteilen möchten.
3. Klicken Sie im rechten Fensterausschnitt auf **Berechtigungsempfänger**.
4. Rechtsklicken Sie in den rechten Fensterausschnitt und wählen Sie **Neu » Berechtigungsempfänger**.
5. Klicken Sie auf den Benutzer bzw. die Rolle, dem bzw. der Sie die Rolle erteilen möchten, und anschließend auf **OK**.
6. (Optional) Verwenden Sie die Spalte **Adm.** (Administrationsrechte), um die Administrationsrechte für die Rolle zu ändern. Eine leere Spalte bedeutet, dass der Benutzer bzw. die Rolle keine Administrationsrechte für die Rolle hat. Ein Häkchen in der Spalte bedeutet, dass der Benutzer bzw. die Rolle die Rolle verwalten (erteilen oder entziehen) kann. Sie können keine Administrationsrechte für Systemrollen erteilen. Nur Benutzer mit MANAGE ROLES-Systemprivileg können Systemrollen verwalten. Klicken Sie in die Spalte, um die Option umzuschalten.  
  
(Optional) Verwenden Sie die Spalte **Ausü.** (Ausübungsrechte), um die Ausübungsrechte für den Benutzer bzw. die Rolle zu ändern. Ein Häkchen in der Spalte bedeutet, dass der Benutzer bzw. die Rolle die Rolle ausüben kann. Das Ausübungsprivileg wird standardmäßig erteilt. Klicken Sie in die Spalte, um die Option umzuschalten.
7. Klicken Sie auf **Datei » Speichern**.

## Ergebnisse

Die Rolle wird dem Benutzer bzw. der Rolle erteilt.

## Siehe auch

- [„Rollen“ auf Seite 1271](#)
- [„GRANT-Anweisung“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [„Vererbung von Rollen und Privilegien“ auf Seite 1348](#)
- [„Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391](#)
- [„Privilegien auf Objektebene erteilen \(Sybase Central\)“ auf Seite 1333](#)
- [„Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen \(Sybase Central\)“ auf Seite 1343](#)

## Rollen erteilen (SQL)

Erteilen Sie eine Rolle einem Benutzer oder einer anderen Rolle.

**Voraussetzungen**

Sie benötigen Administrationsrechte für die zu erteilende Rolle.

**Kontext und Bemerkungen**

Sie können keine Administrationsrechte für Systemrollen erteilen. Nur Benutzer mit MANAGE ROLES-Systemprivileg können Systemrollen verwalten.

**Aufgabe**

- 1. Stellen Sie eine Verbindung mit der Datenbank her.
- 2. Führen Sie eine GRANT ROLE-Anweisung aus. Zum Beispiel:

Option	Anweisung
Rollen ohne Administrationsrechte erteilen	<code>GRANT ROLE role-name TO userid;</code>
Rollen mit Administrationsrechten erteilen	<code>GRANT ROLE role-name TO userid WITH ADMIN OPTION;</code>
Nur Administrationsrechte für eine Rolle erteilen	<code>GRANT ROLE role-name TO userid WITH ADMIN ONLY OPTION;</code>

**Ergebnisse**

Die Rolle wird dem Benutzer bzw. der Rolle erteilt.

**Beispiel**

Wenn Sie der Benutzerin Jane die Rolle RolleB einschließlich der dazugehörigen Administrationsrechte erteilen möchten, führen Sie die folgende Anweisung aus:

`GRANT ROLE RoleB TO Jane WITH ADMIN OPTION`

Wenn Sie dem Benutzer John die Administrationsrechte für RolleB erteilen möchten, jedoch ohne die Möglichkeit, diese Rolle zu nutzen, führen Sie die folgende Anweisung aus:

`GRANT ROLE RoleB TO John WITH ADMIN ONLY OPTION`

**Siehe auch**

- „Rollen“ auf Seite 1271
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391
- „Privilegien auf Objektebene erteilen (Sybase Central)“ auf Seite 1333
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Rollen entziehen (Sybase Central)

Entziehen Sie eine Rolle einem Benutzer, einer benutzererweiterten Rolle oder einer benutzerdefinierten Rolle.

### Voraussetzungen

Sie benötigen Administrationsrechte für die betreffende Rolle, um benutzerdefinierte Rollen entziehen zu können. Sie benötigen das **MANAGE ROLES**-Systemprivileg, um Systemrollen entziehen zu können.

Der **SYS**-Rolle können Sie keine Rollen entziehen. Anderen Systemrollen können Sie Rollen entziehen, vorausgesetzt, diese Rollen gehören nicht zu den Standardrollen für die betreffende Systemrolle.

Sie können eine Rolle nur entziehen, wenn alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die `min_role_admin-`Datenbankoption festgelegt ist.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt entweder auf **Benutzer** oder auf **Rollen** und klicken Sie dann auf einen bestimmten Benutzer bzw. eine bestimmte Rolle.
3. Wählen Sie eine der folgenden Optionen:

Administratoroption	Aktion
Rollen Benutzern oder Rollen entziehen, denen die betreffende Rolle erteilt wurde	<ol style="list-style-type: none"> <li>a. Klicken Sie auf die Registerkarte <b>Berechtigungsempfänger</b>.</li> <li>b. Wenn Sie die Rolle einem Benutzer oder einer Rolle entziehen möchten, rechtsklicken Sie auf den Benutzer bzw. die Rolle und klicken Sie auf <b>Löschen</b>.</li> </ol>
Ausübungs- oder Administrationsrechte für eine Rolle entziehen	<ol style="list-style-type: none"> <li>a. Klicken Sie auf die Registerkarte <b>Rollen</b>.</li> <li>b. Wählen Sie eine Rolle aus, rechtsklicken Sie darauf und wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> <li>• <b>Entziehen » Ausübungsrechte</b>. Dies entspricht dem Ausführen der folgenden Anweisung: <pre>REVOKE ROLE "role-name" FROM "user/role-name"</pre> </li> <li>• <b>Entziehen » Administrationsrechte</b>. Dies entspricht dem Ausführen der folgenden Anweisung: <pre>REVOKE ADMIN OPTION FOR ROLE "role-name" FROM "user/role-name"</pre> </li> </ul> </li> </ol>

**Tipps**

Wenn Sie Ihre Änderungen rückgängig machen möchten, wählen Sie eine oder mehrere Zeilen aus und klicken Sie auf **Bearbeiten » Rückgängig**.

Wenn Sie die **Legende** aktivieren bzw. deaktivieren möchten, klicken Sie auf **Datei » Beschriftung anzeigen**.

4. Klicken Sie auf **Datei » Speichern**.

**Ergebnisse**

Die Rolle wird dem angegebenen Benutzer bzw. der angegebenen Rolle entzogen.

**Siehe auch**

- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277

## Rollen entziehen (SQL)

Entziehen Sie eine Rolle einem Benutzer, einer benutzererweiterten Rolle oder einer benutzerdefinierten Rolle.

**Voraussetzungen**

Sie benötigen Administrationsrechte für die betreffende Rolle, um benutzerdefinierte Rollen entziehen zu können. Sie benötigen das MANAGE ROLES-Systemprivileg, um Systemrollen entziehen zu können.

Der SYS-Rolle können Sie keine Rollen entziehen. Anderen Systemrollen können Sie Rollen entziehen, vorausgesetzt, diese Rollen gehören nicht zu den Standardrollen für die betreffende Systemrolle.

Sie können eine Rolle nur entziehen, wenn alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die min\_role\_admin-Datenbankoption festgelegt ist.

**Aufgabe**

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine REVOKE ROLE-Anweisung aus. Zum Beispiel:

Option	Anweisung
Rollen entziehen	<code>REVOKE ROLE role-name FROM userid;</code>
Administrationsrechte für eine Rolle entziehen, wobei Benutzer die Rolle weiterhin ausüben können	<code>REVOKE ADMIN OPTION FOR ROLE role-name FROM userid;</code>

## Ergebnisse

Die Rolle wird dem angegebenen Benutzer bzw. der angegebenen Rolle entzogen.

## Beispiel

Entziehen Sie dem Benutzer Jim die SYS\_AUTH\_RESOURCE\_ROLE-Kompatibilitätsrolle.

```
REVOKE ROLE SYS_AUTH_RESOURCE_ROLE FROM Jim;
```

Entziehen Sie der Benutzerin AnnW nur die Administrationsrechte für die Rolle myRole.

```
REVOKE ADMIN OPTION FOR ROLE myRole FROM AnnW;
```

## Siehe auch

- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Rollen entziehen (Sybase Central)“ auf Seite 1301
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277

## Rollen löschen (Sybase Central)

Löschen Sie benutzerdefinierte Rollen, benutzererweiterte Rollen und Kompatibilitätsrollen. Systemrollen können Sie nicht löschen.

### Voraussetzungen

Sie benötigen Administrationsrechte für die zu löschende Rolle.

Die zu löschende Rolle darf nicht Eigentümerin von Datenbankobjekten sein.

Sie können eine Rolle nur löschen, wenn alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die min\_role\_admin-Datenbankoption festgelegt ist.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie auf **Rollen** und wählen Sie die Rolle aus, die Sie löschen möchten.
3. Rechtsklicken Sie auf die Rolle und klicken Sie auf **Löschen**.

## Ergebnisse

Die Rolle wird gelöscht und allen Benutzern oder Rollen entzogen, denen sie erteilt war. Wenn Sie eine Rolle löschen, die durch das MANAGE ROLES-Systemprivileg verwaltet werden kann, wird die Rolle auch dem MANAGE ROLES-Systemprivileg entzogen.

### Siehe auch

- „DROP ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „min\_role\_admins-Option“ auf Seite 638
- „Benutzererweiterte Rollen in Benutzer zurückkonvertieren (Sybase Central)“ auf Seite 1291

## Rollen löschen (SQL)

Löschen Sie benutzerdefinierte Rollen, benutzererweiterte Rollen und Kompatibilitätsrollen. Systemrollen können Sie nicht löschen.

### Voraussetzungen

Sie benötigen Administrationsrechte für die zu löschende Rolle.

Sie können eine Rolle nur löschen, wenn alle abhängigen Rollen die erforderliche minimale Anzahl von Administratorbenutzern mit aktiven Kennwörtern erfüllen, die durch die min\_role\_admin-Datenbankoption festgelegt ist.

### Aufgabe

- Führen Sie eine DROP ROLE-Anweisung aus. Zum Beispiel:

```
DROP ROLE role-name;
```

Wenn die Rolle Benutzern zugeordnet ist, müssen Sie zum Löschen der Rolle die WITH REVOKE-Klausel angeben:

```
DROP ROLE role-name WITH REVOKE;
```

Wenn die Rolle Eigentümerin von Objekten ist, müssen Sie zum Löschen der Rolle die WITH DROP OBJECTS-Klausel angeben:

```
DROP ROLE role-name WITH DROP OBJECTS;
```

### Ergebnisse

Die Rolle wird gelöscht.

### Beispiel

Angenommen, in Ihrer Organisation wurde niemandem die SYS\_AUTH\_VALIDATE\_ROLE-Kompatibilitätsrolle erteilt. Sie können sie löschen, indem Sie die folgende Anweisung ausführen:

```
DROP ROLE SYS_AUTH_VALIDATE_ROLE;
```

Wenn Benutzer vorhanden sind, denen die SYS\_AUTH\_VALIDATE\_ROLE-Kompatibilitätsrolle erteilt wurde, können Sie sie trotzdem löschen, indem Sie die folgende Anweisung ausführen:

```
DROP ROLE SYS_AUTH_VALIDATE_ROLE WITH REVOKE;
```

Die folgende Anweisung löscht die SYS\_AUTH\_DBA\_ROLE-Systemrolle. Dieser Vorgang ist möglich, wenn alle dazugehörigen Systemprivilegien in anderen Rollen vorhanden sind, wobei die entsprechende Anzahl an Administratoren für diese Rollen erfüllt sein muss, wie durch die min\_role\_admins-Datenbankoption festgelegt. Die WITH REVOKE-Klausel wird hinzugefügt, weil die Rolle wahrscheinlich anderen Benutzer zugeordnet wurde.

```
DROP ROLE SYS_AUTH_DBA_ROLE WITH REVOKE;
```

#### Siehe auch

- „min\_role\_admins-Option“ auf Seite 638
- „DROP ROLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen“ auf Seite 1275

## Privilegien

Ein Privileg ist ein Recht, einen mit Privilegien verbundenen Vorgang im System auszuführen. Das Ändern einer Tabelle ist beispielsweise ein mit Privilegien verbundener Vorgang, je nach Art der Änderung, die Sie vornehmen. Es gibt zwei Arten von Privilegien: Systemprivilegien und Privilegien auf Objektebene. **Systemprivilegien** geben Ihnen das allgemeine Recht, einen mit Privilegien verbundenen Vorgang auszuführen, während **Privilegien auf Objektebene** Sie darauf beschränken, den Vorgang für ein bestimmtes Objekt auszuführen. Wenn Sie beispielsweise das ALTER ANY TABLE-Systemprivileg haben, können Sie jede beliebige Tabelle im System ändern. Wenn dies nicht der Fall ist, können Sie nur Tabellen bearbeiten, die Sie erstellen, oder Tabellen, für die Sie das ALTER TABLE-Privileg auf Objektebene haben.

Systemprivilegien sind in die Datenbank integriert und können erteilt oder entzogen, jedoch weder erstellt noch gelöscht werden. Mit Ausnahme der Privilegien MANAGE ROLES und UPGRADE ROLE können Systemprivilegien nicht geändert werden. Jedes Systemprivileg, mit Ausnahme des SET USER-Systemprivilegs, wird standardmäßig entweder der SYS\_AUTH\_SA\_ROLE-Systemrolle oder der SYS\_AUTH\_SSO\_ROLE-Systemrolle erteilt, aber nicht beiden. Das SET USER-Systemprivileg wird beiden Rollen erteilt (WITH ADMIN OPTION für SYS\_AUTH\_SSO\_ROLE und WITH NO ADMIN OPTION für SYS\_AUTH\_SA\_ROLE).

Sie können Systemprivilegien und Privilegien auf Objektebene mithilfe der Anweisungen GRANT und REVOKE erteilen und entziehen.

#### Siehe auch

- „sp\_has\_role-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Objektprivilegien

Diese Liste enthält die Privilegien auf Objektebene in SQL Anywhere. Sie können die Rollen und Privilegien, die ein Benutzer hat, in Sybase Central anzeigen, indem Sie darauf klicken und die

angezeigten Details durchgehen. Sie können die Details auch mit der sp\_has\_role-Systemprozedur abrufen. Siehe „[Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen \(Sybase Central\)](#)“ auf Seite 1343 und „[Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen \(SQL\)](#)“ auf Seite 1344.

Privilegname	Unterstützung durch Datenbankobjekte	Über Gruppen mitgliederschaft vererbt?	WITH GRANT OPTION beim Erteilen zulässig?	Beschreibung
ALL	Tabellen, Ansichten	Ja	Ja	Ermöglicht es einem Benutzer, alle mit dem Datenbankobjekt zusammenhängenden Aufgaben auszuführen. Mit diesem Privileg werden die folgenden Privilegien für Tabellen erteilt: ALTER, DELETE, INSERT, REFERENCES, SELECT und UPDATE. Mit diesem Privileg werden die folgenden Privilegien für Ansichten erteilt: DELETE, INSERT, SELECT und UPDATE. Durch Erteilen von ALL werden auch die Privilegien LOAD und TRUNCATE erteilt.
ALTER	Tabellen	Ja	Ja	Ermöglicht es einem Benutzer, die Struktur einer Tabelle zu ändern oder einen Trigger für die Tabelle zu erstellen. Da der Benutzer mit diesem Privileg die Berechtigung zum Ändern des Datenbankschemas erhält, sollte es den meisten Benutzern nicht erteilt werden.
CONNECT	Datenbanken	Nein	Nein	Ermöglicht es einem Benutzer, eine Verbindung mit der aktuellen Datenbank herzustellen.
CONSOLIDATE	Benutzer	Nein	Nein	Ermöglicht es einem Benutzer, eine konsolidierte Datenbank in SQL Remote zu identifizieren.

Privilegname	Unterstützung durch Datenbankobjekte	Über Gruppen mitgliederschaft vererbt?	WITH GRANT OPTION beim Erteilen zulässig?	Beschreibung
CREATE ON	DBSpaces	Ja	Ja	Ermöglicht es einem Benutzer, Objekte im DBSpace zu erstellen. Welche zusätzlichen Privilegien erforderlich sind, hängt von dem zu erstellenden Objekt ab. Zum Erstellen einer Tabelle ist beispielsweise eines der Privilegien CREATE TABLE, CREATE ANY TABLE oder CREATE ANY OBJECT erforderlich.
DELETE	Tabellen, Ansichten	Nein	Ja	Ermöglicht es einem Benutzer, Zeilen aus der Tabelle oder Ansicht zu löschen.
EXECUTE	Trigger, Prozeduren, benutzerdefinierte Funktionen	Nein	Nein	Ermöglicht es einem Benutzer, die Prozedur oder benutzerdefinierte Funktion auszuführen.
INSERT	Tabellen, Ansichten	Ja	Ja	Ermöglicht es einem Benutzer, Zeilen in eine Tabelle oder Ansicht einzufügen.
INTEGRATED LOGIN	Datenbanken	Nein	Nein	Ermöglicht es einem Benutzer, eine Verbindung mit der aktuellen Datenbank unter Verwendung eines integrierten Logins herzustellen.
KERBEROS LOGIN	Datenbanken	Nein	Nein	Ermöglicht es einem Benutzer, eine Verbindung mit der aktuellen Datenbank unter Verwendung eines Kerberos-Logins herzustellen.
LOAD	Tabellen	Ja	Ja	Ermöglicht es einem Benutzer, die Tabelle zu laden, wenn die Datenbankoption -gl auf einen anderen Wert als NONE gesetzt ist.
PUBLISH	Benutzer	Nein	Nein	Identifiziert die Benutzer-ID für eine Datenbank in SQL Remote.

Privilegname	Unterstützung durch Datenbankobjekte	Über Gruppenmitgliedschaft vererbt?	WITH GRANT OPTION beim Erteilen zulässig?	Beschreibung
REFERENCES	Tabellen	Ja	Ja	<p>Ermöglicht es einem Benutzer, Indizes für die Tabelle zu erstellen und Fremdschlüssel, die die Tabelle referenzieren. Dieses Privileg kann auch für einzelne Spalten einer Tabelle erteilt werden. Da der Benutzer mit diesem Privileg das Datenbankschema ändern kann, sollte es den meisten Benutzern nicht erteilt werden.</p> <p>Wenn die Spaltennamen angegeben werden, darf der Benutzer nur diese Spalten in der Tabelle indizieren.</p>
REMOTE	Benutzer	Nein	Nein	Ermöglicht es einem Benutzer, eine entfernte Datenbank in SQL Remote und MobiLink zu identifizieren.
SELECT	Tabellen, Ansichten	Ja	Ja	<p>Ermöglicht es einem Benutzer, die Tabelle oder eine Ansicht abzufragen. Dieses Privileg kann auch für einzelne Spalten einer Tabelle erteilt werden.</p> <p>Wenn die Spaltennamen angegeben werden, darf der Benutzer nur diese Spalten in der Tabelle anzeigen.</p>
TRUNCATE	Tabellen, materialisierte Ansichten	Ja	Ja	Ermöglicht es einem Benutzer, die Tabelle oder materialisierte Ansicht zu kürzen.
UPDATE	Tabellen, Ansichten	Ja	Ja	Ermöglicht es einem Benutzer, Zeilen in der Tabelle oder Ansicht zu aktualisieren. Dieses Privileg kann auch für einzelne Spalten einer Tabelle erteilt werden.
USAGE	Sequenzgeneratoren	Nein	Ja	Ermöglicht es einem Benutzer, den aktuellen oder nächsten Wert in der Sequenz auszuwerten.

## Weitere Hinweise

**WITH GRANT OPTION wird nicht von Gruppenmitgliedern geerbt** Während einige Privilegien auf Objektebene vererbbar sind, ist WITH GRANT OPTION nie vererbbar. Wenn beispielsweise einer benutzererweiterten Rolle, BenutzerA, das SELECT-Privileg für eine Tabelle erteilt und dabei WITH GRANT OPTION angegeben wird, kann BenutzerA SELECT-Anweisungen für die Tabelle ausführen und anderen das SELECT-Privileg für diese Tabelle erteilen. Berechtigungsempfänger dieser benutzererweiterten Rolle erben das SELECT-Privileg für die Tabelle, aber nicht die Möglichkeit, das SELECT-Privileg anderen zu erteilen.

**Ansichten** Sie können Privilegien für deaktivierte Ansichten erteilen. Privilegien für deaktivierte Ansichten werden in der Datenbank gespeichert und treten in Kraft, wenn die betreffende Ansicht aktiviert wird.

**Prozeduren** Ein Benutzer muss Eigentümer der Prozedur sein oder das EXECUTE-Privileg dafür haben, um sie ausführen zu können.

Außerdem gilt: Wenn die Prozedurdefinition SQL SECURITY DEFINER enthält, wird die Prozedur mit den Privilegien des Prozedureigentümers ausgeführt und nicht mit denjenigen des Benutzers, der die Prozedur aufruft. Wenn die Prozedurdefinition SQL SECURITY INVOKER enthält, wird die Prozedur mit den Privilegien ausgeführt, die der Aufrufer hat.

**DBSpaces** Jeder Benutzer, dem das CREATE ON-Privileg für DBSpaces erteilt wird, muss auch das entsprechende CREATE-Privileg zum Erstellen der gewünschten Objekte haben.

**Sequenzen** Das USAGE-Privileg ist das einzige Privileg, das für Sequenzgeneratoren erteilt wird. Mit diesem Privileg können Benutzer den aktuellen oder nächsten Wert in einer Sequenz auswerten. Wenn die Sequenz Teil einer DEFAULT-Klausel für eine Tabelle ist, muss jeder Benutzer, der eine Zeile in die Tabelle einfügt, das Privileg für die Sequenz haben.

## Siehe auch

- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „sp\_objectpermission-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Privilegien auf Objektebene erteilen (Sybase Central)“ auf Seite 1333
- „GRANT ROLE SYS\_RUN\_REPLICATION\_ROLE-Anweisung [MobiLink] [SQL Remote]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Integrierte Windows-Logins“ auf Seite 52
- „Kerberos-Authentifizierung“ auf Seite 63

## Systemprivilegien

In dieser Tabelle sind die Systemprivilegien in SQL Anywhere nach dem Objekt- oder Vorgangstyp aufgelistet, auf den sie sich beziehen. Sie können die Rollen und Privilegien, die ein Benutzer hat, über Sybase Central anzeigen, indem Sie darauf klicken und die angezeigten Details durchgehen. Sie können die Details auch mit der sp\_displayroles-Systemprozedur abrufen. Siehe „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343 und „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344.

**Hinweis**

Standardmäßig erbt ein Benutzer, der die SYS\_RUN\_REPLICATION\_ROLE-Systemrolle hat, alle Systemprivilegien. Dies liegt daran, dass SYS\_RUN\_REPLICATION\_ROLE die SYS\_AUTH\_DBA\_ROLE-Systemrolle erteilt wurde. Sie können die SYS\_AUTH\_DBA\_ROLE-Systemrolle aus SYS\_RUN\_REPLICATION\_ROLE entfernen, um dies zu verhindern, und anschließend der SYS\_RUN\_REPLICATION\_ROLE-Systemrolle nur die Privilegien erteilen, die Ihre Replikation erfordert. Ein Benutzer, dem die SYS\_RUN\_REPLICATION\_ROLE-Systemrolle erteilt wird, kann für entfernte Verbindungen nur die Privilegien dieser Rolle ausüben. Siehe „[Sicherheitshinweise zu rollenbasierter Zugriffssteuerung und Synchronisation](#)“ [*MobiLink - Clientadministration*].

Systemprivileg nach Objekt oder Funktionen	Beschreibung	Benutzer/Rollen können erben aus:
<b>Datenbanken</b>		
ALTER DATA-BASE	Ermöglicht einem Benutzer Folgendes: <ul style="list-style-type: none"> <li>• Upgrade von Datenbanken.</li> <li>• Kostenmodellkalibrierung ausführen.</li> <li>• Datenbankstatistiken laden.</li> <li>• Transaktionslogs ändern. (Erfordert auch das SERVER OPERATOR-Systemprivileg.)</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
BACKUP DATA-BASE	Ermöglicht es einem Benutzer, eine Datenbank zu sichern.	<ul style="list-style-type: none"> <li>• DIAGNOSTICS</li> <li>• SYS_AUTH_BACKUP_ROLE</li> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_PROFILE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
CHECKPOINT	Ermöglicht es einem Benutzer, einen Datenbankserver zum Ausführen eines Checkpoints zu zwingen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
DROP CONNECTION	Ermöglicht es einem Benutzer, Verbindungen mit der Datenbank zu löschen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
MANAGE PROFILING	Ermöglicht es einem Benutzer, die Datenbankserverprotokollierung für die Anwendungsprofilerstellung zu verwalten.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_PROFILE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
MONITOR	Ermöglicht es einem Benutzer, eine Datenbank zu überwachen, einschließlich des Zugriffs auf durch Privilegien geschützte Statistiken, verbundene Benutzer und Sperren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
<b>Datenbankoptionen</b>		
SET ANY PUBLIC OPTION	Ermöglicht es einem Benutzer, PUBLIC-Datenbankoptionen festzulegen, die nicht das Systemprivileg SET ANY SECURITY OPTION oder SET ANY SYSTEM OPTION erfordern.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> </ul>
SET ANY SECURITY OPTION	Ermöglicht es einem Benutzer, PUBLIC-Sicherheitsdatenbankoptionen festzulegen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
SET ANY SYSTEM OPTION	Ermöglicht es einem Benutzer, PUBLIC-Systemdatenbankoptionen festzulegen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
SET ANY USER DEFINED OPTION	Ermöglicht es einem Benutzer, benutzerdefinierte Datenbankoptionen festzulegen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> </ul>
<b>Datentypen</b>		
ALTER DATA-TYPE	Ermöglicht es einem Benutzer, Datentypen zu ändern.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE DATA-TYPE	Ermöglicht es einem Benutzer, Datentypen zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP DATA-TYPE	Ermöglicht es einem Benutzer, Datentypen zu löschen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>DBSpaces</b>		
MANAGE ANY DBSPACE	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• DBSpaces erstellen, ändern, löschen und kommentieren.</li> <li>• CREATE-Privilegien für DBSpaces erteilen und entziehen.</li> <li>• Daten in beliebige DBSpaces verschieben.</li> <li>• Datenbankfunktion zum Löschen von Dateien ausführen.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
<b>Debugging</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
DEBUG ANY PROCEDURE	Ermöglicht es einem Benutzer, das Debugging von Prozeduren, Funktionen, Triggern und Ereignissen auszuführen.	<ul style="list-style-type: none"> <li>• SA_DEBUG</li> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Ereignisse</b>		
MANAGE ANY EVENT	Ermöglicht es einem Benutzer, Ereignisse zu erstellen, zu ändern, zu löschen, auszulösen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
<b>Externe Umgebungen</b>		
CREATE EXTERNAL REFERENCE	<p>Ermöglicht es einem Benutzer, externe Referenzen in der Datenbank zu erstellen.</p> <p>Sie müssen die Systemprivilegien haben, die zum Erstellen bestimmter Datenbankobjekte erforderlich sind, bevor Sie externe Referenzen erstellen können.</p> <p>Das Erstellen eines im eigenen Eigentum stehenden Textkonfigurationsobjekts, das einen externen Begriffsegmentierer und/oder Vorfilter verwendet, erfordert sowohl das CREATE TEXT CONFIGURATION-Systemprivileg als auch das CREATE EXTERNAL REFERENCE-Systemprivileg.</p>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
MANAGE ANY EXTERNAL ENVIRONMENT	Ermöglicht es einem Benutzer, externe Umgebungen zu ändern, zu kommentieren, zu starten und zu stoppen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
MANAGE ANY EXTERNAL OBJECT	Ermöglicht es einem Benutzer, externe Umgebungsobjekte zu installieren, zu kommentieren und zu entfernen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
<b>Dateien</b>		
READ CLIENT FILE	Ermöglicht es einem Benutzer, Dateien auf dem Clientcomputer zu lesen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_READCLIENTFILE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
READ FILE	Ermöglicht es einem Benutzer, Dateien auf dem Datenbankservercomputer zu lesen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_READFILE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
WRITE CLIENT FILE	Ermöglicht es einem Benutzer, Dateien auf dem Clientcomputer zu schreiben.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_AUTH_WRITECLIENTFILE_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
WRITE FILE	Ermöglicht es einem Benutzer, Dateien auf dem Datenbankservercomputer zu schreiben.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_AUTH_WRITEFILE_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Indizes</b>		
ALTER ANY INDEX	Ermöglicht es einem Benutzer, Indizes und Textindizes für Tabellen und Ansichten zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• DIAGNOSTICS</li> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_PROFILE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE ANY INDEX	Ermöglicht es einem Benutzer, Indizes und Textindizes für Tabellen und Ansichten zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
DROP ANY INDEX	Ermöglicht es einem Benutzer, Indizes und Textindizes für Tabellen und Ansichten zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>LDAP</b>		
MANAGE ANY LDAP SERVER	Ermöglicht es einem Benutzer, LDAP-Server zu erstellen, zu ändern, zu löschen, zu validieren und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Materialisierte Ansichten</b>		
ALTER ANY MATERIALIZED VIEW	Ermöglicht es einem Benutzer, materialisierte Ansichten zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE ANY MATERIALIZED VIEW	Ermöglicht es einem Benutzer, materialisierte Ansichten zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE MATERIALIZED VIEW	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende materialisierte Ansichten zu erstellen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP ANY MATERIALIZED VIEW	Ermöglicht es einem Benutzer, materialisierte Ansichten zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Nachrichten</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
CREATE MES- SAGE	Ermöglicht es einem Benutzer, Nachrichten zu erstellen.	<ul style="list-style-type: none"><li>• SYS_AUTH_DBA_ROLE</li><li>• SYS_AUTH_RESOURCE_ROLE</li><li>• SYS_AUTH_SA_ROLE</li><li>• SYS_RUN_REPLICATION_ROLE</li></ul>
DROP MES- SAGE	Ermöglicht es einem Benutzer, Nachrichten zu löschen.	<ul style="list-style-type: none"><li>• SYS_AUTH_DBA_ROLE</li><li>• SYS_AUTH_SA_ROLE</li><li>• SYS_RUN_REPLICATION_ROLE</li></ul>
<b>Verschiedenes</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
ALTER ANY OBJECT	<p>Ermöglicht es einem Benutzer, Objekte der folgenden Typen zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören:</p> <ul style="list-style-type: none"> <li>• Datentypen</li> <li>• Ereignisse</li> <li>• Funktionen</li> <li>• Indizes</li> <li>• Materialisierte Ansichten</li> <li>• Nachrichten</li> <li>• Prozeduren</li> <li>• Sequenzgeneratoren</li> <li>• Räumliche Bezugssysteme</li> <li>• Räumliche Maßeinheiten</li> <li>• Statistiken</li> <li>• Tabellen</li> <li>• Textkonfigurationsobjekte</li> <li>• Textindizes</li> <li>• Trigger</li> <li>• Ansichten</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
ALTER ANY OBJECT OWNER	Ermöglicht es einem Benutzer, den Eigentümer von Objekten beliebigen Typs zu ändern.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
COMMENT ANY OBJECT	Ermöglicht es einem Benutzer, Objekte beliebigen Typs zu kommentieren, die mit dem CREATE ANY OBJECT-Systemprivileg erstellt werden können.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
CREATE ANY OBJECT	<p>Ermöglicht es einem Benutzer, Objekte der folgenden Typen zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören:</p> <ul style="list-style-type: none"><li>• Datentypen</li><li>• Ereignisse</li><li>• Funktionen</li><li>• Indizes</li><li>• Materialisierte Ansichten</li><li>• Nachrichten</li><li>• Prozeduren</li><li>• Sequenzgeneratoren</li><li>• Räumliche Bezugssysteme</li><li>• Räumliche Maßeinheiten</li><li>• Statistiken</li><li>• Tabellen</li><li>• Textkonfigurationsobjekte</li><li>• Textindizes</li><li>• Trigger</li><li>• Ansichten</li></ul>	<ul style="list-style-type: none"><li>• SYS_AUTH_DBA_ROLE</li><li>• SYS_AUTH_SA_ROLE</li><li>• SYS_RUN_REPLICATION_ROLE</li></ul>

Systemprivileg nach Objekt oder Funktionen	Beschreibung	Benutzer/Rollen können erben aus:
DROP ANY OBJECT	<p>Ermöglicht es einem Benutzer, Objekte der folgenden Typen zu löschen, die einem beliebigen Benutzer gehören:</p> <ul style="list-style-type: none"> <li>• Datentypen</li> <li>• Ereignisse</li> <li>• Funktionen</li> <li>• Indizes</li> <li>• Materialisierte Ansichten</li> <li>• Nachrichten</li> <li>• Prozeduren</li> <li>• Sequenzgeneratoren</li> <li>• Räumliche Bezugssysteme</li> <li>• Räumliche Maßeinheiten</li> <li>• Statistiken</li> <li>• Tabellen</li> <li>• Textkonfigurationsobjekte</li> <li>• Textindizes</li> <li>• Trigger</li> <li>• Ansichten</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
MANAGE ANY OBJECT PRIVILEGE	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Privilegien SELECT, INSERT, DELETE, UPDATE ALTER, REFERENCES, LOAD und TRUNCATE für Tabellen erteilen und entziehen, die einem beliebigen Benutzer gehören.</li> <li>• Privilegien SELECT, INSERT, DELETE und UPDATE für Ansichten erteilen und entziehen, die einem beliebigen Benutzer gehören.</li> <li>• EXECUTE-Privilegien für Prozeduren und Funktionen erteilen und entziehen, die einem beliebigen Benutzer gehören.</li> <li>• USAGE-Privilegien für Sequenzgeneratoren erteilen und entziehen, die einem beliebigen Benutzer gehören.</li> <li>• CREATE-Privilegien für DBSpaces erteilen und entziehen.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
MANAGE CERTIFICATES	Ermöglicht es einem Benutzer, Zertifikate zu erstellen, zu ändern, zu löschen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
REORGANIZE ANY OBJECT	Ermöglicht es einem Benutzer, Tabellen und materialisierte Ansichten zu reorganisieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
VALIDATE ANY OBJECT	Ermöglicht es einem Benutzer, Tabellen, materialisierte Ansichten, Indizes und Textindizes zu validieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_AUTH_VALIDATE_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Spiegelserver</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
MANAGE ANY MIRROR SERVER	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Spiegelservers erstellen, ändern, löschen und kommentieren.</li> <li>• Spiegelserverparameter ändern.</li> <li>• Spiegelserveroptionen festlegen.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Prozeduren</b>		
ALTER ANY PROCEDURE	Ermöglicht es einem Benutzer, Prozeduren und Funktionen zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
CREATE ANY PROCEDURE	Ermöglicht es einem Benutzer, Prozeduren und Funktionen zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
CREATE PROCEDURE	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende Prozeduren und Funktionen zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP ANY PROCEDURE	Ermöglicht es einem Benutzer, Prozeduren und Funktionen zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
EXECUTE ANY PROCEDURE	Ermöglicht es einem Benutzer, Prozeduren und Funktionen auszuführen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Auditing</b>		
MANAGE AUDITING	Ermöglicht es einem Benutzer, die sa_audit_string-Systemprozedur auszuführen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>E-Mail</b>		
SEND EMAIL	<p>Ermöglicht es einem Benutzer, die folgenden mit E-Mail zusammenhängenden Systemprozeduren auszuführen:</p> <ul style="list-style-type: none"> <li>• xp_get_mail_error_code</li> <li>• xp_get_mail_error_text</li> <li>• xp_startmail</li> <li>• xp_stopmail</li> <li>• xp_startsmtp</li> <li>• xp_stopsmtp</li> <li>• xp_sendmail</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Replikation</b>		

Systemprivileg nach Objekt oder Funktionen	Beschreibung	Benutzer/Rollen können erben aus:
MANAGE REPLICATION	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Publikationen erstellen, ändern, löschen und kommentieren.</li> <li>• MobiLink-Benutzer erstellen, ändern und löschen.</li> <li>• SQL Remote- und Synchronisations-subskriptionen erstellen, ändern, löschen, starten, stoppen und synchronisieren.</li> <li>• Synchronisationsprofile erstellen, ändern, löschen und kommentieren.</li> <li>• SQL Remote-Nachrichtentypen erstellen, ändern, löschen und kommentieren.</li> <li>• Entfernte Optionen festlegen.</li> <li>• Schemasynchronisation starten und stoppen.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Rollen</b>		
MANAGE ROLES	<p>Ermöglicht es einem Benutzer, neue Rollen zu erstellen und als globaler Administrator für neue und bestehende Rollen zu fungieren. Standardmäßig werden MANAGE ROLES Administrationsrechte für jede neu erstellte Rolle erteilt.</p> <p>Administrationsrechte für eine Rolle können Benutzern auch direkt erteilt werden, entweder während oder nach der Erstellung der Rolle. Wenn Administrationsrechte direkt erteilt wurden, benötigt der betreffende Benutzer nicht das MANAGE ROLES-Systemprivileg, um die Rolle verwalten zu können.</p> <p>Siehe <a href="#">„Rollenadministratoren“ auf Seite 1293</a>.</p>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
UPGRADE ROLE	Ermöglicht es einem Benutzer, Standardadministrator eines beliebigen Systemprivilegs zu werden, das beim Upgrade einer SQL Anywhere-Datenbank auf die Version 16.0 eingeführt wird.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Sequenzen</b>		
ALTER ANY SEQUENCE	Ermöglicht es einem Benutzer, Sequenzgeneratoren zu ändern, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE ANY SEQUENCE	Ermöglicht es einem Benutzer, Sequenzgeneratoren unabhängig vom Eigentümer zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP ANY SEQUENCE	Ermöglicht es einem Benutzer, Sequenzgeneratoren zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
USE ANY SEQUENCE	Ermöglicht es einem Benutzer, Sequenzgeneratoren zu verwenden, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Serveroperatoren</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
SERVER OPERATOR	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Datenbanken erstellen, wiederherstellen, löschen, starten und stoppen, Eigentümer von Datenbanken ändern und (nur) Katalog wiederherstellen.</li> <li>• Fremdserver und Verzeichniszugriffsserver erstellen, ändern und löschen.</li> <li>• Servercaches verwalten.</li> <li>• Datenbankserver starten und stoppen.</li> <li>• Verschlüsselte und entschlüsselte Datenbanken und Dateien erstellen.</li> <li>• Transaktionslogs von Datenbanken ändern.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
<b>Räumliche Objekte</b>		
MANAGE ANY SPATIAL OBJECT	Ermöglicht es einem Benutzer, räumliche Bezugssysteme und räumliche Maßeinheiten zu erstellen, zu ändern, zu löschen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SPATIAL_ADMIN_ROLE</li> </ul>
<b>Statistiken</b>		
MANAGE ANY STATISTICS	Ermöglicht es einem Benutzer, Datenbankstatistiken für eine beliebige Tabelle zu erstellen, zu ändern, zu löschen und zu aktualisieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Tabellen</b>		

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
ALTER ANY TABLE	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Tabellen (einschließlich Proxytabellen) ändern und kommentieren, die einem beliebigen Benutzer gehören.</li> <li>• Spalten in Tabellen (einschließlich Proxytabellen) kommentieren, die einem beliebigen Benutzer gehören.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATI-ON_ROLE</li> </ul>
CREATE ANY TABLE	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Tabellen (einschließlich Proxytabellen) erstellen und kommentieren, die einem beliebigen Benutzer gehören.</li> <li>• Spalten in Tabellen (einschließlich Proxytabellen) kommentieren, die einem beliebigen Benutzer gehören.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATI-ON_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATI-ON_ROLE</li> <li>• SYS_SAMONI-TOR_ADMIN_ROLE</li> </ul>
CREATE PROXY TABLE	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende Proxytabellen zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATI-ON_ROLE</li> </ul>
CREATE TABLE	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende Tabellen zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATI-ON_ROLE</li> </ul>
DELETE ANY TABLE	Ermöglicht es einem Benutzer, Zeilen in Tabellen und Ansichten zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATI-ON_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
DROP ANY TABLE	Ermöglicht es einem Benutzer, Tabellen (einschließlich Proxytabellen) zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
INSERT ANY TABLE	Ermöglicht es einem Benutzer, Zeilen in Tabellen und Ansichten einzufügen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
LOAD ANY TABLE	Ermöglicht es einem Benutzer, Daten in Tabellen zu laden, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
SELECT ANY TABLE	Ermöglicht es einem Benutzer, Tabellen und Ansichten abzufragen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
TRUNCATE ANY TABLE	Ermöglicht es einem Benutzer, Daten in Tabellen und materialisierten Ansichten zu kürzen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
UPDATE ANY TABLE	Ermöglicht es einem Benutzer, Zeilen in Tabellen und Ansichten zu aktualisieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Textkonfigurationsobjekte</b>		
ALTER ANY TEXT CONFIGURATION	Ermöglicht es einem Benutzer, Textkonfigurationsobjekte zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
CREATE ANY TEXT CONFIGURATION	Ermöglicht es einem Benutzer, Textkonfigurationsobjekte zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE TEXT CONFIGURATION	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende Textkonfigurationsobjekte zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP ANY TEXT CONFIGURATION	Ermöglicht es einem Benutzer, Textkonfigurationsobjekte zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Protokollierung</b>		
MANAGE ANY TRACE SESSION	Ermöglicht es einem Benutzer, alle mit der Ereignisprotokollierung zusammenhängenden Vorgänge auszuführen, bis auf das Auslösen von Benutzer-Trace-Ereignissen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
NOTIFY TRACE EVENT	Ermöglicht es einem Benutzer, ein Benutzer-Trace-Ereignis auszulösen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Trigger</b>		
ALTER ANY TRIGGER	Ermöglicht es einem Benutzer, Trigger in Tabellen und Ansichten zu ändern und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE ANY TRIGGER	Ermöglicht es einem Benutzer, Trigger in Tabellen und Ansichten zu erstellen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>

Systemprivileg nach Objekt oder Funktionen	Beschreibung	Benutzer/Rollen können erben aus:
<b>Benutzer und Login-Verwaltung</b>		
CHANGE PASSWORD	<p>Ermöglicht es einem Benutzer, Benutzerkennwörter für jeden Benutzer zu verwalten.</p> <p>Dieses Systemprivileg kann für alle Benutzer gelten oder auf eine Gruppe von angegebenen Benutzern beschränkt sein bzw. auf Benutzer, denen eine oder mehrere angegebene Rollen erteilt werden.</p> <p>Dieses Systemprivileg benötigt ein Benutzer nicht, um sein eigenes Kennwort zu ändern.</p>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
MANAGE ANY LOGIN POLICY	Ermöglicht es einem Benutzer, Login-Richtlinien zu erstellen, zu ändern, zu löschen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>
MANAGE ANY USER	<p>Ermöglicht einem Benutzer Folgendes:</p> <ul style="list-style-type: none"> <li>• Datenbankbenutzer erstellen, ändern, löschen und kommentieren (einschließlich Zuordnen eines anfänglichen Kennworts).</li> <li>• Kennwortänderung beim nächsten Login für Benutzer erzwingen.</li> <li>• Login-Richtlinie für Benutzer zuordnen und zurücksetzen.</li> <li>• Integrierte Logins und Kerberos-Logins erstellen, löschen und kommentieren.</li> <li>• Externe Logins erstellen und löschen.</li> </ul>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_SAMONITOR_ADMIN_ROLE</li> </ul>

<b>Systemprivileg nach Objekt oder Funktionen</b>	<b>Beschreibung</b>	<b>Benutzer/Rollen können erben aus:</b>
SET USER	<p>Ermöglicht es einem Benutzer, vorübergehend die Rollen und Privilegien eines anderen Benutzers anzunehmen.</p> <p>Dieses Systemprivileg kann für alle Benutzer gelten oder auf eine Gruppe von angegebenen Benutzern beschränkt sein bzw. auf Benutzer, denen eine oder mehrere angegebene Rollen erteilt werden.</p>	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_AUTH_SSO_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Ansichten</b>		
ALTER ANY VIEW	Ermöglicht es einem Benutzer, Ansichten zu ändern und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE ANY VIEW	Ermöglicht es einem Benutzer, Ansichten zu erstellen und zu kommentieren, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
CREATE VIEW	Ermöglicht es einem Benutzer, im eigenen Eigentum stehende Ansichten zu erstellen.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_RESOURCE_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
DROP ANY VIEW	Ermöglicht es einem Benutzer, Ansichten zu löschen, die einem beliebigen Benutzer gehören.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> </ul>
<b>Webdienste</b>		
MANAGE ANY WEB SERVICE	Ermöglicht es einem Benutzer, Webdienste zu erstellen, zu ändern, zu löschen und zu kommentieren.	<ul style="list-style-type: none"> <li>• SYS_AUTH_DBA_ROLE</li> <li>• SYS_AUTH_SA_ROLE</li> <li>• SYS_RUN_REPLICATION_ROLE</li> <li>• SYS_REPLICATION_ADMIN_ROLE</li> </ul>

## Benutzerprivilegien beurteilen

Rollen führen zu höherer Komplexität bei den Privilegien einzelner Benutzer. Nehmen Sie an, Benutzer M\_Haneeef hat die Privilegien SELECT und UPDATE für eine bestimmte Tabelle, ist aber auch Mitglied von zwei Rollen. Nehmen Sie außerdem an, eine dieser Rollen hat überhaupt keinen Zugriff auf die Tabelle und die andere hat nur das SELECT-Privileg. Welche Privilegien gelten nun für den Benutzer?

Wenn der Benutzer-ID explizit die zum Ausführen der betreffenden Aktion erforderlichen Privilegien erteilt wurden, wird die Aktion ausgeführt.

Andernfalls hängt die Berechtigung zum Ausführen der Aktion von den Privilegien der einzelnen Rollen ab, deren Mitglied der Benutzer ist. Wenn eine dieser Rollen das erforderliche Privileg hat, um die Aktion auszuführen, hat die Benutzer-ID als Mitglied dieser Rolle ebenfalls das Privileg und die Aktion wird ausgeführt.

## Systemprivilegien erteilen (Sybase Central)

Durch Erteilen eines Systemprivilegs können Sie einen Benutzer oder eine Rolle autorisieren, einen Vorgang in der Datenbank auszuführen.

### Voraussetzungen

Sie benötigen die Administrationsrechte für das zu erteilende Systemprivileg.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie auf **Systemprivilegien** und wählen Sie ein Systemprivileg aus.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Berechtigungsempfänger**.
4. Rechtsklicken Sie in den rechten Fensterausschnitt und wählen Sie dann **Neu » Berechtigungsempfänger**.
5. Wählen Sie den Benutzer bzw. die Rolle, dem bzw. der Sie das Systemprivileg erteilen möchten.
6. Klicken Sie auf **OK**.

Eine neue Zeile wird zur Tabelle **Systemprivilegien** hinzugefügt.

7. (Optional) Verwenden Sie die Spalte **Adm.** (Administrationsrechte), um die Administrationsrechte für das Systemprivileg zu ändern. Ein Häkchen in der Spalte bedeutet, dass der Benutzer bzw. die Rolle das Systemprivileg verwalten (erteilen oder entziehen) kann. Eine leere Spalte bedeutet, dass der Benutzer bzw. die Rolle keine Administrationsrechte für das Systemprivileg hat. Klicken Sie in die Spalte, um die Option umzuschalten.

(Optional) Verwenden Sie die Spalte **Ausü.** (Ausübungsrechte), um die Ausübungsrechte für den Benutzer bzw. die Rolle zu ändern. Ein Häkchen in der Spalte bedeutet, dass der Benutzer bzw. die

Rolle das Systemprivileg ausüben kann. Das Ausübungsprivileg wird standardmäßig erteilt. Klicken Sie in die Spalte, um die Option umzuschalten.

8. (Optional) Wenn Sie das Systemprivileg **CHANGE PASSWORD** oder **SET USER** erteilt haben, enthält die Spalte **Optionen** den Eintrag **Alle Benutzer**. Die Spalte **Optionen** gilt nur für diese beiden Systemprivilegien.
  - Wenn Sie das **CHANGE PASSWORD**-Systemprivileg erteilt haben, kann der Benutzer bzw. die Rolle standardmäßig das Kennwort für jeden beliebigen Benutzer ändern. Um die Benutzer einzuschränken, deren Kennwörter geändert werden können, rechtsklicken Sie auf die Zeile und klicken Sie auf **Optionen festlegen**.
  - Wenn Sie das **SET USER**-Systemprivileg erteilt haben, kann der Benutzer bzw. die Rolle standardmäßig jeden beliebigen Benutzer impersonieren. Um die Benutzer einzuschränken, die impersoniert werden können, rechtsklicken Sie auf die Zeile und klicken Sie auf **Optionen festlegen**. Die Spalte **Optionen** gilt nur für die Systemprivilegien **CHANGE PASSWORD** und **SET USER**.
9. Klicken Sie auf **Datei » Speichern**.

### Ergebnisse

Dem Benutzer bzw. der Rolle werden die Systemprivilegien erteilt. Wenn Sie ein Systemprivileg einer Rolle erteilt haben, erbt jeder Benutzer oder jede Rolle, der diese Rolle erteilt wird, das neue Systemprivileg.

### Siehe auch

- „Privilegien“ auf Seite 1305
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Privilegien auf Objektebene erteilen (Sybase Central)“ auf Seite 1333
- „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343

## Systemprivilegien erteilen (SQL)

Durch Erteilen eines Systemprivilegs können Sie einen Benutzer oder eine Rolle autorisieren, einen Vorgang in der Datenbank auszuführen.

### Voraussetzungen

Sie benötigen Administrationsrechte für das zu erteilende Systemprivileg.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine Anweisung ähnlich der folgenden aus:

Option	Anweisung
Privilegien ohne Administrationsrechte erteilen	<code>GRANT privilege-name TO userid;</code>
Privilegien mit Administrationsrechten erteilen	<code>GRANT privilege-name TO userid WITH ADMIN OPTION;</code>
Nur Administrationsrechte für ein Privileg erteilen	<code>GRANT privilege-name TO userid WITH ADMIN ONLY OPTION;</code>

## Ergebnisse

Dem Benutzer bzw. der Rolle wird das Systemprivileg erteilt. Wenn Sie ein Systemprivileg einer Rolle erteilt haben, erbt jeder Benutzer oder jede Rolle, der diese Rolle erteilt wird, das neue Systemprivileg.

## Beispiel

Wenn Sie der Rolle RolleA das CREATE ANY OBJECT-Systemprivileg erteilen möchten, ohne ihr Administrationsrechte zu geben, führen Sie die folgende Anweisung aus:

```
GRANT CREATE ANY OBJECT TO RoleA
```

Wenn Sie der Rolle RolleA das CREATE ANY OBJECT-Systemprivileg erteilen möchten, zusammen mit der Möglichkeit, Benutzern und anderen Rollen das Systemprivileg zu erteilen oder zu entziehen, führen Sie die folgende Anweisung aus:

```
GRANT CREATE ANY OBJECT TO RoleA WITH ADMIN OPTION
```

Wenn Sie der Rolle RolleA Administrationsrechte für das BACKUP DATABASE-Systemprivileg erteilen möchten, aber nicht die Möglichkeit, das BACKUP DATABASE-Privileg zu nutzen, führen Sie die folgende Anweisung aus:

```
GRANT BACKUP DATABASE TO RoleA WITH ADMIN ONLY OPTION
```

Wenn Sie der Rolle RolleA (nur) Administrationsrechte für die Privilegien BACKUP DATABASE und CHECKPOINT erteilen möchten, führen Sie die folgende Anweisung aus:

```
GRANT BACKUP DATABASE, CHECKPOINT TO RoleA WITH ADMIN ONLY OPTION;
```

## Siehe auch

- „Privilegien“ auf Seite 1305
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Privilegien auf Objektebene erteilen (Sybase Central)“ auf Seite 1333
- „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Privilegien auf Objektebene erteilen (Sybase Central)

Erteilen Sie Privilegien auf Objektebene, um den Zugriff auf ein bestimmtes Objekt zu ermöglichen, z.B. auf eine Tabelle, eine Ansicht, eine Prozedur, eine Sequenz oder einen DBSpace. Sie können Privilegien pro Benutzer, pro Rolle oder pro Datenbankobjekt anzeigen und ändern.

## Voraussetzungen

Damit Sie ein Privileg auf Objektebene erteilen können, muss eine der folgenden Bedingungen erfüllt sein:

- Sie sind der Eigentümer des Datenbankobjekts, für das Sie Berechtigungen erteilen möchten.
- Ihnen wurde das Privileg erteilt und Sie haben dafür Administrationsrechte.
- Sie haben das **MANAGE ANY OBJECT PRIVILEGE**-Systemprivileg.

## Kontext und Bemerkungen

Wenn Sie Rollen Privilegien erteilen, werden diese von den Mitgliedern der Rolle geerbt.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie im linken Fensterausschnitt auf **Benutzer** und wählen Sie einen Benutzer aus.
3. Klicken Sie im rechten Fensterausschnitt auf die entsprechende Privilegien-Registerkarte. Wenn Sie beispielsweise Privilegien für eine Tabelle erteilen möchten, klicken Sie auf die Registerkarte **Tabellenprivilegien**.

Die Registerkarte enthält eine Liste der Privilegien, die dem Benutzer explizit erteilt wurden.

4. Rechtsklicken Sie in den Fensterausschnitt und wählen Sie **Neu » Privilegien**.
5. Wählen Sie die Datenbankobjekte aus, für die Sie Privilegien erteilen möchten, und klicken Sie dann auf **OK**.

Das Datenbankobjekt wird als Zeile auf der Registerkarte hinzugefügt. Standardmäßig werden alle Privilegien für das Datenbankobjekt erteilt.

6. (Optional) Wenn Sie die Privilegien ändern möchten, die dem Benutzer für ein Datenbankobjekt erteilt wurden, klicken Sie auf der entsprechenden Privilegien-Registerkarte auf die relevante Zelle in der Tabelle. (Zellendefinitionen finden Sie in der Legende.)

Ein Häkchen bedeutet, dass das Privileg dem Benutzer erteilt wird. Ein Häkchen mit Pluszeichen (+) bedeutet, dass das Privileg dem Benutzer erteilt wird und der Benutzer dasselbe Privileg anderen Benutzern erteilen darf. Ein Häkchen mit Pluszeichen (+) entspricht dem Ausführen der GRANT-Anweisung mit der **WITH GRANT OPTION**-Klausel.

Wenn Sie auf der Registerkarte **Tabellenprivilegien** eine Tabelle auswählen, wird unten die entsprechende Tabelle **Spaltenprivilegien** angezeigt. Das Ändern eines Spaltenprivilegs bewirkt, dass in der Tabelle **Tabellenprivilegien** das Symbol **Spaltenprivilegien werden erteilt/mit Weitergaberecht erteilt** angezeigt wird. Änderungen an Tabellenprivilegien haben Auswirkungen darauf, ob bestimmte Spaltenprivilegien erteilt werden können.

**Tipp**

- Wenn Sie Ihre Änderungen rückgängig machen möchten, wählen Sie auf der Registerkarte **Privilegien** eine oder mehrere Zeilen aus und klicken Sie auf **Bearbeiten** » **Rückgängig**.
- Wenn Sie die **Legende** aktivieren bzw. deaktivieren möchten, klicken Sie auf **Datei** » **Beschriftung anzeigen**.

7. Klicken Sie auf **Datei** » **Speichern**.

**Ergebnisse**

Dem Benutzer werden die angegebenen Privilegien auf Objektebene erteilt.

**Siehe auch**

- „Objektprivilegien“ auf Seite 1305
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Privilegien auf Objektebene entziehen (Sybase Central)“ auf Seite 1339
- „Privilegien auf Objektebene erteilen (SQL)“ auf Seite 1335
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343

**Privilegien auf Objektebene erteilen (SQL)**

Erteilen Sie Privilegien auf Objektebene, um den Zugriff auf ein bestimmtes Objekt zu ermöglichen, z.B. auf eine Tabelle, eine Ansicht, eine Prozedur, eine Sequenz oder einen DBSpace. Sie können Privilegien pro Benutzer, pro Rolle oder pro Datenbankobjekt anzeigen und ändern.

**Voraussetzungen**

Damit Sie ein Privileg auf Objektebene erteilen können, muss eine der folgenden Bedingungen erfüllt sein:

- Sie sind der Eigentümer des Datenbankobjekts, für das Sie Berechtigungen erteilen möchten.
- Ihnen wurde das Privileg erteilt und Sie haben dafür Administrationsrechte.
- Sie haben das **MANAGE ANY OBJECT PRIVILEGE**-Systemprivileg.

**Kontext und Bemerkungen**

Wenn Sie Rollen Privilegien erteilen, werden diese von den Mitgliedern der Rolle geerbt.

**Aufgabe**

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine GRANT-Anweisung aus.

## Ergebnisse

Dem Benutzer wird das angegebene Privileg auf Objektebene erteilt.

## Beispiel

Die folgende Anweisung erteilt der Benutzerin AnnW das SELECT-Privileg für die Tabelle myTable:

```
GRANT SELECT ON myTable TO AnnW;
```

Die folgende Anweisung erteilt der Benutzerin AnnW das SELECT-Privileg für die Tabelle myTable und gibt ihr Administrationsrechte für das Privileg:

```
GRANT SELECT ON myTable TO AnnW WITH GRANT OPTION;
```

## Siehe auch

- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Objektprivilegien“ auf Seite 1305
- „Privilegien auf Objektebene erteilen (Sybase Central)“ auf Seite 1333
- „Privilegien auf Objektebene erteilen (SQL)“ auf Seite 1340
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Systemprivilegien entziehen (Sybase Central)

Entziehen Sie ein Systemprivileg einem Benutzer, einer benutzererweiterten Rolle oder einer benutzerdefinierten Rolle.

### Voraussetzungen

Sie benötigen Administrationsrechte für das Systemprivileg.

Der SYS-Rolle können Sie keine Privilegien entziehen. Anderen Systemrollen können Sie Privilegien entziehen, vorausgesetzt, diese Privilegien gehören nicht zu den Standardprivilegien für die betreffende Systemrolle.

### Kontext und Bemerkungen

Wenn einem Benutzer Ausübungs- und Administrationsrechte für ein Privileg erteilt wurden, können Sie entweder die Administrationsrechte entziehen oder die Ausübungs- und Administrationsrechte. Sie können nicht (nur) das Ausübungsrecht entziehen und das Administrationsrecht belassen. Um dies zu erreichen, müssen Sie das Systemprivileg vollständig entziehen und anschließend nur mit Administrationsrechten neu erteilen.

Einer Kompatibilitätsrolle können Sie keine Systemprivilegien entziehen. Sie können jedoch eine Kompatibilitätsrolle in eine benutzerdefinierte Rolle migrieren und dann der benutzerdefinierten Rolle Privilegien entziehen.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **Systemprivilegien** und anschließend auf ein Systemprivileg.
3. Klicken Sie auf die Registerkarte **Berechtigungsempfänger**.
4. Wählen Sie eine der folgenden Optionen:

Option	Aktion
Privileg einschließlich der dazugehörigen Administrationsrechte entziehen	Rechtsklicken Sie auf den Benutzer bzw. die Rolle und klicken Sie auf <b>Löschen</b> .
Nur Administrationsrechte entziehen	Klicken Sie in die Spalte <b>Adm.</b> (Administrationsrechte), um das Häkchen zu entfernen.
Nur das Privileg entziehen	Klicken Sie in die Spalte <b>Ausü.</b> (Ausübungsrechte), um das Häkchen zu entfernen.

### Tipp

- Wenn Sie Ihre Änderungen rückgängig machen möchten, wählen Sie eine oder mehrere Zeilen aus und klicken Sie auf **Bearbeiten » Rückgängig**.
- Wenn Sie die **Legende** aktivieren bzw. deaktivieren möchten, klicken Sie auf **Datei » Beschriftung anzeigen**.

5. Klicken Sie auf **Datei » Speichern**.

## Ergebnisse

Das Systemprivileg bzw. das Administrationsrecht wird dem Benutzer bzw. der Rolle entzogen.

## Siehe auch

- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343

## Systemprivilegien entziehen (SQL)

Entziehen Sie ein Systemprivileg einem Benutzer, einer benutzererweiterten Rolle oder einer benutzerdefinierten Rolle.

### Voraussetzungen

Sie benötigen Administrationsrechte für das Systemprivileg.

Der SYS-Rolle können Sie keine Privilegien entziehen. Anderen Systemrollen können Sie Privilegien entziehen, vorausgesetzt, diese Privilegien gehören nicht zu den Standardprivilegien für die betreffende Systemrolle.

### Kontext und Bemerkungen

Wenn einem Benutzer Ausübungs- und Administrationsrechte für ein Privileg erteilt wurden, können Sie entweder die Administrationsrechte entziehen oder die Ausübungs- und Administrationsrechte. Sie können nicht (nur) das Ausübungsrecht entziehen und das Administrationsrecht belassen. Um dies zu erreichen, müssen Sie das Systemprivileg vollständig entziehen und anschließend nur mit Administrationsrechten neu erteilen.

Einer Kompatibilitätsrolle können Sie keine Systemprivilegien entziehen. Sie können jedoch eine Kompatibilitätsrolle in eine benutzerdefinierte Rolle migrieren und dann der benutzerdefinierten Rolle Privilegien entziehen.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine REVOKE-Anweisung ähnlich der folgenden aus:

```
REVOKE privilege FROM grantee;
```

### Ergebnisse

Das Systemprivileg bzw. das Administrationsrecht wird dem Benutzer bzw. der Rolle entzogen.

### Siehe auch

- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen in benutzerdefinierte Rollen migrieren (Sybase Central)“ auf Seite 1277
- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

### Beispiel

Angenommen, Sie haben einen Benutzer DaveW, dem das CREATE ANY TABLE-Systemprivileg mit Administrationsrechten erteilt wurde. In diesem Beispiel wird dem Benutzer DaveW das CREATE ANY TABLE-Systemprivileg entzogen:

```
REVOKE CREATE ANY TABLE FROM DaveW;
```

In diesem Beispiel werden dem Benutzer DaveW (nur) die Administrationsrechte für das CREATE ANY TABLE-Systemprivileg entzogen:

```
REVOKE ADMIN OPTION FOR CREATE ANY TABLE FROM DaveW;
```

## Privilegien auf Objektebene entziehen (Sybase Central)

Entziehen Sie ein Privileg auf Objektebene, das einem Benutzer oder einer Rolle erteilt wurde, um den Zugriff auf ein bestimmtes Objekt einzuschränken, z.B. auf eine Tabelle, eine Ansicht, eine Prozedur, eine Sequenz oder einen DBSpace.

### Voraussetzungen

Damit Sie ein Privileg auf Objektebene entziehen können, muss eine der folgenden Bedingungen erfüllt sein:

- Sie sind der Eigentümer des Datenbankobjekts, für das Sie Berechtigungen entziehen möchten.
- Ihnen wurde das Privileg erteilt und Sie haben dafür Administrationsrechte.
- Sie haben das MANAGE ANY OBJECT PRIVILEGE-Systemprivileg.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt entweder auf das Datenbankobjekt, für das Sie ein Benutzerprivileg entziehen möchten, oder klicken Sie auf **Benutzer** oder **Rollen** und anschließend auf den Benutzer bzw. die Rolle, dem bzw. der Sie Privilegien entziehen möchten.

Option	Aktion
Privilegien auf Objektebene pro Benutzer oder Rolle entziehen	<ol style="list-style-type: none"> <li>a. Klicken Sie im rechten Fensterausschnitt auf die Privilegien-Registerkarte für das Datenbankobjekt, für das Sie Privilegien entziehen möchten. Wenn Sie beispielsweise Privilegien für eine Tabelle entziehen möchten, klicken Sie auf die Registerkarte <b>Tabellenprivilegien</b>.</li> <li>b. Rechtsklicken Sie auf das Privileg und klicken Sie auf <b>Entziehen</b> und anschließend entweder auf <b>Alle Privilegien</b> oder auf das Privileg, das Sie entziehen möchten.</li> </ol>
Privilegien auf Objektebene pro Datenbankobjekt entziehen	<ol style="list-style-type: none"> <li>a. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte <b>Privilegien</b>.</li> <li>b. Rechtsklicken Sie auf den Benutzer bzw. die Rolle und klicken Sie auf <b>Entziehen</b> und anschließend entweder auf <b>Alle Privilegien</b> oder auf das Privileg, das Sie entziehen möchten.</li> </ol>

3. Klicken Sie auf **Datei » Speichern**.

## Ergebnisse

Das Privileg wird dem angegebenen Benutzer bzw. der angegebenen Rolle entzogen.

### Siehe auch

- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Objektprivilegien“ auf Seite 1305
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343

## Privilegien auf Objektebene erteilen (SQL)

Entziehen Sie ein Privileg auf Objektebene, das einem Benutzer oder einer Rolle erteilt wurde, um den Zugriff auf ein bestimmtes Objekt einzuschränken, z.B. auf eine Tabelle, eine Ansicht, eine Prozedur, eine Sequenz oder einen DBSpace.

### Voraussetzungen

Damit Sie ein Privileg auf Objektebene entziehen können, muss eine der folgenden Bedingungen erfüllt sein:

- Sie sind der Eigentümer des Datenbankobjekts, für das Sie Berechtigungen entziehen möchten.
- Ihnen wurde das Privileg erteilt und Sie haben dafür Administrationsrechte.
- Sie haben das MANAGE ANY OBJECT PRIVILEGE-Systemprivileg.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine REVOKE-Anweisung ähnlich der folgenden aus:

```
REVOKE privilege-name ON object-name FROM userid;
```

## Ergebnisse

Das Privileg wird dem angegebenen Benutzer bzw. der angegebenen Rolle entzogen.

### Siehe auch

- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Objektprivilegien“ auf Seite 1305
- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344

## Benutzer

Allen neuen Benutzern wird automatisch die PUBLIC-Systemrolle erteilt. Sie können steuern, welche Privilegien neuen Benutzern automatisch erteilt werden, indem Sie die Privilegien der PUBLIC-Rolle bearbeiten.

Standardmäßig umfassen die neuen Benutzern zugeordneten Privilegien Folgendes:

- Die Möglichkeit, eine Verbindung zur Datenbank herzustellen (vorausgesetzt, es wurde ein Kennwort für den Benutzer angegeben).
- Die Möglichkeit, die in den Systemansichten gespeicherten Daten anzuzeigen.
- Die Möglichkeit, die meisten gespeicherten Systemprozeduren auszuführen.

Wenn Sie einen neuen Benutzer erstellt haben, können Sie Folgendes durchführen:

- Dem Benutzer Systemrollen und Systemprivilegien erteilen.
- Die Privilegien des Benutzers auf Objektebene festlegen.
- Dem Benutzer eine Login-Richtlinie zuordnen. Standardmäßig wird dem Benutzer die Root-Login-Richtlinie zugeordnet.
- Den Benutzer als Publikationseigentümer oder als entfernten Benutzer der Datenbank für die Verwendung in einem SQL Remote-System festlegen.

#### **Siehe auch**

- „Superuser“ auf Seite 1295

## **Benutzer erstellen (Sybase Central)**

Erstellen Sie einen Benutzer mithilfe des **Assistenten zum Erstellen von Benutzern** in Sybase Central.

### **Voraussetzungen**

Sie müssen das **MANAGE ANY USER**-Systemprivileg haben.

### **Kontext und Bemerkungen**

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie im linken Fensterausschnitt auf **Benutzer** und klicken Sie auf **Neu » Benutzer**.
3. Befolgen Sie die Anweisungen des Assistenten.

## Ergebnisse

Ein Benutzer wird erstellt.

## Nächste Schritte

Erteilen Sie dem Benutzer Rollen und Privilegien.

## Siehe auch

- [Einschränkungen und Hinweise zu Benutzer-IDs und Kennwörtern auf Seite 1367](#)
- [„Login-Richtlinien“ auf Seite 535](#)
- [„CREATE USER-Anweisung“ \[\*SQL Anywhere Server - SQL-Referenzhandbuch\*\]](#)
- [„Benutzer in benutzererweiterte Rollen konvertieren \(Sybase Central\)“ auf Seite 1289](#)
- [„Rollen erteilen \(Sybase Central\)“ auf Seite 1298](#)
- [„Verbundene Benutzer verwalten“ auf Seite 99](#)

## Benutzer erstellen (SQL)

Erstellen Sie einen Benutzer mit der CREATE USER-Anweisung.

## Voraussetzungen

Sie müssen das MANAGE ANY USER-Systemprivileg haben.

## Kontext und Bemerkungen

- Benutzer-IDs dürfen Folgendes nicht:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
- Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gilt Folgendes:
  - Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
  - Sie dürfen nicht mit Leerstellen enden.
  - Sie dürfen keine Semikola enthalten.
  - länger als 255 Byte sein

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie eine CREATE USER-Anweisung aus, die eine IDENTIFIED BY-Klausel enthält.

Standardmäßig wird Benutzern die Root-Login-Richtlinie zugeordnet. Wenn Sie einem Benutzer eine andere Login-Richtlinie zuordnen möchten, können Sie diese mit der LOGIN POLICY-Klausel der CREATE USER-Anweisung angeben.

## Ergebnisse

Ein Benutzer wird erstellt und die angegebene Login-Richtlinie wird dem Benutzer zugeordnet. Wenn keine Login-Richtlinie angegeben wurde, wird die Root-Login-Richtlinie angewendet.

## Nächste Schritte

Erteilen Sie dem Benutzer Rollen und Privilegien.

## Beispiel

In diesem Beispiel wird der Datenbank ein neuer Benutzer mit der Benutzer-ID "M\_Haneef" und dem Kennwort "Welcome" hinzugefügt.

```
CREATE USER M_Haneef  
IDENTIFIED BY Welcome;
```

## Siehe auch

- „CREATE USER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)“ auf Seite 1289
- „Login-Richtlinien“ auf Seite 535

## Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)

Zeigen Sie die Rollen und Privilegien an, die Benutzern und Rollen erteilt wurden.

## Voraussetzungen

Sie müssen die PUBLIC-Rolle haben.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.

2.	<b>Option</b>	<b>Aktion</b>
	Rollen und Privilegien für einen Benutzer anzeigen	a. Klicken Sie im linken Fensterausschnitt auf <b>Benutzer</b> . b. Klicken Sie auf den Benutzer, den Sie anzeigen möchten. c. Klicken Sie im rechten Fensterausschnitt auf <b>Rollen</b> oder <b>Systemprivilegien</b> , um die Rollen bzw. Privilegien des Benutzers anzuzeigen. d. Optional können Sie mit <b>Ererbte anzeigen</b> geerbte Rollen und Privilegien einbeziehen.
	Rollen und Privilegien für eine Rolle anzeigen	a. Klicken Sie im linken Fensterausschnitt auf <b>Rollen</b> . b. Klicken Sie auf die Rolle, die Sie anzeigen möchten. c. Klicken Sie im rechten Fensterausschnitt auf <b>Rollen</b> oder <b>Systemprivilegien</b> , um die Rollen bzw. Privilegien anzuzeigen. d. Optional können Sie mit <b>Ererbte anzeigen</b> geerbte Rollen und Privilegien einbeziehen.

### Ergebnisse

Im rechten Fensterausschnitt werden die Rollen und Privilegien angezeigt, die dem angegebenen Benutzer bzw. der angegebenen Rolle erteilt oder vererbt wurden.

### Siehe auch

- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344
- „sp\_displayroles-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_objectpermission-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)

Zeigen Sie die Rollen und Privilegien an, die ein Benutzer hat, einschließlich der geerbten Rollen und Privilegien. Sie können diese Aufgabe auch verwenden, um die Rollen und Privilegien für eine bestimmte Rolle anzuzeigen.

### Voraussetzungen

- **sp\_displayroles-Systemprozedur:** Wenn Sie diese Prozedur für sich selbst ausführen möchten, benötigen Sie keine Privilegien. Um jedoch die Systemprivilegien oder Rollen für eine andere Benutzer-ID oder eine Rolle zurückgeben zu können, müssen Sie das **MANAGE ROLES**-Systemprivileg haben.
- **sp\_objectpermission-Systemprozedur:** Wenn Sie diese Prozedur für sich selbst oder für in Ihrem Eigentum stehende Objekte ausführen möchten, benötigen Sie keine Privilegien. Um diese Prozedur jedoch für eine andere Benutzer-ID oder für ein im Eigentum einer anderen Benutzer-ID stehendes Objekt aufrufen zu können, müssen Sie das **MANAGE ANY OBJECT PRIVILEGE**-Systemprivileg haben.

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Um die Rollen und Systemprivilegien des Benutzers anzuzeigen, führen Sie eine Anweisung aus, die die `sp_displayroles`-Systemprozedur aufruft (ähnlich der folgenden, wobei `userid` die Benutzer-ID des Benutzers ist):

```
SELECT * FROM sp_displayroles( 'userid', 'expand_down');
```

3. Um die Privilegien eines Benutzers auf Objektebene anzuzeigen, führen Sie eine Anweisung aus, die die `sp_objectpermission`-Systemprozedur aufruft (ähnlich der folgenden):

```
SELECT * FROM sp_objectpermission('userid');
```

## Ergebnisse

Die `role_name`-Spalte in den Ergebnissen für `sp_displayroles` enthält geerbte Rollen und Systemprivilegien sowie diejenigen, die dem Benutzer explizit erteilt wurden. Wenn die Rolle bzw. das Systemprivileg von einer anderen Rolle geerbt wurde, wird der Name dieser Rolle in der `parent_role_name`-Spalte angezeigt. Der `grant_type`-Spalte können Sie entnehmen, ob der Benutzer Administrationsrechte für die Rolle bzw. das Systemprivileg hat. Die `role_level`-Spalte zeigt eine Hierarchie für die Vererbung, da Vererbung durch Mitgliedschaft in einer Rolle eintreten kann, die wiederum Mitglied einer anderen Rolle ist, usw. Dies kann Ihnen bei der Fehlerbehandlung helfen, wenn Sie einem Benutzer eine Rolle oder ein Privileg entziehen, aber feststellen, dass dieser die Rolle bzw. das Privileg weiterhin nutzen kann.

Die Ergebnisse für `sp_objectpermission` enthalten geerbte Privilegien auf Objektebene sowie diejenigen, die dem Benutzer explizit erteilt wurden. In der `grantee`-Spalte können Sie sehen, woher das Privileg auf Objektebene geerbt wurde. Die `grantor`-Spalte zeigt, wer die eigentliche Erteilung ausgeführt hat. Der `grantable`-Spalte können Sie entnehmen, ob der Benutzer Administrationsrechte für das Privileg hat.

## Siehe auch

- „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343
- „`sp_displayroles`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_objectpermission`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Benutzer löschen (Sybase Central)

Löschen Sie einen Benutzer, um gleichzeitig alle Datenbankobjekte (z.B. Tabellen) zu löschen, deren Eigentümer er ist, sowie etwaige externe Logins für den Benutzer.

### Voraussetzungen

Sie müssen das `MANAGE ANY USER`-Systemprivileg haben.

Der zu entfernende Benutzer darf nicht mit der Datenbank verbunden sein, während Sie diese Prozedur ausführen.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Klicken Sie im linken Fensterausschnitt auf **Benutzer**.
3. Rechtsklicken Sie im rechten Fensterausschnitt auf einen Benutzer und klicken Sie dann auf **Löschen**.
4. Klicken Sie auf **Ja**, um die Aktion zu bestätigen.

## Ergebnisse

Der Benutzer wird gelöscht, ebenso alle Datenbankobjekte (z.B. Tabellen oder Prozeduren), deren Eigentümer er war, und etwaige externe Logins für den Benutzer. Wenn der Benutzer als benutzererweiterte Rolle fungiert hat, wird diese benutzererweiterte Rolle allen Benutzern und Rollen entzogen, denen sie erteilt war. Wenn der Benutzer in der USER-Klausel für Dienste angegeben war, werden die betreffenden Dienste ebenfalls gelöscht.

## Siehe auch

- „DROP USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Benutzererweiterte Rollen“ auf Seite 1287

## Gruppen

Eine Gruppe besteht aus Benutzern mit gemeinsamen Rollen und Privilegien.

Gruppen stellen eine effiziente Methode dar, um Rollen und Privilegien für mehrere Benutzer zu verwalten.

Mitgliedschaft in einer Gruppe, die Eigentümerin von Objekten ist, bedeutet auch, dass Benutzer nicht die Objektnamen qualifizieren müssen, wenn sie Vorgänge ausführen wie das Ausführen einer Prozedur, die der Gruppe gehört, oder das Abfragen einer Tabelle, die der Gruppe gehört. Wenn beispielsweise eine Tabelle namens MyData Eigentum einer Gruppe namens PersonnelData ist, in der wiederum die Benutzer-ID "M\_Haneef" Mitglied ist, kann M\_Haneef die Tabelle in Abfragen als MyData referenzieren statt als PersonnelData.MyData. Wenn ein Benutzer Eigentümer einer Tabelle ist, die denselben Namen hat wie eine Tabelle im Eigentum einer Gruppe, verwendet der Datenbankserver die Tabelle, die dem Benutzer gehört, nicht diejenige, die der Gruppe gehört. Wenn ein Benutzer mehreren Gruppen angehört, die eine Tabelle mit demselben Namen haben, muss auch der Benutzer den Tabellennamen qualifizieren.

In SQL Anywhere ist eine Gruppe kein Datenbankobjekt. Stattdessen werden Gruppen mithilfe von benutzerdefinierten Rollen erzeugt, wobei zwei verschiedene Ansätze möglich sind:

- **Auf benutzererweiterten Rollen basierender Ansatz zum Erstellen von Gruppen** Benutzererweiterte Rollen sind benutzerdefinierte Rollen, die durch Erweitern einer vorhandenen Benutzer-ID zu einer Rolle erstellt werden. Bei diesem Ansatz zur Gruppenerstellung wird die Benutzer-ID erstellt und anschließend werden ihr alle für die Gruppe erforderlichen Rollen und Privilegien erteilt. Die Benutzer-ID wird in eine benutzererweiterte Rolle konvertiert und dann

den Benutzern erteilt, die sie benötigen. Diese Schritte können auch in anderer Reihenfolge ausgeführt werden.

Dieser Ansatz wird beim Erstellen von Gruppen für die Replikation häufig angewendet, weil der Benutzer, der zu einer Rolle erweitert wurde, auch über Login-Funktionen verfügt.

Für Benutzer früherer Versionen von SQL Anywhere ist dieser Ansatz identisch mit dem nicht mehr empfohlenen Ansatz, bei dem mit der GRANT-Anweisung einem Benutzer GROUP erteilt wurde und anschließend anderen Benutzern MEMBERSHIP IN GROUP erteilt werden konnte.

Wenn Sie eine nach diesem Ansatz erstellte Gruppe löschen möchten, konvertieren Sie die benutzererweiterte Rolle in einen normalen Benutzer zurück (`DROP ROLE FROM USER userid`). Das Eigentum an Objekten bleibt bei dem Benutzer, der in einen normalen Benutzer zurückkonvertiert wird.

Wenn der auf benutzererweiterten Rollen basierende Ansatz verwendet wird, können Gruppen und die dazugehörigen Mitgliederinformationen aus der konsolidierten Ansicht `SYSDROLEGRANTS` oder aus der `SYSGROUPS`-Kompatibilitätsansicht abgefragt werden.

- **Auf eigenständigen Rollen basierender Ansatz zum Erstellen von Gruppen** Eigenständige Rollen sind benutzerdefinierte Rollen, die keiner Benutzer-ID zugeordnet sind. Bei diesem Ansatz zur Gruppenerstellung wird die Rolle erstellt und anschließend werden ihr alle von einer definierten Benutzergruppe benötigten Rollen und Privilegien erteilt. Die Rolle wird dann den Benutzern erteilt, die sie benötigen.

Wenn Sie eine nach diesem Ansatz erstellte Gruppe löschen möchten, löschen Sie die Rolle. Optional können Sie beim Löschen der Rolle gleichzeitig auch die Objekte löschen, deren Eigentümerin die Rolle ist.

Wenn der auf eigenständigen Rollen basierende Ansatz verwendet wird, können Gruppen und die dazugehörigen Mitgliederinformationen nicht aus der `SYSGROUPS`-Kompatibilitätsansicht abgefragt werden. Stattdessen können die Informationen aus der konsolidierten Ansicht `SYSDROLEGRANTS` abgefragt werden.

Bei beiden Ansätzen erfolgt die Verwaltung der Privilegien für Gruppenmitglieder auf der Ebene der jeweiligen benutzerdefinierten Rolle statt auf der Ebene der einzelnen Benutzer-IDs.

## Beispiele für beide Ansätze

Die folgenden SQL-Anweisungen zeigen ein stark vereinfachtes Beispiel zum Erstellen einer Gruppe mit drei Mitgliedern, die das `SELECT ANY TABLE`-Systemprivileg und die `SA_DEBUG`-Systemrolle benötigen. Die erste Gruppe von Anweisungen zeigt den auf benutzererweiterten Rollen basierenden Ansatz, die zweite Gruppe von Anweisungen den auf eigenständigen Rollen basierenden Ansatz.

Beide Gruppen können als aus drei Mitgliedern bestehend gelten, obwohl im Fall des auf benutzererweiterten Rollen basierenden Ansatzes ein Mitglied (`member1`) sowohl als Rolle als auch als Mitglied fungiert.

```
CREATE USER member1 IDENTIFIED BY sql;
CREATE USER member2 IDENTIFIED BY sql;
CREATE USER member3 IDENTIFIED BY sql;
```

```
CREATE ROLE FOR USER member1;
GRANT ROLE member1 TO member2, member3;
GRANT SELECT ANY TABLE TO member1;
GRANT ROLE SA_DEBUG TO member1;

CREATE ROLE standaloneRole;
CREATE USER member1 IDENTIFIED BY sql;
CREATE USER member2 IDENTIFIED BY sql;
CREATE USER member3 IDENTIFIED BY sql;
GRANT ROLE standaloneRole TO member1, member2, member3;
GRANT SELECT ANY TABLE TO standaloneRole;
GRANT ROLE SA_DEBUG TO standaloneRole;
```

### Siehe auch

- „Benutzerdefinierte Rollen“ auf Seite 1285
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Konsolidierte Ansicht SYSROLEGRANTS“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SYSGROUP-Kompatibilitätsansicht“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Benutzerdefinierte Rollen erstellen (SQL)“ auf Seite 1286
- „Benutzerdefinierte Rollen erstellen (Sybase Central)“ auf Seite 1285
- „Benutzer in benutzererweiterte Rollen konvertieren (SQL)“ auf Seite 1290
- „Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central)“ auf Seite 1289
- „Rollen erteilen (Sybase Central)“ auf Seite 1298
- „Rollen erteilen (SQL)“ auf Seite 1299
- „Gruppen werden nun mithilfe von Rollen erzeugt“ auf Seite 1389

## Vererbung von Rollen und Privilegien

Die Berechtigungen, die eine Rolle oder ein Benutzer hat, können folgendermaßen kategorisiert werden:

- **Explizit einem Benutzer oder einer Gruppe (Rolle)erteilte Privilegien** Dies sind die Privilegien, die explizit für einen Benutzer oder eine Rolle festgelegt werden, um zu steuern, ob sie Datenbankobjekte erstellen, ausführen, löschen, ändern oder verwenden können. Siehe „[Privilegien auf Objektebene erteilen \(Sybase Central\)](#)“ auf Seite 1333.

Sie können nur Privilegien entziehen, die explizit erteilt wurden. Nehmen Sie beispielsweise an, der Benutzer BobW ist Mitglied einer Rolle namens Sales. Wenn ein Benutzer der Sales-Rolle das DELETE-Privileg für die Tabelle "T" erteilt, kann BobW Zeilen aus dieser Tabelle löschen. Um zu verhindern, dass BobW Zeilen aus der Tabelle "T" löscht, können Sie dazu nicht BobW das DELETE-Privileg für die Tabelle "T" entziehen, weil das DELETE ON T-Privileg nie explizit BobW erteilt wurde.

- **Durch das Eigentum an einem Objekt erworbene Privilegien** Ein Benutzer, der innerhalb der Datenbank ein neues Objekt erstellt, wird Eigentümer des betreffenden Objekts und erhält automatisch die Berechtigung, beliebige Vorgänge für dieses Objekt auszuführen. Der Eigentümer einer Tabelle kann beispielsweise die Struktur dieser Tabelle ändern oder anderen Datenbankbenutzern Berechtigungen zum Aktualisieren der Daten in der Tabelle erteilen.

Wenn ein Benutzer eine benutzererweiterte Rolle ist, erben Berechtigungsempfänger dieser Rolle nicht die mit dem Eigentum an den Objekten verbundenen Privilegien. Die Privilegien müssen ihnen explizit erteilt oder durch eine Rolle vererbt werden.

- **Durch Rollen geerbte Privilegien** Jeder Benutzer-ID können eine oder mehrere Rollen erteilt werden. Berechtigungsempfänger erben die mit dieser Rolle verbundenen Privilegien.

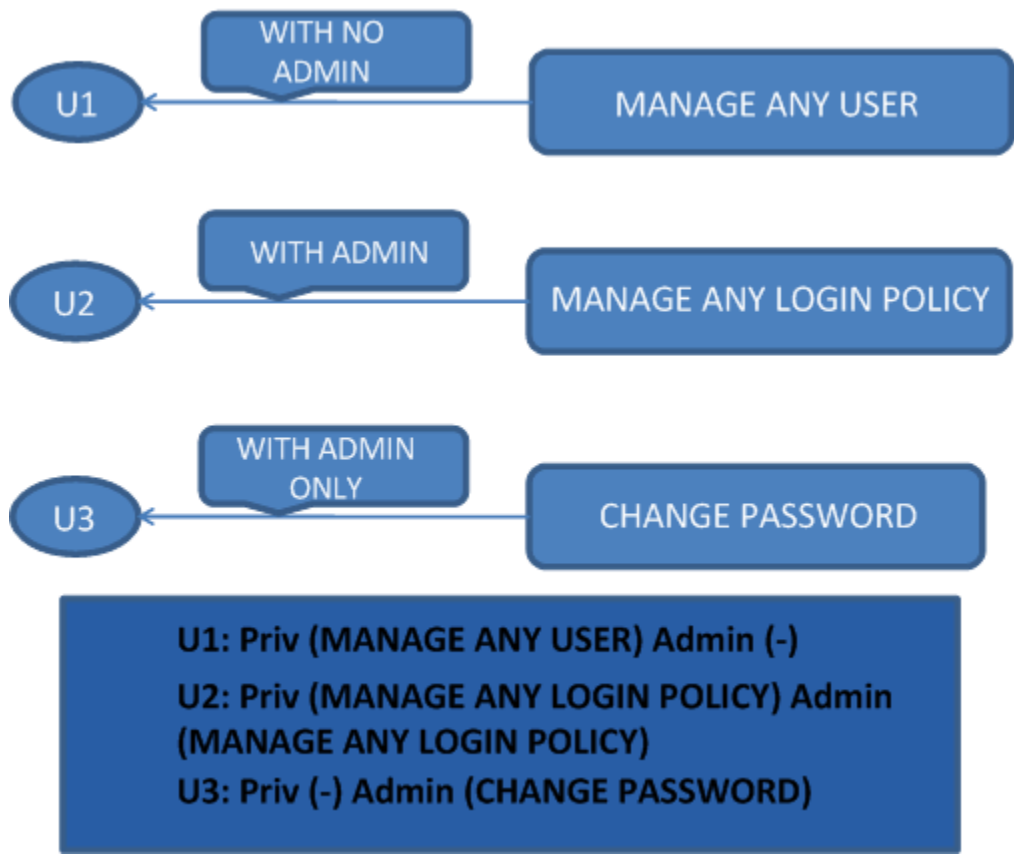
Bei Privilegien auf Objektebene ist das Eigentum an Datenbankobjekten einer einzelnen Benutzer-ID zugeordnet. Wenn der Eigentümer eine benutzererweiterte Rolle oder eine eigenständige Rolle ist, wird das Eigentum an dem Datenbankobjekt nicht von den Berechtigungsempfängern der Rolle geerbt. Wenn beispielsweise eine benutzererweiterte Rolle oder eine eigenständige Rolle Eigentümerin von Objekten ist, können Berechtigungsempfänger der benutzererweiterten bzw. eigenständigen Rolle nicht automatisch die Objekte abfragen. Dafür muss ihnen weiterhin das SELECT-Privileg erteilt werden.

- **Durch Gruppen geerbte Privilegien** Gruppen werden über benutzerdefinierte Rollen erzeugt. Daher erfolgt die Vererbung von Privilegien durch Gruppenmitgliedschaften genauso wie durch Rollen.
- **Für deaktivierte Objekte erteilte Privilegien** Sie können Privilegien für deaktivierte Objekte erteilen. Privilegien für deaktivierte Objekte werden in der Datenbank gespeichert und treten in Kraft, wenn das betreffende Objekt aktiviert wird. Die Vererbungshierarchie kann viele Ebenen haben, wenn Rollen wiederum Rollen erteilt wurden.

Hinweise zum Anzeigen der Rollen und Privilegien, die eine Rolle oder ein Benutzer hat, finden Sie unter [„Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen \(Sybase Central\)“ auf Seite 1343](#) und [„Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen \(SQL\)“ auf Seite 1344](#).

Die folgenden Szenarien zeigen, wie Privilegien geerbt werden, besonders im Hinblick auf verschiedene Erteilungsebenen von Administrationsrechten durch Vererbung.

Szenario 1



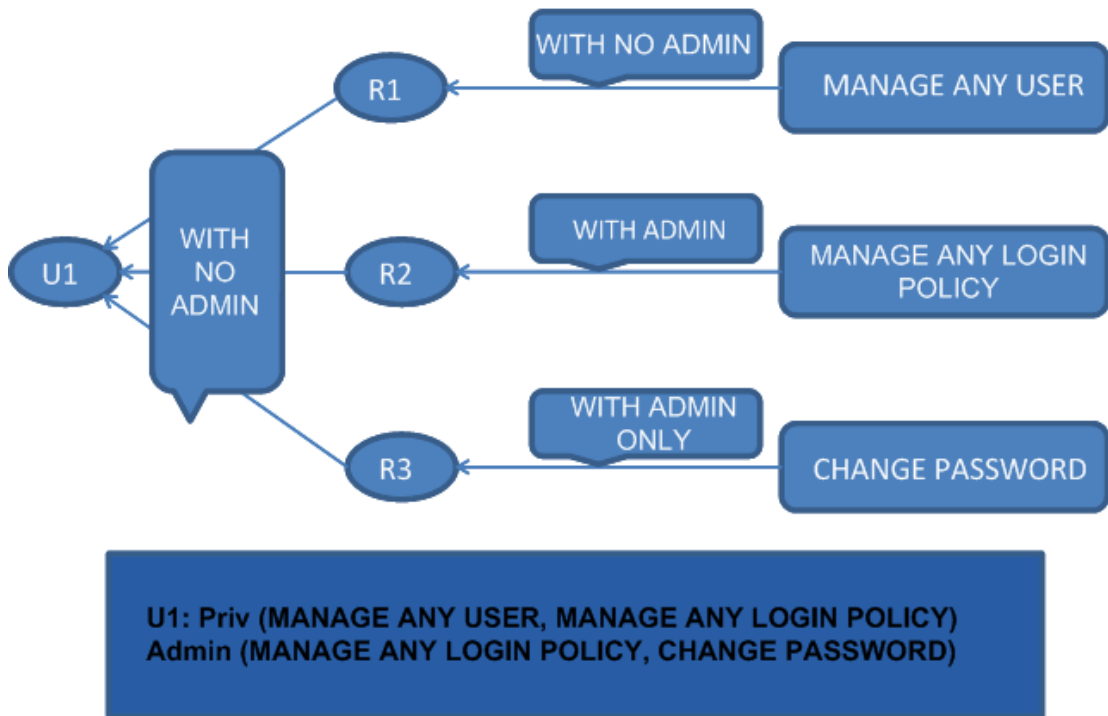
Dieses Diagramm zeigt Folgendes:

- Benutzer 1 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Benutzer 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Benutzer 3 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.

Daraus ergeben sich für die Benutzer 1, 2 und 3 die folgenden Privilegien:

	Benutzer 1	Benutzer 2	Benutzer 3
MANAGE ANY USER	Ausübung	-	-
MANAGE ANY LOGIN POLICY	-	Ausübung, Administration	-
CHANGE PASSWORD	-	-	Administration

## Szenario 2



Dieses Diagramm zeigt Folgendes:

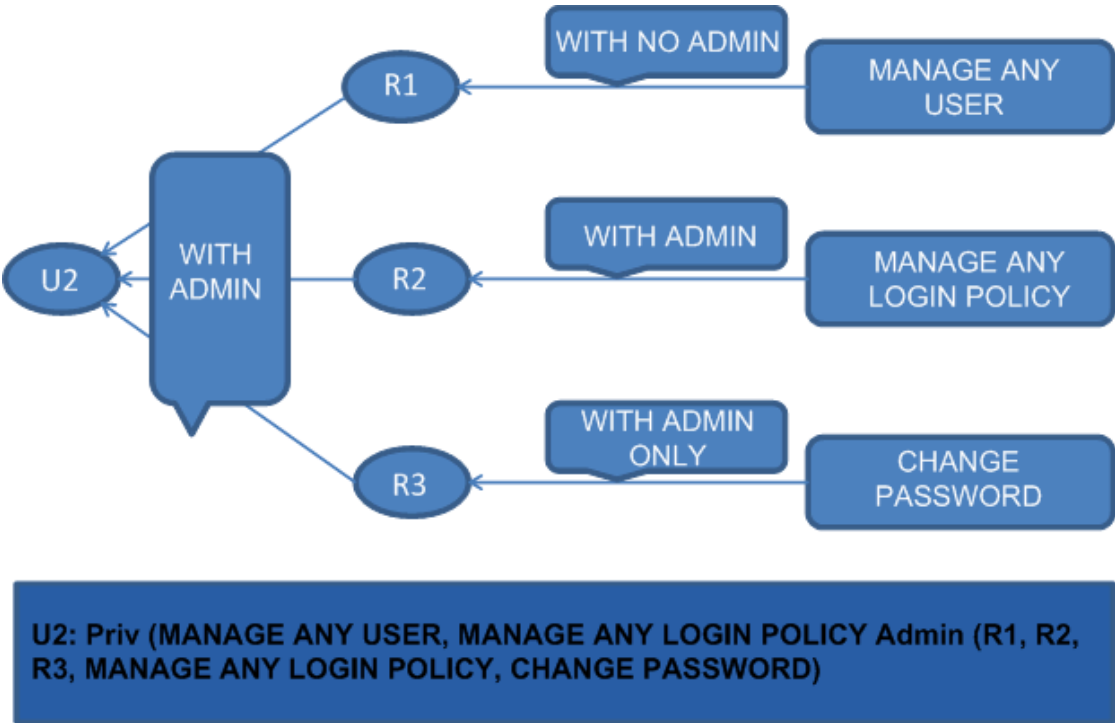
- Rolle 1 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 3 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.
- Benutzer 1 wurden Rolle 1, Rolle 2 und Rolle 3 ohne Administrationsrechte erteilt.

Benutzer 1 hat die folgenden Privilegien:

Rolle/Privileg	Benutzer 1
MANAGE ANY USER	Ausübung
MANAGE ANY LOGIN POLICY	Ausübung, Administration
CHANGE PASSWORD	Administration
R1	-
R2	-

Rolle/Privileg	Benutzer 1
R3	-

Szenario 3



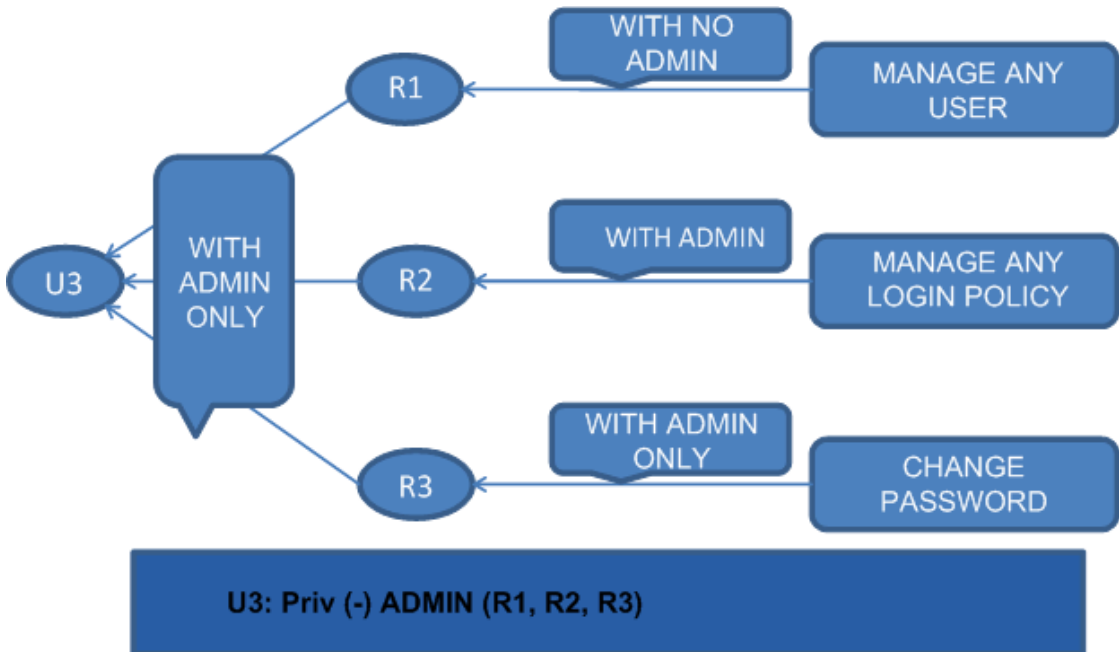
Dieses Diagramm zeigt Folgendes:

- Rolle 1 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 3 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.
- Benutzer 2 wurden Rolle 1, Rolle 2 und Rolle 3 mit Administrationsrechten erteilt.

Benutzer 2 hat die folgenden Privilegien:

Rolle/Privileg	Benutzer 2
MANAGE ANY USER	Ausübung
MANAGE ANY LOGIN POLICY	Ausübung, Administration

Rolle/Privileg	Benutzer 2
CHANGE PASSWORD	Administration
R1	Administration
R2	Administration
R3	Administration

**Szenario 4**

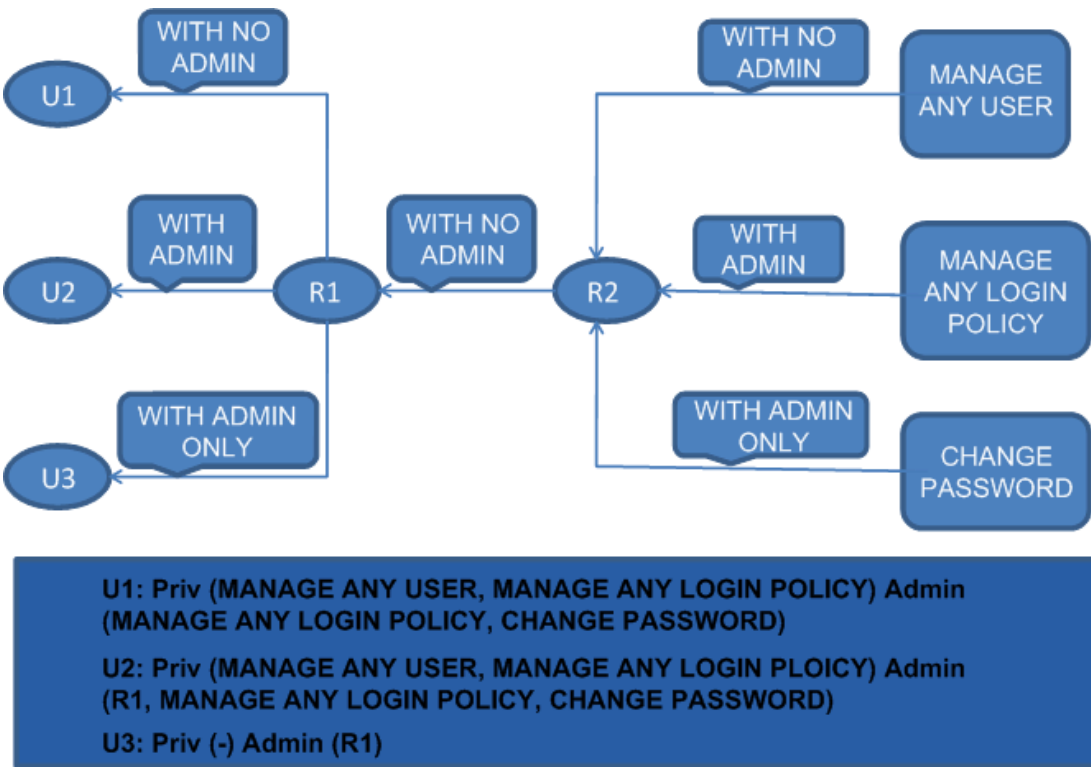
Dieses Diagramm zeigt Folgendes:

- Rolle 1 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 3 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.
- Benutzer 3 wurden Rolle 1, Rolle 2 und Rolle 3 nur mit Administrationsrechten erteilt.

Benutzer 3 hat die folgenden Privilegien:

Rolle/Privileg	Benutzer 3
MANAGE ANY USER	-
MANAGE ANY LOGIN POLICY	-
CHANGE PASSWORD	-
R1	Administration
R2	Administration
R3	Administration

Szenario 5



Dieses Diagramm zeigt Folgendes:

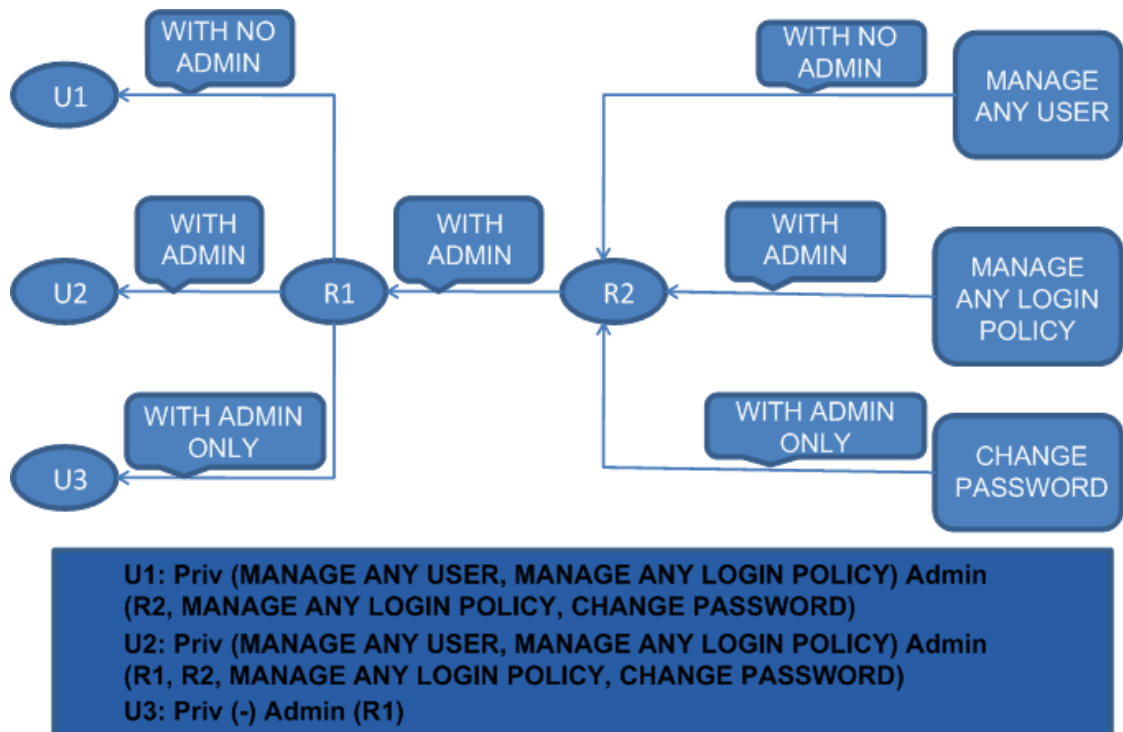
- Rolle 2 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 2 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.

- Rolle 1 wurde Rolle 2 ohne Administrationsrechte erteilt.
- Benutzer 1 wurde Rolle 1 ohne Administrationsrechte erteilt.
- Benutzer 2 wurde Rolle 1 mit Administrationsrechten erteilt.
- Benutzer 3 wurde Rolle 1 nur mit Administrationsrechten erteilt.

Benutzer 1, 2 und 3 haben die folgenden Privilegien:

Rolle/Privileg	Benutzer 1	Benutzer 2	Benutzer 3
MANAGE ANY USER	Ausübung	Ausübung	-
MANAGE ANY LOGIN POLICY	Ausübung, Administration	Ausübung, Administration	-
CHANGE PASSWORD	Administration	Administration	-
R1	-	Administration	Administration
R2	-	-	-

### Szenario 6

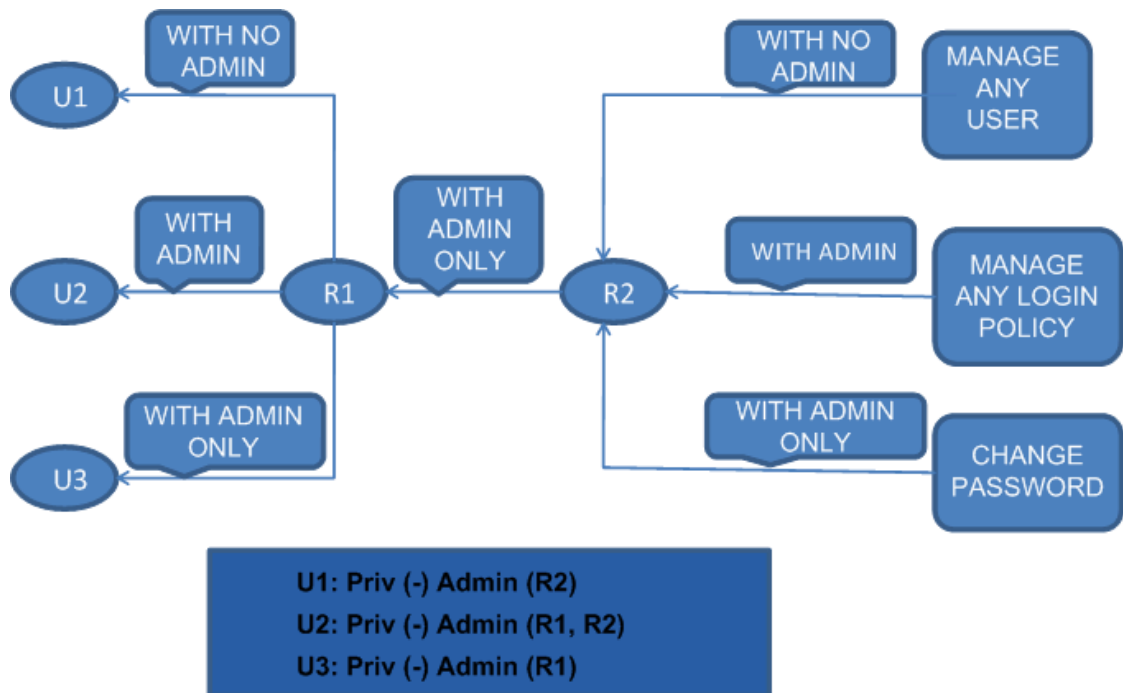


Dieses Diagramm zeigt Folgendes:

- Rolle 2 wurde das MANAGE ANY USER-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das MANAGE ANY LOGIN POLICY-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 2 wurde das CHANGE PASSWORD-Systemprivileg nur mit Administrationsrechten erteilt.
- Rolle 1 wurde Rolle 2 mit Administrationsrechten erteilt.
- Benutzer 1 wurde Rolle 1 ohne Administrationsrechte erteilt.
- Benutzer 2 wurde Rolle 1 mit Administrationsrechten erteilt.
- Benutzer 3 wurde Rolle 1 nur mit Administrationsrechten erteilt.

Benutzer 1, 2 und 3 haben die folgenden Privilegien:

Rolle/Privileg	Benutzer 1	Benutzer 2	Benutzer 3
MANAGE ANY USER	Ausübung	Ausübung	-
MANAGE ANY LOGIN POLICY	Ausübung, Administration	Ausübung, Administration	-
CHANGE PASSWORD	Administration	Administration	-
R1	-	Administration	Administration
R2	Administration	Administration	-

**Szenario 7**

Dieses Diagramm zeigt Folgendes:

- Rolle 2 wurde das **MANAGE ANY USER**-Systemprivileg ohne Administrationsrechte erteilt.
- Rolle 2 wurde das **MANAGE ANY LOGIN POLICY**-Systemprivileg mit Administrationsrechten erteilt.
- Rolle 2 wurde das **CHANGE PASSWORD**-Systemprivileg nur mit Administrationsrechten erteilt.
- Rolle 1 wurde Rolle 2 nur mit Administrationsrechten erteilt.
- Benutzer 1 wurde Rolle 1 ohne Administrationsrechte erteilt.
- Benutzer 2 wurde Rolle 1 mit Administrationsrechten erteilt.
- Benutzer 3 wurde Rolle 1 nur mit Administrationsrechten erteilt.

Benutzer 1, 2 und 3 haben die folgenden Privilegien:

Rolle/Privileg	Benutzer 1	Benutzer 2	Benutzer 3
MANAGE ANY USER	-	-	-
MANAGE ANY LOGIN POLICY	-	-	-

Rolle/Privileg	Benutzer 1	Benutzer 2	Benutzer 3
CHANGE PASSWORD	-	-	-
R1	-	Administration	Administration
R2	Administration	Administration	-

**Siehe auch**

- „Benutzerprivilegien beurteilen“ auf Seite 1331
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Vererbung von Rollen

Standardmäßig werden Systemprivilegien und Rollen von Berechtigungsempfängern der Rollen geerbt. Aus Gründen der Abwärtskompatibilität mit Datenbanken vor Version 16.0 musste jedoch die Möglichkeit zugelassen werden, die Vererbung von Rollen zu blockieren, die bisher nicht vererbte Berechtigungen waren. Dazu gehören die folgenden Rollen:

- SYS\_AUTH\_DBA\_ROLE-Systemrolle (in früheren Versionen die DBA-Berechtigung)
- SYS\_AUTH\_RESOURCE\_ROLE (in früheren Versionen die RESOURCE-Berechtigung)
- SYS\_AUTH\_BACKUP\_ROLE (in früheren Versionen die BACKUP-Berechtigung)
- SYS\_AUTH\_VALIDATE\_ROLE (in früheren Versionen die VALIDATE-Berechtigung)
- SYS\_RUN\_REPLICATION\_ROLE (in früheren Versionen die REMOTE DBA-Berechtigung)

Weitere Hinweise finden Sie unter „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

Wenn Sie Datenbanken vor Version 16.0 haben, finden Sie im folgenden Thema weitere Hinweise: „[Änderungen des Vererbungsverhaltens für einige Berechtigungen, die zu Rollen geworden sind](#)“ auf Seite 1400.

## Impersonierung

Ein Benutzer kann vorübergehend die Identität eines anderen Benutzers in der Datenbank annehmen (sogenannte **Impersonierung**), um Vorgänge auszuführen, sofern er eine Obermenge der Privilegien des zu impersonierenden Benutzers hat. Diese Einschränkung wird als die **Mindestkriterien** bezeichnet und gilt auch für Administrationsrechte und Privilegien auf Objektebene. Wenn ein Benutzer nicht *mindestens* dieselben Privilegien und Administrationsrechte hat wie der zu impersonierende Benutzer, kann er diesen nicht impersonieren.

Möglicherweise fragen Sie sich nun, warum ein Benutzer, der die Mindestkriterien erfüllt und sogar übertrifft, nicht einfach die Vorgänge selbst ausführt, statt für diesen Zweck einen anderen Benutzer zu impersonieren. Die Antwort darauf lautet: Wenn der impersonierende Benutzer mehr Privilegien hat als für die Aufgabe erforderlich, können die zusätzlichen Berechtigungen Auswirkungen auf die Ausgabe der Aufgabe haben. Durch das Impersonieren des Benutzers, der die Aufgabe normalerweise ausführt, wird

dies verhindert. Ziel ist es, genau die Privilegien, und möglicherweise auch Datenbankoptionen, zu simulieren, die für den impersonierten Benutzer in Kraft sind.

Die Möglichkeit, einen anderen Benutzer zu impersonieren, wird durch das SET USER-Systemprivileg gesteuert. Beim Erteilen des SET USER-Systemprivilegs können Sie konfigurieren, wen der betreffende Benutzer impersonieren kann:

- alle Benutzer in der Datenbank
- Benutzer aus einer angegebenen Liste von Benutzern
- Benutzer, die Berechtigungsempfänger von mindestens einer Rolle aus einer angegebenen Liste von Rollen sind

Die Mindestkriterien werden nicht zu dem Zeitpunkt ausgewertet, zu dem das SET USER-Systemprivileg erteilt wird. Stattdessen werden sie ausgewertet, wenn ein Benutzer versucht, einen anderen Benutzer zu impersonieren, indem er eine SETUSER-Anweisung ausführt.

Während einer Impersonierungssitzung werden GRANT- oder REVOKE-Vorgänge, durch die die Mindestkriterien verletzt würden, vom Datenbankserver nicht zugelassen. Es wird eine Fehlermeldung zurückgegeben, die anzeigt, dass der GRANT- bzw. REVOKE-Vorgang nicht fortgesetzt werden kann.

### Beispiel

Nehmen wir an, ein Datenerfasser mit dem Benutzernamen JSmithClerk hat Schwierigkeiten, einen Vorgang in der Datenbank auszuführen. Er spricht mit PJonesIT in der IT-Abteilung und PJonesIT beschließt, JSmithClerk zu impersonieren, um die bei JSmithClerk aufgetretenen Probleme beobachten und beheben zu können. Damit PJonesIT JSmithClerk impersonieren kann, müssen die folgenden Bedingungen erfüllt sein:

1. PJonesIT muss eine Obermenge der Privilegien haben, die JSmithClerk hat.
2. PJonesIT muss das SET USER-Systemprivileg auf eine der folgenden drei Arten erteilt worden sein:
  - Impersonierungsrechte direkt für einen oder mehrere Benutzer, einschließlich JSmithClerk  
(GRANT SET USER (JSmithClerk) TO PJonesIT;)
  - Impersonierungsrechte für alle Benutzer (GRANT SET USER TO PJonesIT;)
  - Impersonierungsrechte für Benutzer mit einer oder mehreren der Rollen, die auch JSmithClerk hat  
(GRANT SET USER (WITH ROLES ...) TO PJonesIT;)
3. PJonesIT muss eine SETUSER-Anweisung absetzen, um eine Impersonierungssitzung als JSmithClerk zu initiieren (SETUSER JSmithClerk). Für Vorgänge, die während der Impersonierungssitzung ausgeführt werden, werden die Privilegien von JSmithClerk verwendet. PJonesIT kann beschließen, dass die für JSmithClerk in Kraft befindlichen Datenbankoptionen in die Impersonierungssitzung übernommen werden sollen. In diesem Fall bezieht PJonesIT die WITH OPTION-Klausel in die SETUSER-Anweisung ein (SETUSER WITH OPTION JSmithClerk;).

## Weitere Hinweise zur Impersonierung

- Eine Impersonierungssitzung wird fortgesetzt, bis der impersonierende Benutzer eine SETUSER-Anweisung ausführt (ohne Angabe eines Benutzers), bis die Verbindung beendet wird oder bis der Benutzer beginnt, einen anderen Benutzer zu impersonieren.
- In Sybase Central enthält die Registerkarte **Systemprivilegien** für einen Benutzer in der SET USER-Zeile (falls vorhanden) Details dazu, wen ein Benutzer impersonieren kann. Bewegen Sie die Maus über die Zelle **Optionen**, um die Details zu überprüfen. Die Details umfassen nur SET USER-Privilegien, die dem Benutzer direkt erteilt wurden, keine geerbten SET USER-Privilegien.
- Wenn ein Benutzer einen anderen Benutzer impersoniert und einen Vorgang ausführt, wird im Transaktionslog die Benutzer-ID des impersonierten Benutzers erfasst. Die SETUSER-Anweisung wird jedoch ebenfalls im Transaktionslog erfasst, sodass ein Administrator den Beginn (und das Ende) einer Impersonierungssitzung erkennen kann.
- Wenn ein Benutzer nicht sicher ist, ob er immer noch einen anderen Benutzer impersoniert, kann er `SELECT CURRENT USER` ausführen. Der zurückgegebene Wert ist die für den Vorgang verwendete Benutzer-ID.
- In Interactive SQL wird die aktuelle Benutzer-ID beim Ausführen von Anweisungen in der Titelleiste des Fensters angezeigt.

## Siehe auch

- „Details zu den Mindestkriterien für die Impersonierung“ auf Seite 1360
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SETUSER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Details zu den Mindestkriterien für die Impersonierung

Ein Benutzer kann nur dann erfolgreich einen anderen Benutzer impersonieren, wenn die Mindestkriterien erfüllt sind. Die Validierung der Kriterien erfolgt, wenn eine SETUSER-Anweisung ausgeführt wird, nicht beim Erteilen des SET USER-Systemprivilegs. Wenn ein Benutzer beim Absetzen der SETUSER-Anweisung nicht alle Kriterien erfüllt, schlägt die Impersonierung fehl und ein Fehler wird zurückgegeben.

Es gibt vier Kriterien für eine erfolgreiche Impersonierung:

1. Dem impersonierenden Benutzer wurde das Recht erteilt, den Zielbenutzer zu impersonieren.
2. Der impersonierende Benutzer hat mindestens alle Rollen und Privilegien, die dem Zielbenutzer erteilt wurden.
3. Dem impersonierenden Benutzer wurden die Rollen und Systemprivilegien mit ähnlichen oder mehr Administrationsrechten erteilt.

In Bezug auf die Erfüllung der Kriterien zu Administrationsrechten gelten die Klauseln `WITH ADMIN OPTION` und `WITH ADMIN ONLY OPTION` als Erteilung ähnlicher Administratorberechtigungen. Außerdem gelten sie als Erteilung von mehr Administrationsrechten

als bei der WITH NO ADMIN OPTION-Klausel. Beispiel: Benutzer1 wird Rolle1 mit der WITH ADMIN OPTION-Klausel erteilt, Benutzer2 wird Rolle1 mit der WITH ADMIN ONLY-Klausel erteilt und Benutzer3 wird Rolle1 mit der WITH NO ADMIN OPTION-Klausel erteilt. Benutzer1 und Benutzer2 gelten dann als Benutzer mit Rolle1 und ähnlichen dazugehörigen Administrationsrechten. Außerdem gelten Benutzer1 und Benutzer2 als Benutzer mit mehr Administrationsrechten für Rolle1 als Benutzer3.

4. Falls dem Zielbenutzer ein Systemprivileg erteilt wurde, das zusätzliche Parameter unterstützt (auch als **Erweiterungen** bezeichnet, z.B. können Sie beim Erteilen des SET USER-Systemprivilegs eine Liste von Benutzer-IDs angeben), sind die Klauseln, die verwendet werden, um das Systemprivileg dem impersonierenden Benutzer zu erteilen, eine Obermenge derjenigen, die für den Zielbenutzer verwendet werden.

Derzeit unterstützen nur die Systemprivilegien SET USER und CHANGE PASSWORD Erweiterungen. Die beim Erteilen von SET USER und CHANGE PASSWORD an den impersonierenden Benutzer angegebenen Erweiterungen müssen denjenigen entsprechen, oder eine Obermenge davon sein, die angegeben wurden, als SET USER bzw. CHANGE PASSWORD dem Zielbenutzer erteilt wurden. Dies wird folgendermaßen ausgewertet:

- Die ANY-Erweiterung gilt als Obermenge der Erweiterungen *role-list* (Rollenliste) und *users-list* (Benutzerliste). Wenn der Zielbenutzer das SET USER-Systemprivileg mit ANY-Erweiterung hat (z.B. GRANT SET USER ANY TO user1), muss der impersonierende Benutzer ebenfalls die ANY-Erweiterung haben.
- Falls der Zielbenutzer das SET USER-Systemprivileg sowohl mit der *role-list*-Erweiterung als auch mit der *users-list*-Erweiterung hat, muss der impersonierende Benutzer ebenfalls das Systemprivileg mit beiden Erweiterungen haben und die Liste für jede Erweiterung muss der betreffenden Erweiterung des Zielbenutzers entsprechen oder eine Obermenge davon sein. Wenn beispielsweise die Erweiterungslisten sowohl beim impersonierenden Benutzer als auch beim Zielbenutzer Benutzer1 und Benutzer2 bzw. Rolle1 und Rolle2 enthalten, gelten die erteilten Ziellisten für jede der Klauseln als gleich. Alternativ gilt: Wenn die *users-list* für den impersonierenden Benutzer Benutzer1 und Benutzer2 bzw. Rolle1 und Rolle2 enthalten, während die *users-list* für den Zielbenutzer nur Benutzer1 bzw. Rolle2 enthalten, gilt die jeweilige *users-list* des impersonierenden Benutzers als Obermenge der Liste des Zielbenutzers.
- Falls der Zielbenutzer das SET USER-Systemprivileg mit einer einzelnen Listenerweiterung hat, muss die Erweiterungsliste des impersonierenden Benutzers der Liste des Zielbenutzers entsprechen oder eine Obermenge davon sein. Wenn beispielsweise die *Benutzerliste* sowohl beim impersonierenden Benutzer als auch beim Zielbenutzer Benutzer1 und Benutzer2 enthält, gelten beide als gleich. Wenn die *Benutzerliste* beim impersonierenden Benutzer Benutzer1 und Benutzer2 enthält, während die *Benutzerliste* beim Zielbenutzer nur Benutzer2 enthält, gilt die *Benutzerliste* des impersonierenden Benutzers als Obermenge der *Benutzerliste* des Zielbenutzers.

Daraus folgt: Wenn der impersonierende Benutzer die Systemprivilegien SET USER und CHANGE PASSWORD mit Erweiterungen hat, die ihre Verwendungsmöglichkeiten einschränken, aber der Zielbenutzer die Systemprivilegien ohne Einschränkungen hat, schlägt die Impersonierung fehl, weil die Mindestkriterien im Hinblick auf Erweiterungen nicht erfüllt sind.

## Szenario 1

Betrachten Sie das folgende Szenario unter der Annahme, dass das zweite und dritte Kriterium erfüllt sind:

- Es gibt fünf Benutzer: Benutzer1, Benutzer2, Benutzer3, Benutzer4 und Benutzer5.
- Es gibt zwei Rollen: Rolle1 und Rolle2.
- Benutzer1 wurde das SET USER-Systemprivileg mit ANY-Klausel erteilt.
- Benutzer2 wurde das SET USER-Systemprivileg mit *Benutzerliste*-Klausel für Benutzer1 und Benutzer4 erteilt.
- Benutzer3 wurde das SET USER-Systemprivileg erteilt, und zwar mit *Benutzerliste*-Klausel für Benutzer1, Benutzer2, Benutzer4 und Benutzer5 sowie mit der Klausel ANY WITH ROLES *Rollenliste* für Rolle1 und Rolle2.
- Benutzer4 wurde das SET USER-Systemprivileg mit ANY-Klausel und mit der *Rollenliste*-Klausel für Rolle1 erteilt.
- Benutzer5 wurde das SET USER-Systemprivileg erteilt, und zwar mit *Benutzerliste*-Klausel für Benutzer4 und mit der Klausel ANY WITH ROLES *Rollenliste* für Rolle1.
- Benutzer1 und Benutzer4 können Benutzer2, Benutzer3 und Benutzer5 impersonieren, weil beiden das SET USER-Systemprivileg mit ANY-Klausel erteilt wurde (Kriterium 4).

Benutzer2, Benutzer3 und Benutzer5 können weder Benutzer1 noch Benutzer4 impersonieren, weil bei ihnen die Erteilung nicht mit ANY-Klausel erfolgt ist (Kriterium 4).

Benutzer2 kann aus den folgenden Gründen weder Benutzer3 noch Benutzer5 impersonieren:

- Benutzer2 wird nicht das Recht erteilt, diese Benutzer zu impersonieren (Kriterium 1).
- Das SET USER-Systemprivileg wird Benutzer2 nicht mit *Rollenliste*-Klausel erteilt (Kriterium 4).

Benutzer3 kann aus den folgenden Gründen Benutzer2 impersonieren:

- Benutzer3 wird über die *Benutzerliste*-Klausel das Recht erteilt, Benutzer2 zu impersonieren (Kriterium 1).
- Die *Benutzerliste*-Klausel für Benutzer3 ist eine Obermenge derjenigen von Benutzer2 (Kriterium 4). Obwohl die Erteilung bei Benutzer3 mit *Rollenliste*-Klausel erfolgt ist, müssen die Anforderungen für die Impersonierung von Benutzer2 nicht erfüllt werden, weil dieser nicht dieselbe Erteilung hat.

Benutzer3 kann aus den folgenden Gründen Benutzer5 impersonieren:

- Benutzer3 wird über die *Benutzerliste*-Klausel das Recht erteilt, Benutzer5 zu impersonieren (Kriterium 1).
- Die Liste in der *Benutzerliste*-Klausel für Benutzer3 ist eine Obermenge derjenigen von Benutzer5 (Kriterium 4).

- Die Listen in den *Rollenlisten*-Klauseln von Benutzer3 und Benutzer5 sind äquivalent (Kriterium 4).

Benutzer5 kann aus den folgenden Gründen keinen der anderen Benutzer impersonieren:

- Bei Benutzer1 und Benutzer4 ist die Erteilung mit ANY-Klausel erfolgt (Kriterium 4).
- Bei Benutzer2 und Benutzer3 ist die Erteilung mit einer *Benutzerliste*-Klausel erfolgt, die keine Teilmenge derjenigen von Benutzer5 ist (Kriterium 4).

## Szenario 2

Betrachten Sie das folgende Szenario unter der Annahme, dass das erste und vierte Kriterium erfüllt sind:

- Es gibt zwei Benutzer: Benutzer6 und Benutzer7.
- Es gibt zwei Rollen: Rolle4 und Rolle5.
- Benutzer6 wurden Rolle4 mit WITH ADMIN OPTION-Klausel, Rolle5 mit der WITH ADMIN ONLY OPTION-Klausel und das MANAGE ANY USER-Systemprivileg mit WITH ADMIN OPTION-Klausel erteilt.
- Benutzer7 wurden Rolle4 mit WITH ADMIN OPTION-Klausel und Rolle5 mit WITH NO ADMIN OPTION-Klausel erteilt.

Benutzer6 kann aus den folgenden Gründen Benutzer7 impersonieren:

- Sowohl Benutzer6 und Benutzer7 werden Rolle4 und Rolle5 erteilt. Es ist unerheblich, dass Benutzer6 zusätzliche Privilegien (MANAGE ANY USER-Systemprivileg) erteilt wurden (Kriterium 2).
- Benutzer6 wird Rolle4 mit gleichwertigen Administrationsrechten wie Benutzer7 erteilt. Benutzer6 wird Rolle5 mit mehr Administrationsrechten erteilt als Benutzer7 (Kriterium 3).

Benutzer7 kann aus den folgenden Gründen nicht Benutzer6 impersonieren:

- Benutzer7 werden zwar Rolle4 und Rolle5 erteilt, aber nicht das MANAGE ANY USER-Systemprivileg (Kriterium 2).
- Benutzer7 wird Rolle5 mit niedrigeren Administrationsrechten erteilt als Benutzer6 (Kriterium 3).

## Szenario 3

Betrachten Sie das folgende Szenario:

- Es gibt drei Benutzer: Benutzer8, Benutzer9 und Benutzer10.
- Es gibt zwei Rollen: Rolle5 und Rolle6.
- Benutzer8 wurden Rolle5 mit der WITH ADMIN OPTION-Klausel und das MANAGE ANY USER-Systemprivileg mit der WITH ADMIN OPTION-Klausel erteilt.
- Benutzer9 und Benutzer10 wurde Rolle5 mit WITH NO ADMIN OPTION-Klausel erteilt.

- Benutzer8 wurde das SET USER-Systemprivileg zum Impersonieren von Benutzer9 und Benutzer10 mit der *Benutzerliste*-Klausel erteilt.
- Benutzer9 wurde das SET USER-Systemprivileg zum Impersonieren von Benutzer10 mit der *Benutzerliste*-Klausel erteilt.

Benutzer8 kann aus den folgenden Gründen Benutzer9 impersonieren:

- Benutzer8 wird über die *Benutzerliste*-Klausel das Recht erteilt, Benutzer9 zu impersonieren (Kriterium 1).
- Die Liste in der *Benutzerliste*-Klausel für Benutzer8 ist eine Obermenge derjenigen von Benutzer9 (Kriterium 4).
- Sowohl Benutzer8 als auch Benutzer9 wird Rolle5 erteilt, wobei Benutzer8 mehr Administrationsrechte für die Rolle erteilt werden als Benutzer9 (Kriterien 2 und 3).

Benutzer8 kann aus den folgenden Gründen Benutzer10 impersonieren:

- Benutzer8 wird das Recht erteilt, Benutzer10 zu impersonieren (Kriterium 1).
- Da Benutzer10 nicht das SET USER-Systemprivileg erteilt wird, ist Kriterium 4 nicht anwendbar.
- Sowohl Benutzer8 als auch Benutzer9 wird Rolle5 erteilt, und zwar mit denselben Administrationsrechten für die Rolle (Kriterien 2 und 3).

Benutzer9 kann aus den folgenden Gründen nicht Benutzer8 impersonieren:

- Benutzer9 wird nicht das Recht erteilt, Benutzer8 zu impersonieren (Kriterium 1).
- Obwohl Rolle5 sowohl Benutzer8 als auch Benutzer9 erteilt wird, erhält Benutzer9 weniger Administrationsrechte für die Rolle als Benutzer8 (Kriterium 3).

Die Validierung der Kriterien erfolgt beim Ausführen der SETUSER-Anweisung, nicht beim Erteilen des SET USER-Systemprivilegs. Wenn ein Benutzer beim Absetzen der SETUSER-Anweisung nicht alle Kriterien erfüllt, wird eine Meldung angezeigt, dass die Berechtigung verweigert wurde, und die Impersonierung beginnt nicht.

### Siehe auch

- „Impersonierung“ auf Seite 1358
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SETUSER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Rollenbasierte Sicherheitshierarchien planen und implementieren

### Sicherheitshierarchie planen

1. Ermitteln Sie die verschiedenen autorisierten Aufgaben, die von Benutzern ausgeführt werden sollen. Gruppieren Sie eng zusammenhängende Aufgaben. Gruppierungen können auf beliebigen

Organisationsstrukturen basieren: Abteilung, Funktion usw. Ordnen Sie jeder Gruppierung einen Namen zu. Diese Gruppierungen sind die **Rollen**, die Sie erstellen werden.

2. Ermitteln Sie die **Systemprivilegien** und **Privilegien auf Objektebene**, die für die einzelnen ermittelten Aufgaben erforderlich sind.
3. Ermitteln Sie die **Benutzer**, die die verschiedenen autorisierten Aufgaben ausführen müssen, einschließlich derjenigen, die die zu erstellenden Rollen benötigen.
4. (Optional) Ermitteln Sie **Administratoren** für die Rollen, die Sie erstellen möchten. Administratoren können anderen Benutzern die Rolle erteilen und entziehen.
5. (Optional) Ermitteln Sie Administratoren für die Systemprivilegien und Privilegien auf Objektebene, die nicht Teil der zu erstellenden Rollen sind.

### Sicherheitshierarchie aufbauen

1. Erstellen Sie die erforderlichen Rollen.
2. Erteilen Sie für jede Rolle die erforderlichen Systemprivilegien und Privilegien auf Objektebene.
3. Erstellen Sie die Benutzer.
4. Erteilen Sie die anwendbaren Rollen den Benutzern, ggf. einschließlich der dazugehörigen Administrationsrechte.
5. Erteilen Sie zusätzliche Rollen und Privilegien, die von einzelnen Benutzern benötigt werden.

## Eigentum an verschachtelten Objekten

Ansichten und Prozeduren können auf untergeordnete Objekte zugreifen, die andere Eigentümer haben. Wenn z.B. BenutzerA, BenutzerB, BenutzerC und BenutzerD vier verschiedene Benutzer sind, könnte BenutzerD.AnsichtD auf BenutzerC.AnsichtC basieren, die auf BenutzerB.AnsichtB basiert und die wiederum auf BenutzerA.TabelleA basiert. Ähnliches gilt für diese Prozeduren: BenutzerD.ProzedurD könnte BenutzerC.ProzedurC aufrufen, die wiederum BenutzerB.ProzedurB aufrufen könnte, die in BenutzerA.TabelleA einfügen könnte.

Die folgenden Regeln für Discretionary Access Control (DAC - beliebig bestimmbare Zugriffssteuerung) betreffen verschachtelte Ansichten und Tabellen:

- Um eine Ansicht erstellen zu können, benötigt der Benutzer das SELECT-Privileg für alle Basisobjekte (z.B. Tabellen und Ansichten) in der Ansicht.
- Damit der Zugriff auf eine Ansicht möglich ist, muss dem Eigentümer der Ansicht das entsprechende Privileg für die Basistabellen oder -ansichten (mit Administrationsrechten) erteilt worden sein und dem Benutzer muss das entsprechende Privileg für die Ansicht erteilt worden sein.
- Das Aktualisieren mit WHERE-Klausel erfordert sowohl das SELECT-Privileg als auch das UPDATE-Privileg.

- Wenn ein Benutzer Eigentümer der Tabellen in einer Ansichtsdefinition ist, kann der Benutzer über eine Ansicht auf die Tabellen zugreifen, auch wenn der Benutzer nicht der Eigentümer der Ansicht ist und ihm keine Zugriffsrechte für die Ansicht zugewiesen wurden.

Die folgenden DAC-Regeln betreffen verschachtelte Prozeduren:

- Ein Benutzer benötigt keine Privilegien für die zugrunde liegenden Objekte (z.B. Tabellen, Ansichten oder Prozeduren), um eine Prozedur erstellen zu können.
- Damit eine Prozedur ausgeführt werden kann, benötigt der Eigentümer der Prozedur die entsprechenden Privilegien für die von der Prozedur referenzierten Objekte.
- Auch wenn ein Benutzer Eigentümer aller von einer Prozedur referenzierten Tabellen ist, kann der Benutzer die Prozedur nur dann ausführen, um auf die Tabellen zuzugreifen, wenn ihm das EXECUTE-Privileg für die Prozedur erteilt wurde.

Es folgen einige Beispiele, die dieses Verhalten beschreiben.

### **Beispiel 1: Benutzer1 erstellt Tabelle1 und Benutzer2 erstellt Ansicht2 für Tabelle1**

- Benutzer1 kann immer auf Tabelle1 zugreifen, da Benutzer1 der Eigentümer ist.
- Benutzer1 kann immer über Ansicht2 auf Tabelle1 zugreifen, da Benutzer1 Eigentümer der Basistabelle ist. Dies gilt auch dann, wenn Benutzer2 Benutzer1 nicht das Privileg für Ansicht2 erteilt.
- Benutzer2 kann direkt oder über Ansicht2 auf Tabelle1 zugreifen, wenn Benutzer1 Benutzer2 das Privileg für Tabelle1 erteilt.
- Benutzer3 kann auf Tabelle1 zugreifen, wenn Benutzer1 Benutzer3 das Privileg für Tabelle1 erteilt.
- Benutzer3 kann über Ansicht2 auf Tabelle1 zugreifen, wenn Benutzer1 Benutzer2 das Privileg für Tabelle1 mit Weitergaberecht erteilt *und* Benutzer2 Benutzer3 das Privileg für Ansicht2 erteilt.

### **Beispiel 2: Benutzer2 erstellt Prozedur2, die auf Tabelle1 zugreift**

- Benutzer1 kann über Prozedur2 auf Tabelle1 zugreifen, wenn Benutzer2 Benutzer1 das EXECUTE-Privileg für Prozedur2 erteilt. Dies ist ein Unterschied zum Fall von Ansicht2, in dem Benutzer1 kein Privileg für Ansicht2 benötigt.

### **Beispiel 3: Benutzer1 erstellt Tabelle1, Benutzer2 erstellt Tabelle2 und Benutzer3 erstellt Ansicht3, die Tabelle1 und Tabelle2 verbindet**

- Benutzer3 kann über Ansicht3 auf Tabelle1 und Tabelle2 zugreifen, wenn Benutzer1 Benutzer3 das Privileg für Tabelle1 erteilt *und* Benutzer2 Benutzer3 das Privileg für Tabelle2 erteilt.

- Wenn Benutzer3 das Privileg für Tabelle1 hat, jedoch nicht für Tabelle2, kann Benutzer3 Ansicht3 nicht verwenden, auch nicht für den Zugriff auf die Teilmenge der Spalten, die zu Tabelle1 gehören.
- Benutzer1 oder Benutzer2 können Ansicht3 verwenden, wenn (a) Benutzer1 Benutzer3 das Privileg für Tabelle1 mit Weitergaberecht erteilt, (b) Benutzer2 Benutzer3 das Privileg für Tabelle2 mit Weitergaberecht erteilt *und* (c) Benutzer3 dem betreffenden Benutzer das Privileg für Ansicht3 erteilt.

## Kennwörter

Ein Benutzer kann eine Verbindung mit der Datenbank nur herstellen, wenn er ein Kennwort hat.

### Einschränkungen und Hinweise zu Benutzer-IDs und Kennwörtern

Benutzer-IDs dürfen Folgendes nicht:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.

Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.
- Sie dürfen nicht länger als 255 Byte sein.

Wenn Kennwörter erstellt oder geändert werden, werden sie in UTF-8 konvertiert, bevor sie einem Hash unterzogen und in der Datenbank gespeichert werden. Wenn die Datenbank entladen und in eine neue Datenbank mit einem anderen Zeichensatz geladen wird, funktionieren bestehende Kennwörter weiterhin. Wenn der Datenbankserver nicht vom Zeichensatz des Clients in UTF-8 konvertieren kann, wird empfohlen, dass das Kennwort aus 7-Bit ASCII-Zeichen zusammengesetzt ist, da andere Zeichen möglicherweise nicht korrekt funktionieren.

Standardmäßig müssen Kennwörter 3 Byte lang sein. Wenn Sie diese Anforderung ändern möchten, legen Sie die `min_password_length`-Datenbankoption fest.

Zusätzliche Regeln für Kennwörter können in der Login-Richtlinie eines Benutzers festgelegt werden.

### Siehe auch

- „Kennwörter für die Doppelkontrolle“ auf Seite 1370
- „Login-Richtlinien“ auf Seite 535

## Kennwörter ändern (Sybase Central)

Ändern Sie das Kennwort für einen Benutzer, indem Sie die Benutzereigenschaften bearbeiten.

## Voraussetzungen

Jeder Benutzer kann sein eigenes Kennwort ändern.

Um das Kennwort für einen anderen Benutzer ändern zu können, benötigen Sie das CHANGE PASSWORD-Systemprivileg.

Sie können das Kennwort für einen anderen Benutzer nicht mit Sybase Central ändern, wenn für diesen die Kennwortänderung mit Doppelkontrolle aktiviert ist (d.h., die Login-Richtlinienoption `change_password_dual_control` auf ON gesetzt ist). Wenn Sie Ihr eigenes Kennwort ändern und die Kennwortänderung mit Doppelkontrolle auf ON gesetzt ist, können Sie Ihr Kennwort trotzdem normal ändern. Die Doppelkontrolle wird nicht angewendet.

## Kontext und Bemerkungen

Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.
- Sie dürfen nicht länger als 255 Byte sein.

## Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Doppelklicken Sie auf **Benutzer**, rechtsklicken Sie auf einen Benutzer und klicken Sie dann auf **Eigenschaften**.
3. Vergewissern Sie sich, dass die Option **Dieser Benutzer hat ein Kennwort** aktiviert ist.
4. Füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.
5. Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

## Ergebnisse

Das Benutzerkennwort wird geändert.

## Nächste Schritte

Informieren Sie den Benutzer über sein neues Kennwort.

## Siehe auch

- „Login-Richtlinien“ auf Seite 535
- „ALTER USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kennwörter für die Doppelkontrolle festlegen (SQL)“ auf Seite 1370

## Kennwörter ändern (SQL)

Ändern Sie das Kennwort für einen Benutzer mithilfe einer ALTER USER-Anweisung mit IDENTIFIED BY-Klausel.

### Voraussetzungen

Jeder Benutzer kann sein eigenes Kennwort ändern. Um das Kennwort für einen anderen Benutzer ändern zu können, benötigen Sie das CHANGE PASSWORD-Systemprivileg.

Wenn Sie Ihr eigenes Kennwort ändern und die Kennwortänderung mit Doppelkontrolle auf ON gesetzt ist, können Sie Ihr Kennwort trotzdem normal ändern. Die Doppelkontrolle ist dann nicht erforderlich.

### Kontext und Bemerkungen

Kennwörter berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.
- Sie dürfen nicht länger als 255 Byte sein.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Führen Sie die ALTER USER-Anweisung aus, die eine IDENTIFIED BY-Klausel mit Angabe des neuen Kennworts enthält.

### Ergebnisse

Das Benutzerkennwort wird geändert.

### Nächste Schritte

Informieren Sie den Benutzer über sein neues Kennwort.

### Beispiel

Führen Sie die folgende Anweisung aus, um das Kennwort für den DBA-Benutzer in "welcome\_DBA" zu ändern:

```
ALTER USER DBA  
IDENTIFIED BY welcome_DBA;
```

### Siehe auch

- „ALTER USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kennwörter für die Doppelkontrolle festlegen (SQL)“ auf Seite 1370

## Kennwörter für die Doppelkontrolle

Die Kennwortfunktion für die Doppelkontrolle erfordert zwei Administratoren zum Ändern eines Kennworts. Diese Konfiguration verhindert, dass ein einzelner Administrator das vollständige Kennwort eines anderen Benutzers kennt. Ein Administrator legt den ersten Teil eines Kennworts fest und ein anderer Administrator den zweiten Teil des Kennworts. Der Benutzer gibt die beiden Kennwortteile an, um eine Verbindung mit der Datenbank herzustellen.

In der Login-Richtlinie des Zielbenutzers muss die `change_password_dual_control`-Option aktiviert sein.

### Siehe auch

- „ALTER USER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- Login-Richtlinienoptionen und Standardwerte auf Seite 536
- „Kennwörter für die Doppelkontrolle festlegen (SQL)“ auf Seite 1370

## Kennwörter für die Doppelkontrolle festlegen (SQL)

Legen Sie ein Kennwort für die Doppelkontrolle fest bzw. ändern Sie den ersten oder letzten Teil eines Kennworts für die Doppelkontrolle. Diese Funktion verhindert, dass ein einzelner Administrator das vollständige Kennwort eines Benutzers kennt.

### Voraussetzungen

Sie müssen das `CHANGE PASSWORD`-Systemprivileg haben.

In der Login-Richtlinie des Zielbenutzers muss die `change_password_dual_control`-Option aktiviert sein.

### Kontext und Bemerkungen

Ein anderer Administrator muss den anderen Teil des Kennworts ändern. Der Benutzer kombiniert die beiden Kennwortteile und verwendet dieses kombinierte Kennwort für Verbindungen mit der Datenbank.

Kennwortteile berücksichtigen die Groß- und Kleinschreibung. Im Übrigen gelten folgende Voraussetzungen:

- Sie dürfen nicht mit Leerstellen, Apostrophen oder Anführungszeichen beginnen.
- Sie dürfen nicht mit Leerstellen enden.
- Sie dürfen keine Semikola enthalten.
- Sie dürfen nicht länger als 127 Byte sein.

### Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Ein Administrator führt die folgende Anweisung aus, um den ersten Teil des Kennworts für die Doppelkontrolle festzulegen, und teilt anschließend dem Benutzer *password-part1* mit:

```
ALTER USER user-name IDENTIFIED FIRST BY password-part1;
```

3. Ein anderer Administrator führt die folgende Anweisung aus, um den zweiten Teil des Kennworts für die Doppelkontrolle festzulegen, und teilt anschließend dem Benutzer *password-part2* mit:

```
ALTER USER user-name IDENTIFIED LAST BY password-part2;
```

### Ergebnisse

Das Kennwort für den Zielbenutzer wird auf die Kombination aus dem ersten und letzten Kennwortteil gesetzt (*password-part1 password-part2*).

### Nächste Schritte

Der Zielbenutzer stellt mit den kombinierten Teilen als Kennwort eine Verbindung mit der Datenbank her und wird aufgefordert, ein neues Kennwort zu erstellen.

### Siehe auch

- „ALTER USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Kennwörter für die Doppelkontrolle“ auf Seite 1370
- „Login-Richtlinien“ auf Seite 535

## Praktische Einführung: Rollen und Privilegien erteilen (Sybase Central)

Im rollenbasierten Sicherheitsmodell müssen Benutzer bestimmte Privilegien oder Rollen haben, um bestimmte Datenbankvorgänge ausführen zu können. In dieser praktischen Einführung sind Sie ein Datenbankadministrator mit vollen Administrationsrechten. Sie möchten zwei Kollegen die Verantwortung für das Debugging von Prozeduren und für das Korrigieren der dabei gefundenen Fehler übertragen. Außerdem sollen dieselben Kollegen für das Ausführen von Sicherungen der Unternehmensdatenbank verantwortlich sein. (In diesem Szenario ist die Datenbank die SQL Anywhere-Beispieldatenbank.) Schließlich sollen beide Kollegen die Möglichkeit haben, die Tabelle "Employees" in der Datenbank zu aktualisieren.

Sie müssen Benutzer-IDs für beide Kollegen erstellen und ihnen die für diese Aufgaben notwendigen Privilegien und Rollen erteilen. In dieser praktischen Einführung verwenden Sie Sybase Central, um die gestellten Aufgaben auszuführen.

#### Hinweis

Sybase Central legt Informationen zur Datenbank im Cache ab, z.B. dazu, welche Privilegien und Rollen ein Benutzer hat. Wenn Sie Änderungen an der Datenbank über eine andere Verbindung vornehmen, erkennt Sybase Central die Änderungen erst, wenn Sie die Datenbank in Sybase Central aktualisieren. Dazu können Sie in der Struktur im linken Fensterausschnitt die Datenbank oder ein beliebiges Objekt auswählen und anschließend F5 drücken.

### Privilegien

Keine. Sie melden sich bei der Datenbank mit der Benutzer-ID DBA an, die alle für die praktische Einführung erforderlichen Systemprivilegien und Rollen hat.

### Siehe auch

- „Benutzersicherheit (Rollen und Privilegien)“ auf Seite 1271
- „Upgrade auf rollenbasierte Sicherheit“ auf Seite 1385

## Lektion 1: Zwei neue Benutzer erstellen, Benutzer1 und Benutzer2 (Sybase Central)

Melden Sie sich über Sybase Central bei der Beispieldatenbank an und erstellen Sie zwei neue Benutzer.

### Voraussetzungen

Keine.

### Aufgabe

1. Starten Sie Sybase Central und stellen Sie eine Verbindung zur Datenbank her.
  - a. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.
  - b. Klicken Sie auf **Verbindungen » Verbinden mit SQL Anywhere 16**.
  - c. Wählen Sie in der Dropdown-Liste **Aktion** die Option **Mit ODBC-Datenquelle verbinden**.
  - d. Klicken Sie im Feld **ODBC-Datenquellenname** auf **Durchsuchen**, wählen Sie **SQL Anywhere 16 Demo** und klicken Sie dann auf **OK**.
  - e. Klicken Sie auf **Verbinden**. Damit verbinden Sie sich als Benutzer namens DBA mit dem Kennwort "sql" mit der Beispieldatenbank. Dieser Benutzer hat volle Administrationsrechte für die Datenbank.
2. Erstellen Sie zwei neue Benutzer.
  - a. Rechtsklicken Sie im linken Fensterausschnitt auf **Benutzer** und klicken Sie dann auf **Neu » Benutzer**.
  - b. Im Feld **Wie lautet der Name des neuen Benutzers?** geben Sie **User1** ein. Klicken Sie dann auf **Weiter**.
  - c. Ordnen Sie Benutzer1 das Kennwort **sql** zu und klicken Sie dann auf **Fertig stellen**.
  - d. Wiederholen Sie die oben angegebenen Schritte, um den zweiten Benutzer, **User2**, zu erstellen.

### Ergebnisse

Sie haben zwei neue Benutzer erstellt, Benutzer1 und Benutzer2.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 2: Benutzer1 Privilegien erteilen \(Sybase Central\)](#)“ auf Seite 1373.

**Siehe auch**

- „Benutzer erstellen (Sybase Central)“ auf Seite 1341
- „Benutzer erstellen (SQL)“ auf Seite 1342
- „CREATE USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

**Lektion 2: Benutzer1 Privilegien erteilen (Sybase Central)**

Erteilen Sie Benutzer1 Systemprivilegien und Privilegien auf Objektebene.

**Voraussetzungen**

In dieser Lektion wird davon ausgegangen, dass Sie die vorherige Lektion in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 1: Zwei neue Benutzer erstellen, Benutzer1 und Benutzer2 \(Sybase Central\)](#)“ auf Seite 1372.

**Aufgabe**

1. Klicken Sie im linken Fensterausschnitt von Sybase Central auf **Benutzer**, um den Eintrag zu erweitern, und klicken Sie dann auf **User1**.
2. Erteilen Sie Benutzer1 die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT.
  - a. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Systemprivilegien**.
  - b. Rechtsklicken Sie auf die Registerkarte und klicken Sie auf **Neu » Erteilte Systemprivilegien**.
  - c. Klicken Sie auf das **BACKUP DATABASE**-Systemprivileg und anschließend auf **OK**.
  - d. Wiederholen Sie die oben beschriebenen Schritte. Klicken Sie diesmal auf das **VALIDATE ANY OBJECT**-Systemprivileg und anschließend auf **OK**.
  - e. Klicken Sie auf **Datei » Speichern**, um Ihre Änderungen in der Datenbank zu speichern.
3. Erteilen Sie Benutzer1 die Privilegien SELECT und UPDATE auf Objektebene für die Tabelle "Employees", mit Administrationsrechten.
  - a. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Tabellenprivilegien**.
  - b. Rechtsklicken Sie auf die Registerkarte und klicken Sie auf **Neu » Privilegien**.
  - c. Klicken Sie auf die Tabelle **Employees** und anschließend auf **OK**. Die Tabelle "Employees" wird zur Liste der Tabellen für Benutzer1 hinzugefügt. Jedes Häkchen in den Buchstabenspalten zeigt ein Privileg auf Objektebene an, das Benutzer1 für die Tabelle hat, z.B. **S** für SELECT, **I** für INSERT usw. In dieser Lektion darf jedoch nur Benutzer1 die Möglichkeit haben, aus der Tabelle "Employees" auszuwählen und sie zu aktualisieren.
  - d. Klicken Sie auf die Zellen unterhalb der Spalten, um ihren Inhalt zu löschen, bis nur noch in den Spalten **S** (für SELECT) und **U** (für UPDATE) Häkchen mit Pluszeichen (+) angezeigt werden. Das Pluszeichen zeigt Administrationsrechte an. Alle anderen Zellen in der Zeile müssen leer sein.
  - e. Klicken Sie auf **Datei » Speichern**, um Ihre Änderungen in der Datenbank zu speichern.

## Ergebnisse

Benutzer1 hat nun die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT, die erforderlich sind, um die SQL Anywhere-Beispieldatenbank zu sichern. Außerdem hat Benutzer1 die Privilegien SELECT und UPDATE auf Objektebene für die Tabelle "Employees" und kann diese Privilegien anderen Benutzern erteilen.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: Rolle erstellen und Benutzer1 erteilen \(Sybase Central\)](#)“ auf Seite 1374.

## Siehe auch

- „Systemprivilegien“ auf Seite 1309
- „Systemprivilegien erteilen (Sybase Central)“ auf Seite 1331
- „Systemprivilegien erteilen (SQL)“ auf Seite 1332
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Lektion 3: Rolle erstellen und Benutzer1 erteilen (Sybase Central)

Erstellen Sie eine Rolle mit den Privilegien, die notwendig sind, um das Debugging einer Prozedur durchzuführen und während dieses Prozesses gefundene Fehler zu korrigieren, und erteilen Sie diese Rolle Benutzer1. Erteilen Sie Benutzer1 außerdem Administrationsrechte für die Rolle, damit er die Rolle ggf. anderen Benutzern erteilen oder entziehen kann.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 2: Benutzer1 Privilegien erteilen \(Sybase Central\)](#)“ auf Seite 1373.

## Aufgabe

1. Erstellen Sie die Rolle.
  - a. Rechtsklicken Sie im linken Fensterausschnitt von Sybase Central auf **Rollen** und klicken Sie auf **Neu » .Rolle**.
  - b. Im Feld **Wie soll der Name der neuen benutzerdefinierten Rolle lauten?** geben Sie **DebugAndAlter** ein und klicken Sie dann auf **Weiter**.
  - c. Klicken Sie auf dem Bildschirm **Administratoren wählen** auf **Fertig stellen**, um den Standardwert zu akzeptieren und damit zuzulassen, dass Benutzer mit dem MANAGE ROLES-Systemprivileg (sogenannte globale Administratoren) die Rolle verwalten.
2. Erteilen Sie der Rolle die erforderlichen Systemprivilegien.
  - a. Doppelklicken Sie im linken Fensterausschnitt auf **Rollen** und wählen Sie **DebugAndAlter** aus.
  - b. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Systemprivilegien**.
  - c. Rechtsklicken Sie auf die Registerkarte und klicken Sie auf **Neu » Erteilte Systemprivilegien**.

- d. Klicken Sie auf das **ALTER ANY OBJECT**-Systemprivileg und anschließend auf **OK**.
  - e. Rechtsklicken Sie erneut auf die Registerkarte, klicken Sie auf **Neu » Erteilte Systemprivilegien**, wählen Sie **DEBUG ANY PROCEDURE** aus und klicken Sie dann auf **OK**.
  - f. Klicken Sie auf **Datei » Speichern**, um Ihre Änderungen in der Datenbank zu speichern.
3. Erteilen Sie Benutzer1 die Rolle mit Administrationsrechten.
    - a. Doppelklicken Sie im linken Fensterausschnitt auf **Benutzer** und wählen Sie **User1** aus.
    - b. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Rollen**.
    - c. Rechtsklicken Sie auf die Registerkarte und klicken Sie dann auf **Neu » Erteilte Rollen**.
    - d. Klicken Sie auf **DebugAndAlter** und anschließend auf **OK**. Benutzer1 wird die Möglichkeit gewährt, die DebugAndAlter-Rolle auszuüben, jedoch ohne Administrationsrechte.
    - e. Klicken Sie im rechten Fensterausschnitt in der Zeile für die DebugAndAlter-Rolle auf die Zelle in der Spalte **Adm.**, um ein Häkchen hinzuzufügen. Dadurch werden Benutzer1 Administrationsrechte für die Rolle erteilt.
    - f. Klicken Sie auf **Datei » Speichern**, um Ihre Änderungen in der Datenbank zu speichern.

## Ergebnisse

Die DebugAndAlter-Rolle, die die Systemprivilegien DEBUG ANY PROCEDURE und ALTER ANY OBJECT hat, wurde erstellt und Benutzer1 erteilt. Außerdem wurden Benutzer1 Administrationsrechte für die Rolle erteilt.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 4: Benutzer1 in eine benutzererweiterte Rolle konvertieren und diese Rolle Benutzer2 erteilen \(Sybase Central\)“](#) auf Seite 1375.

## Siehe auch

- [„Benutzerdefinierte Rollen erstellen \(Sybase Central\)“](#) auf Seite 1285
- [„Rollen und Privilegien für Rollen konfigurieren \(Sybase Central\)“](#) auf Seite 1296
- [„Rollen erteilen \(Sybase Central\)“](#) auf Seite 1298
- [„GRANT-Anweisung“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Lektion 4: Benutzer1 in eine benutzererweiterte Rolle konvertieren und diese Rolle Benutzer2 erteilen (Sybase Central)

Angenommen, Sie möchten Benutzer2 dieselben Privilegien und Rollen erteilen wie Benutzer1. Statt denselben langwierigen Prozess durchzuführen wie bei Benutzer1, dem Sie die Rollen und Privilegien explizit erteilt haben, können Sie Benutzer1 in eine benutzererweiterte Rolle konvertieren und diese Rolle Benutzer2 erteilen. Benutzer1 bleibt weiterhin ein Benutzer, der sich bei der Datenbank anmelden kann, und fungiert zusätzlich als Rolle.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 3: Rolle erstellen und Benutzer1 erteilen \(Sybase Central\)](#)“ auf Seite 1374.

## Aufgabe

1. Konvertieren Sie Benutzer1 in eine benutzererweiterte Rolle.
  - a. Klicken Sie im linken Fensterausschnitt von Sybase Central auf **Benutzer** und anschließend auf **User1**.
  - b. Rechtsklicken Sie in den rechten Fensterausschnitt und klicken Sie auf **In benutzererweiterte Rolle ändern**.
2. Erteilen Sie Benutzer2 die benutzererweiterte Rolle Benutzer1.
  - a. Doppelklicken Sie im linken Fensterausschnitt auf **Benutzer** und klicken Sie auf **User2**.
  - b. Klicken Sie auf die Registerkarte **Rollen**.
  - c. Rechtsklicken Sie auf die Registerkarte und klicken Sie auf **Neu » Erteilte Rollen**.
  - d. Klicken Sie auf **User1** und anschließend auf **OK**.
  - e. Klicken Sie auf **Datei » Speichern**, um Ihre Änderungen in der Datenbank zu speichern.

## Ergebnisse

Benutzer1 wurde in eine benutzererweiterte Rolle konvertiert und diese Rolle wurde Benutzer2 erteilt.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 5: Rollen und Privilegien für Benutzer2 anzeigen \(Sybase Central\)](#)“ auf Seite 1376.

## Siehe auch

- „Benutzererweiterte Rollen“ auf Seite 1287
- „CREATE ROLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Lektion 5: Rollen und Privilegien für Benutzer2 anzeigen (Sybase Central)

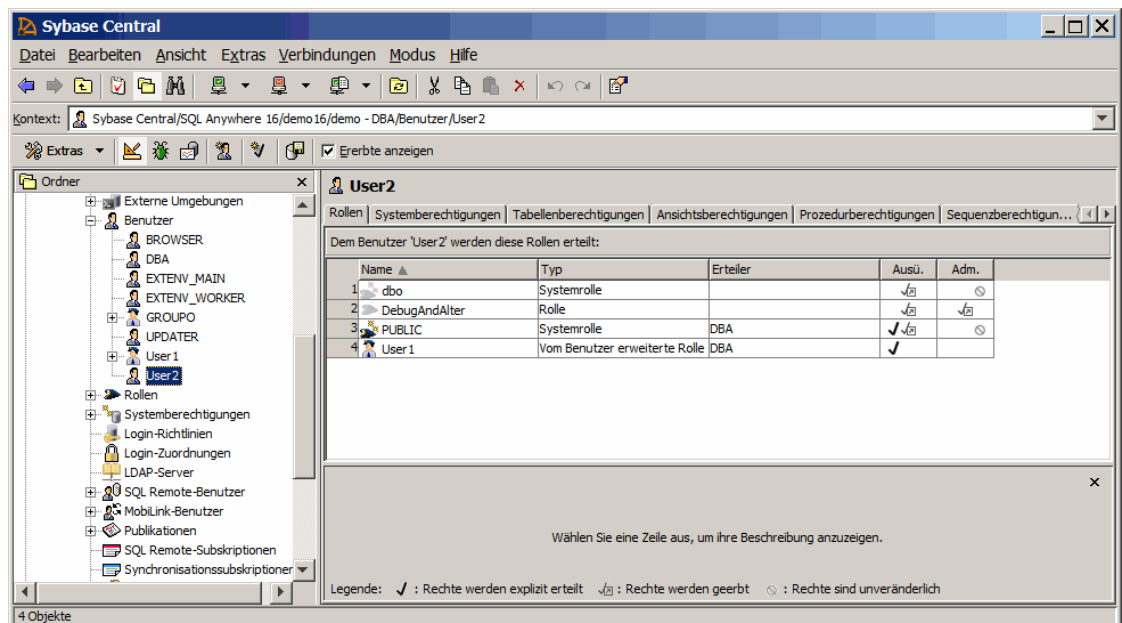
Sie können die Rollen und Privilegien eines Benutzers anzeigen, einschließlich derjenigen, die der Benutzer durch Mitgliedschaft in anderen Rollen geerbt hat.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 4: Benutzer1 in eine benutzererweiterte Rolle konvertieren und diese Rolle Benutzer2 erteilen \(Sybase Central\)](#)“ auf Seite 1375.

## Aufgabe

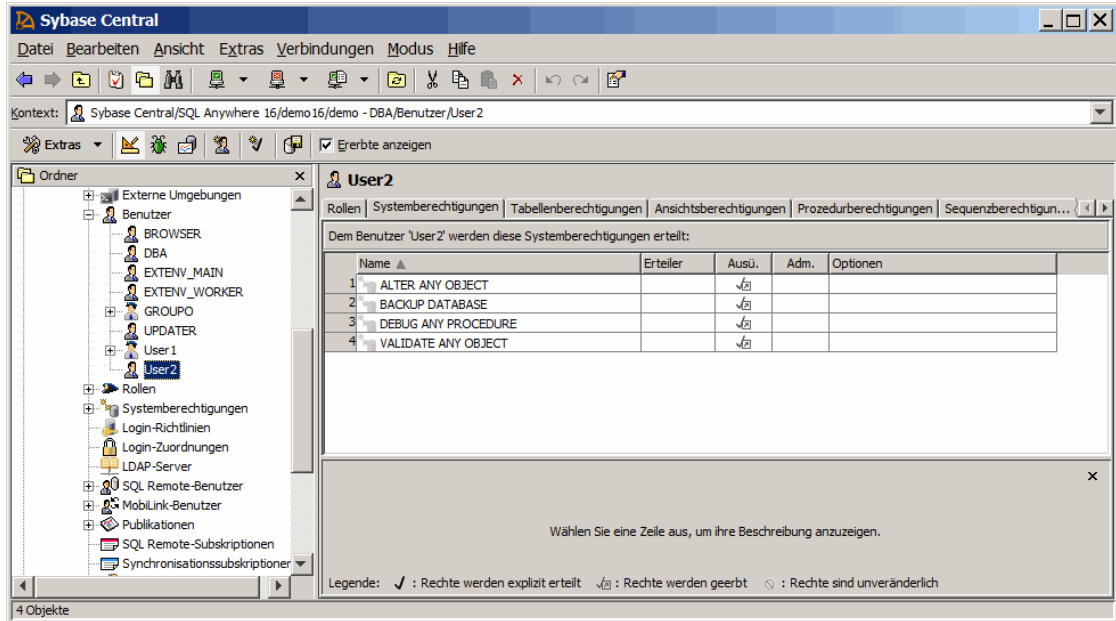
1. Doppelklicken Sie im linken Fensterausschnitt von Sybase Central auf **Benutzer** und klicken Sie auf **User2**.
2. Vergewissern Sie sich, dass am oberen Bildschirmrand das Kontrollkästchen **Ererbte anzeigen** aktiviert ist.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Rollen**, um die Rollen für Benutzer2 anzuzeigen.



Auf dem Screenshot sehen Sie, dass Benutzer2 die folgenden Rollen hat:

- **dbo-Systemrolle** Benutzer2 hat Ausübungsrechte, aber keine Administrationsrechte für die dbo-Systemrolle. Ein Berechtigungsgeber ist nicht vorhanden, weil Benutzer2 diese Systemrolle als Mitglied der PUBLIC-Systemrolle erbt. Benutzern wird beim Erstellen standardmäßig die PUBLIC-Systemrolle erteilt.
- **Benutzerdefinierte Rolle DebugAndAlter** Benutzer2 hat Ausübungs- und Administrationsrechte für die DebugAndAlter-Rolle. Ein Berechtigungsgeber ist nicht vorhanden, weil Benutzer2 diese benutzerdefinierte Rolle von Benutzer1 erbt.
- **PUBLIC-Systemrolle** Benutzer2 hat Ausübungsrechte für die PUBLIC-Rolle. Benutzern wird beim Erstellen standardmäßig die PUBLIC-Systemrolle erteilt. Der Berechtigungsgeber ist DBA, weil Sie beim Erstellen von Benutzer2 unter dieser Benutzer-ID angemeldet waren.
- **Benutzererweiterte Rolle Benutzer1** Benutzer2 hat Ausübungsrechte, aber keine Administrationsrechte für die benutzererweiterte Rolle Benutzer1. Der Berechtigungsgeber ist DBA, weil Sie beim Erteilen der Rolle an Benutzer2 unter dieser Benutzer-ID angemeldet waren.

4. Klicken Sie auf die Registerkarte **Systemprivilegien**, um die Systemprivilegien anzuzeigen, die Benutzer2 hat. Die Spalte für den Berechtigungsgeber ist bei allen leer, weil die Systemprivilegien geerbt wurden, nicht explizit Benutzer2 erteilt. Die Spalte **Adm.** ist leer, weil beim Erteilen der Systemprivilegien keine Administrationsrechte erteilt wurden.



## Ergebnisse

Sie haben die Rollen, Privilegien und Administrationsrechte für Benutzer2 überprüft.

## Siehe auch

- „Vererbung von Rollen und Privilegien“ auf Seite 1348
- „Systemprivilegien erteilen (Sybase Central)“ auf Seite 1331
- „Rollen erteilen (Sybase Central)“ auf Seite 1298
- „Rollenadministratoren“ auf Seite 1293

## Praktische Einführung: Rollen und Privilegien erteilen (SQL)

Im rollenbasierten Sicherheitsmodell müssen Benutzer bestimmte Privilegien oder Rollen haben, um bestimmte Datenbankvorgänge ausführen zu können. In dieser praktischen Einführung sind Sie ein Datenbankadministrator mit vollen Administrationsrechten. Sie möchten zwei Kollegen die Verantwortung für das Debugging von Prozeduren und für das Korrigieren der dabei gefundenen Fehler übertragen. Außerdem sollen dieselben Kollegen für das Ausführen von Sicherungen der Unternehmensdatenbank verantwortlich sein. (In diesem Szenario ist die Datenbank die SQL Anywhere-Beispieldatenbank.) Schließlich sollen beide Kollegen die Möglichkeit haben, die Tabelle "Employees" in der Datenbank zu aktualisieren.

Sie müssen Benutzer-IDs für beide Kollegen erstellen und ihnen die für diese Aufgaben notwendigen Privilegien und Rollen erteilen.

### Privilegien

Keine. Sie melden sich bei der Datenbank mit der Benutzer-ID DBA an, die alle für die praktische Einführung erforderlichen Systemprivilegien und Rollen hat.

### Siehe auch

- „Benutzersicherheit (Rollen und Privilegien“ auf Seite 1271
- „Upgrade auf rollenbasierte Sicherheit“ auf Seite 1385

## Lektion 1: Zwei neue Benutzer erstellen, UserA und UserB (SQL)

Melden Sie sich mit der Benutzer-ID DBA bei Sybase Central an und erstellen Sie zwei neue Benutzer, die für das Sichern der Beispieldatenbank, für das Debugging von Prozeduren und für das Korrigieren der dabei gefundenen Fehler verantwortlich sein sollen.

### Voraussetzungen

Keine.

### Aufgabe

1. Starten Sie Sybase Central.
  - a. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.
  - b. Klicken Sie auf **Extras » SQL Anywhere 16 » Interactive SQL öffnen**.  
Füllen Sie die folgenden Felder aus, um eine Verbindung mit der Beispieldatenbank herzustellen:
    - i. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
    - ii. Im Feld **Kennwort** geben Sie **sql** ein.
    - iii. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**.
    - iv. Im Feld **Servername** geben Sie **demo16** ein.Klicken Sie auf **Verbinden**. Interactive SQL stellt eine Verbindung mit der Datenbank her.
2. Erstellen Sie zwei neue Benutzer.
  - a. Führen Sie die folgende Anweisung aus, um UserA zu erstellen:

```
CREATE USER UserA IDENTIFIED BY sql;
```

- b. Führen Sie die folgende Anweisung aus, um UserB zu erstellen:

```
CREATE USER UserB IDENTIFIED BY sql;
```

## Ergebnisse

Sie haben zwei neue Benutzer erstellt, UserA und UserB.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 2: UserA Privilegien erteilen \(SQL\)](#)“ auf Seite 1380.

## Siehe auch

- „Benutzer erstellen (Sybase Central)“ auf Seite 1341
- „Benutzer erstellen (SQL)“ auf Seite 1342
- „CREATE USER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Lektion 2: UserA Privilegien erteilen (SQL)

Erteilen Sie UserA Systemprivilegien und Privilegien auf Objektebene.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 1: Zwei neue Benutzer erstellen, UserA und UserB \(SQL\)](#)“ auf Seite 1379.

### Aufgabe

1. Führen Sie in Interactive SQL die folgende Anweisung aus, um UserA die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT zu erteilen:

```
GRANT BACKUP DATABASE, VALIDATE ANY OBJECT TO UserA;
```

2. Führen Sie die folgende Anweisung aus, um UserA die Privilegien SELECT und UPDATE auf Objektebene für die Tabelle "Employees" zu erteilen, mit Administrationsrechten:

```
GRANT SELECT, UPDATE ON GROUPO.EMPLOYEES TO UserA WITH GRANT OPTION;
```

3. Dadurch kann UserA Daten in der Tabelle "Employees" auswählen und aktualisieren. UserA kann außerdem anderen Benutzern die Möglichkeit gewähren, Daten in der Tabelle "Employees" auszuwählen und zu aktualisieren.

## Ergebnisse

UserA hat nun die Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT, die erforderlich sind, um die Beispieldatenbank zu sichern. Außerdem hat UserA die Privilegien SELECT und UPDATE auf Objektebene für die Tabelle "Employees" und kann diese Privilegien anderen Benutzern erteilen.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: Rolle erstellen und UserA erteilen \(SQL\)](#)“ auf Seite 1381.

**Siehe auch**

- „Systemprivilegien“ auf Seite 1309
- „Objektprivilegien“ auf Seite 1305
- „Systemprivilegien erteilen (Sybase Central)“ auf Seite 1331
- „Systemprivilegien erteilen (SQL)“ auf Seite 1332
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Lektion 3: Rolle erstellen und UserA erteilen (SQL)

Erstellen Sie eine Rolle mit den Privilegien, die notwendig sind, um das Debugging einer Prozedur durchzuführen und während dieses Prozesses gefundene Fehler zu korrigieren, und erteilen Sie anschließend diese Rolle UserA. Achten Sie darauf, dass UserA Administrationsrechte für die Rolle erteilt werden, damit er die Rolle ggf. anderen Benutzern erteilen oder entziehen kann.

**Voraussetzungen**

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 2: UserA Privilegien erteilen \(SQL\)](#)“ auf Seite 1380.

**Aufgabe**

1. Führen Sie in Interactive SQL die folgende Anweisung aus, um die Rolle zu erstellen:

```
CREATE ROLE DebugAndFix;
```

2. Führen Sie die folgende Anweisung aus, um der Rolle die erforderlichen Systemprivilegien zu erteilen:

```
GRANT ALTER ANY OBJECT, DEBUG ANY PROCEDURE TO DebugAndFix;
```

3. Führen Sie die folgende Anweisung aus, um UserA die neue Rolle mit Administrationsrechten zu erteilen:

```
GRANT ROLE DebugAndFix TO UserA WITH ADMIN OPTION;
```

**Ergebnisse**

Die DebugAndFix-Rolle, die die Systemprivilegien DEBUG ANY PROCEDURE und ALTER ANY OBJECT hat, wurde erstellt und UserA zusammen mit Administrationsrechten erteilt.

**Nächste Schritte**

Gehen Sie weiter zu „[Lektion 4: UserA in eine benutzererweiterte Rolle konvertieren und diese Rolle UserB erteilen \(SQL\)](#)“ auf Seite 1382.

### Siehe auch

- „Benutzerdefinierte Rollen erstellen (Sybase Central)“ auf Seite 1285
- „Rollen und Privilegien für Rollen konfigurieren (Sybase Central)“ auf Seite 1296
- „Rollen erteilen (Sybase Central)“ auf Seite 1298
- „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Lektion 4: UserA in eine benutzererweiterte Rolle konvertieren und diese Rolle UserB erteilen (SQL)

Angenommen, Sie möchten UserB dieselben Privilegien und Rollen erteilen wie UserA. Statt denselben langwierigen Prozess durchzuführen und dieselben Rollen und Privilegien, die Sie UserA erteilt haben, UserB zu erteilen, können Sie UserA in eine benutzererweiterte Rolle konvertieren und diese Rolle anschließend UserB erteilen. UserA bleibt weiterhin ein Benutzer, der sich bei der Datenbank anmelden kann, und fungiert zusätzlich als Rolle.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 3: Rolle erstellen und UserA erteilen \(SQL\)](#)“ auf Seite 1381.

### Aufgabe

1. Konvertieren Sie in Interactive SQL UserA in eine benutzererweiterte Rolle, indem Sie die folgende Anweisung ausführen:

```
CREATE ROLE FOR USER UserA;
```

2. Erteilen Sie UserB die benutzererweiterte Rolle UserA, indem Sie die folgende Anweisung ausführen:

```
GRANT ROLE UserA TO UserB;
```

Dies gibt UserB die Möglichkeit, die Rolle UserA auszuüben. Das bedeutet, dass UserB alle Rollen und Privilegien ausüben kann, die auch UserA ausüben kann.

### Ergebnisse

UserA wurde in eine benutzererweiterte Rolle konvertiert und diese Rolle wurde UserB erteilt.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 5: Rollen und Privilegien für UserB anzeigen \(SQL\)](#)“ auf Seite 1383.

### Siehe auch

- „Benutzererweiterte Rollen“ auf Seite 1287
- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Lektion 5: Rollen und Privilegien für UserB anzeigen (SQL)

Sie können die Rollen, Systemprivilegien und Privilegien auf Objektebene eines Benutzers anzeigen, einschließlich derjenigen, die der Benutzer durch Mitgliedschaft in anderen Rollen erbt.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie alle vorherigen Lektionen in dieser praktischen Einführung abgeschlossen haben. Siehe „[Lektion 4: UserA in eine benutzererweiterte Rolle konvertieren und diese Rolle UserB erteilen \(SQL\)](#)“ auf Seite 1382.

### Aufgabe

1. Führen Sie in Interactive SQL die folgende Anweisung aus, um die Rollen und Privilegien von userB, einschließlich dazugehöriger Administrationsrechte, anzuzeigen:

```
CALL sp_displayroles ( 'UserB', 'expand_down' );
```

role_name	parent_role_name	grant_type	role_level
UserA	(NULL)	NO ADMIN	1
PUBLIC	(NULL)	NO ADMIN	1
dbo	PUBLIC	NO ADMIN	2
PUBLIC	UserA	NO ADMIN	2
DebugAndFix	UserA	ADMIN	2
BACKUP DATABASE	UserA	NO ADMIN	2
VALIDATE ANY OBJECT	UserA	NO ADMIN	2
ALTER ANY OBJECT	DebugAndFix	NO ADMIN	3
DEBUG ANY PROCEDURE	DebugAndFix	NO ADMIN	3
dbo	PUBLIC	NO ADMIN	3

Betrachten Sie den role\_level-Wert als eine Ebene in einer Vererbungshierarchie, wobei UserB Ebene 1 ist:

- Den Zeilen mit role\_level-Wert 1 können Sie entnehmen, dass die Rolle UserA direkt UserB erteilt wurde. Außerdem sehen Sie, dass die PUBLIC-Rolle direkt UserB erteilt wurde. Die PUBLIC-Rolle wird neuen Benutzern automatisch erteilt.
- Den Zeilen mit role\_level-Wert 2 können Sie entnehmen, dass UserB die Rollen dbo und PUBLIC von UserA erbt. UserB erbt außerdem die DebugAndFix-Rolle, die UserA erteilt wurde, einschließlich der Administrationsrechte für die Rolle. Schließlich erbt UserB die

Systemprivilegien BACKUP DATABASE und VALIDATE ANY OBJECT, die UserA erteilt wurden.

- Den Zeilen mit role\_level-Wert 3 können Sie entnehmen, dass UserB die Systemprivilegien ALTER ANY OBJECT und DEBUG ANY PROCEDURE von UserA erbt, der sie wiederum aus der DebugAndFix-Rolle geerbt hat. UserB erbt außerdem dbo nochmals, diesmal aus der PUBLIC-Rolle, die der DebugAndFix-Rolle beim Erstellen automatisch erteilt wurde.

2. Führen Sie die folgende Anweisung aus, um die Privilegien von UserB auf Objektebene anzuzeigen.

```
CALL sp_objectpermission ( 'UserB' );
```

grantor	grantee	object_name	owner	object_type	column_name	permission	grantable
...	...	...	...	...	...	...	...
DBA	UserA	Employees	GROU- PO	TABLE	(NULL)	SELECT	J
DBA	UserA	Employees	GROU- PO	TABLE	(NULL)	UPDATE	J
SYS	PUB- LIC	spt_collati- on_map	dbo	TABLE	(NULL)	SELECT	N
...	...	...	...	...	...	...	...

Die Ergebnismenge ist recht lang, weil die Benutzer vieles durch ihre Mitgliedschaft in der PUBLIC-Rolle erben. Die relevanten Zeilen sind jedoch die zweite und dritte Zeile in der Tabelle, da diese zeigen, dass UserB die Privilegien SELECT und UPDATE für die Tabelle "Employees" erbt. Außerdem sehen Sie hier, dass diese beiden Privilegien vom Benutzer DBA erteilt wurden.

3. Administrationsrechte für Privilegien auf Objektebene können nicht vererbt werden. Deshalb kann UserB nicht die Administrationsrechte für die Privilegien SELECT und UPDATE in der Tabelle "Employees" erben, obwohl DBA UserA das Recht zum Erteilen dieser Privilegien erteilt hat. Das "J" in der grantable-Spalte für diese Zeilen gibt an, dass UserA Administrationsrechte für die Privilegien hat.

## Ergebnisse

Sie haben die Rollen und Privilegien überprüft, die UserB erteilt und vererbt wurden.

## Siehe auch

- [„Vererbung von Rollen und Privilegien“ auf Seite 1348](#)
- [„Systemprivilegien erteilen \(Sybase Central\)“ auf Seite 1331](#)
- [„Rollen erteilen \(Sybase Central\)“ auf Seite 1298](#)
- [„Rollenadministratoren“ auf Seite 1293](#)

## Upgrade auf rollenbasierte Sicherheit

Dieses Kapitel richtet sich an Benutzer der SQL Anywhere-Versionen vor Version 16.0. Es wird erläutert, welche Änderungen bei einem Upgrade der Datenbank auf rollenbasierte Sicherheit vorgenommen werden und was Sie möglicherweise tun müssen, wenn Sie Anwendungen haben, die SQL-Anweisungen wie GRANT oder REVOKE ausführen.

### Was ist aus den Berechtigungen und Gruppen geworden?

In SQL Anywhere 16.0 wird ein rollenbasiertes Sicherheitsmodell eingeführt. Während Sie zuvor Berechtigungen, Berechtigungen auf Objektebene und Gruppen hatten, gibt es nun Rollen, Systemprivilegien, Privilegien auf Objektebene und benutzererweiterte Rollen.

#### Hinweis

Sie können einen SQL Anywhere 16.0-Datenbankserver mit einer Datenbank vor Version 16.0 verwenden. Wenn Sie dies tun, ist volle Abwärtskompatibilität für die betreffende Datenbank gewährleistet und deren Sicherheitsmodell wird nicht geändert.

In Datenbanken vor Version 16.0 gab es **Berechtigungen** auf Datenbankebene. Ein Benutzer mit BACKUP-Berechtigung konnte beispielsweise die Datenbank sichern. In einigen solchen Berechtigungen wurden auch Berechtigungen auf Objektebene gebündelt. Ein Benutzer mit PROFILE-Berechtigung konnte beispielsweise Aufgaben für Anwendungsprofilerstellung und Datenbankprotokollierung ausführen, bei denen Systemprozeduren verwendet werden, die sonst nicht verfügbar sind. Sie konnten weder neue Berechtigungen erstellen noch die darin enthaltenen Berechtigungen ändern oder Berechtigungen löschen. Sie konnten Administrationsrechte (WITH GRANT) erteilen, aber die Erteilung nicht auf die Administrationsrechte beschränken.

Nun treten **Rollen** funktional an die Stelle der Berechtigungen, mit dem zusätzlichen Vorteil, dass Sie neue Rollen erstellen, die in Rollen enthaltenen Privilegien ändern und Rollen löschen können. Der Wechsel zu Rollen und Privilegien bedeutet, dass Sie eine bessere Kontrolle über die Privilegien haben, die Sie einem Benutzer erteilen möchten, und eine einfachere Methode, um sie anderen Benutzern zu erteilen. Außerdem können Sie die Rolle einem Benutzer nur mit Administrationsrechten erteilen, was bedeutet, dass der betreffende Benutzer die Rolle erteilen und entziehen, aber nicht die zugrunde liegenden Privilegien ausüben kann.

In Datenbanken vor Version 16.0 konnten Sie mit **Berechtigungen** Datenbankobjekte wie Tabellen, Ansichten oder Benutzer erstellen, ändern, abfragen, verwenden oder löschen. Sie konnten beispielsweise die SELECT-Berechtigung für eine Tabelle haben.

Nun treten **Privilegien** funktional an die Stelle der Berechtigungen, mit dem zusätzlichen Vorteil, dass es wesentlich mehr Privilegien gibt als Berechtigungen. Für jeden mit Privilegien verbundenen Vorgang, der auf ein Datenbankobjekt angewendet werden kann, gibt es ein erteilbares Privileg. Sie können Benutzern Privilegien einzeln erteilen oder ihnen eine Rolle erteilen. Der Begriff *Berechtigung* ist nicht verschwunden, wird aber etwas anders verwendet. Bisher bedeutete das Wort "Berechtigung" eine erteilbare Funktion. Nun bedeutet das Wort "Berechtigung" das Ergebnis einer Auswertung, ob ein Vorgang ausgeführt werden kann. Sie haben beispielsweise die *Berechtigung* zum Ändern einer Tabelle, wenn Sie der Eigentümer sind oder das ALTER ANY TABLE-Systemprivileg haben.

In Datenbanken vor Version 16.0 waren **Gruppen** Sammlungen von einem oder mehreren Benutzern, deren Berechtigungen durch die Einstellungen auf Gruppenebene bestimmt wurden. Einem Benutzer wurde Gruppenstatus erteilt und anderen Benutzern die Mitgliedschaft in dieser Gruppe.

Das Gruppenkonzept spiegelt sich nun in den **benutzererweiterten Rollen** wider. Wenn ein Benutzer über Privilegien verfügt, die Sie anderen Benutzern erteilen möchten, können Sie den Benutzer zu einer benutzererweiterten Rolle erweitern und diese Rolle anderen Benutzern erteilen. Außerdem können Sie das Gruppenkonzept umsetzen, indem Sie eine **eigenständige Rolle** erstellen, die keiner Benutzer-ID zugeordnet ist, aber die Rollen und Privilegien hat, die Sie Benutzern erteilen möchten.

Während des Upgrades einer Datenbank vor Version 16.0 wird die bestehende Berechtigungs- und Gruppenhierarchie automatisch in eine äquivalente Hierarchie aus Rollen, Privilegien und benutzererweiterten Rollen konvertiert. Für jede Berechtigung auf Datenbankebene vor Version 16.0 gibt es eine äquivalente **Kompatibilitätsrolle**. Diese Rollen sind in der Datenbank einfach zu erkennen, da ihre Namen mit SYS\_AUTH beginnen. Kompatibilitätsrollen enthalten die Systemprivilegien, die Benutzer vor Version 16.0 benötigen, um die dieselben Vorgänge ausführen zu können wie mit den bisherigen Berechtigungen.

### Siehe auch

- „Rollen“ auf Seite 1271
- „Privilegien“ auf Seite 1305
- „Benutzererweiterte Rollen“ auf Seite 1287

## Berechtigungen auf Datenbankebene werden zu Kompatibilitätsrollen

Beim Upgrade einer Datenbank erhalten Benutzer, denen Berechtigungen in Datenbanken vor Version 16.0 erteilt wurden, automatisch eine äquivalente Kompatibilitätsrolle für diese Berechtigung, mit einer Ausnahme: Die REMOTE DBA-Berechtigung wird tatsächlich zur SYS\_RUN\_REPLICATION\_ROLE-Systemrolle. Sie ist in der Tabelle enthalten, um zu zeigen, was aus der REMOTE DBA-Berechtigung geworden ist.

Wenn ein Benutzer Administrationsrechte für die bisherige Berechtigung hatte, erhält er auch Administrationsrechte für die Kompatibilitätsrolle.

Kompatibilitätsrollen können nicht geändert werden. Sie können sie jedoch in eine benutzerdefinierte Rolle migrieren und diese anschließend ändern. Das Migrieren von Kompatibilitätsrollen ist einfach, ebenso eine spätere Wiederherstellung. Beim Migrieren einer Kompatibilitätsrolle in eine benutzerdefinierte Rolle wird allen Benutzern, denen die Kompatibilitätsrolle erteilt war, automatisch die neue benutzerdefinierte Rolle erteilt. Die Kompatibilitätsrolle wird nach dem Migrieren automatisch gelöscht. Sie können Kompatibilitätsrollen jedoch mit der CREATE ROLE-Anweisung wiederherstellen.

Die Abwärtskompatibilität für SQL-Anweisungen ist gewährleistet, sodass Anwendungen, die Berechtigungen auf Datenbankebene erteilen oder entziehen, weiterhin funktionieren. Die alte Syntax wird jedoch nicht mehr empfohlen und Sie sollten in Erwägung ziehen, Ihre Anwendungen auf die neue SQL-Syntax für Rollen umzustellen.

Die folgende Tabelle zeigt die Berechtigungen auf Datenbankebene vor Version 16.0 und die Rollen, zu denen sie bei einem Upgrade der Datenbank werden.

<b>Berechtigung vor Version 16.0</b>	<b>Äquivalente Rolle</b>	<b>Beschreibung</b>
ALL	SYS_AUTH_RESOURCE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, Datenbankobjekte wie Tabellen, Ansichten, gespeicherte Prozeduren und Trigger zu erstellen.
BACKUP	SYS_AUTH_BACKUP_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, mithilfe der BACKUP-Anweisung oder des Dienstprogramms dbbackup Datenbanken und Transaktionslogs mit Archiv- oder Sicherungskopien zu sichern.
DBA	SYS_AUTH_DBA_ROLE-Kompatibilitätsrolle  SYS_AUTH_SA_ROLE-Kompatibilitätsrolle  SYS_AUTH_SSO_ROLE-Kompatibilitätsrolle	<p>Ermöglicht es Benutzern, alle möglichen mit Privilegien verbundenen Vorgänge auszuführen. Benutzer mit SYS_AUTH_DBA_ROLE-Kompatibilitätsrolle können Datenbankobjekte erstellen und das Eigentum an diesen Objekten anderen Benutzer-IDs zuordnen, Tabellenstrukturen ändern, neue Benutzer-IDs erstellen, Benutzern Berechtigungen entziehen, die Datenbank sichern usw.</p> <p>Von den möglichen mit Privilegien verbundenen Vorgängen, die die SYS_AUTH_DBA_ROLE-Kompatibilitätsrolle ausführen kann, ermöglicht es die SYS_AUTH_SA_ROLE-Kompatibilitätsrolle dem Benutzer, alle mit der Datenbankadministration zusammenhängenden Aktivitäten auszuführen, z.B. das Erstellen von Tabellen und das Sichern von Daten.</p> <p>Von den möglichen mit Privilegien verbundenen Vorgängen, die die SYS_AUTH_DBA_ROLE-Kompatibilitätsrolle ausführen kann, ermöglicht es die SYS_AUTH_SSO_ROLE-Kompatibilitätsrolle dem Benutzer, die mit Sicherheit und Zugriff zusammenhängenden Administrationsaktivitäten auszuführen, z.B. das Erstellen von Benutzern und das Erteilen von Privilegien für Objekte.</p>
PROFILE	SYS_AUTH_PROFILE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, Profilerstellungs-, Protokollierungs- und Diagnosevorgänge auszuführen.

Berechtigung vor Version 16.0	Äquivalente Rolle	Beschreibung
READCLIENTFILE	SYS_AUTH_READCLIENTFILE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, Dateien auf dem Clientcomputer zu lesen, z.B. wenn Daten aus einer Datei auf einem Clientcomputer geladen werden.
READFILE	SYS_AUTH_READFILE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, die OPENSTRING-Klausel in einer SELECT-Anweisung zum Lesen einer Datei zu verwenden.
REMOTE DBA	SYS_RUN_REPLICATION_ROLE-Systemrolle	<p>Ermöglicht es einem SQL Remote-Benutzer, Replikationsaktivitäten mit dem Dienstprogramm dbremote auszuführen, bzw. einem MobiLink-Benutzer, Synchronisationsaktivitäten mit dem Dienstprogramm dbmlsync auszuführen. Lässt jedoch keine Administration der Replikation zu.</p> <p>Es gibt auch eine neue Systemrolle, SYS_REPLICATION_ADMIN_ROLE, die Sie Replikationsadministratoren erteilen können. In Datenbanken vor Version 16.0 benötigten Replikationsadministratoren die DBA-Berechtigung, um Administrationaufgaben ausführen zu können. Die SYS_REPLICATION_ADMIN_ROLE-Systemrolle umfasst die Privilegien, die zum Ausführen dieser Administrationaufgaben erforderlich sind.</p>
RESOURCE	SYS_AUTH_RESOURCE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, Datenbankobjekte wie Tabellen, Ansichten, gespeicherte Prozeduren und Trigger zu erstellen.
VALIDATE	SYS_AUTH_VALIDATE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, mithilfe der VALIDATE-Anweisung oder des Dienstprogramms dbvalid Datenbanken, Tabellen, Indizes und Prüfsummen zu validieren.
WRITECLIENTFILE	SYS_AUTH_WRITECLIENTFILE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, in Dateien auf einem Clientcomputer zu schreiben, z.B. wenn die UNLOAD TABLE-Anweisung verwendet wird, um Daten auf einen Clientcomputer zu schreiben.
WRITEFILE	SYS_AUTH_WRITEFILE_ROLE-Kompatibilitätsrolle	Ermöglicht es einem Benutzer, die xp_write_file-Systemprozedur auszuführen.

**Siehe auch**

- „Rollen“ auf Seite 1271
- „Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273
- „CREATE ROLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391
- „Änderungen der REVOKE-Anweisungssyntax“ auf Seite 1396
- „Änderungen des Vererbungsverhaltens für einige Berechtigungen, die zu Rollen geworden sind“ auf Seite 1400

## Berechtigungen werden zu Privilegien

In Datenbanken vor Version 16.0 gab es Berechtigungen auf Objektebene, z.B. ALTER oder SELECT für Tabellen und Ansichten usw. Während Anweisungen, die diese Berechtigungen erteilen oder entziehen, weiterhin funktionieren, werden diese Berechtigungen nun als Privilegien bezeichnet, behalten aber dieselben Namen. Zusätzlich zu Privilegien auf Objektebene gibt es für jeden Vorgang, dessen Ausführung eine Autorisierung erfordert, ein erteilbares Systemprivileg. Beim Upgrade Ihrer Datenbank werden Benutzer, die Berechtigungen hatten, automatisch aktualisiert und erhalten die äquivalenten Privilegien, die sie benötigen, um ihre bisherigen Aufgaben weiterhin ausführen zu können.

**Siehe auch**

- „Privilegien“ auf Seite 1305

## Gruppen werden nun mithilfe von Rollen erzeugt

Während des Upgrades einer Datenbank vor Version 16.0 wird jede einzelne Gruppe in eine Rolle mit demselben Namen konvertiert (entweder in eine benutzererweiterte Rolle oder in eine eigenständige Rolle). Mitgliedern der ursprünglichen Gruppe werden automatisch die neue Rolle und alle ihr zugrunde liegenden Privilegien erteilt. Berechtigungen auf Datenbank- und Objektebene, die der ursprünglichen Gruppe erteilt wurden, werden in die äquivalenten Rollen und Systemprivilegien konvertiert und der benutzererweiterten Rolle erteilt.

Wenn eine Berechtigung vererbbar war, wird die Kompatibilitätsrolle von Berechtigungsempfängern der neuen benutzererweiterten Rolle geerbt. Wenn die Berechtigung nicht vererbbar war, erben die Berechtigungsempfänger der benutzererweiterten Rolle nicht die Kompatibilitätsrolle.

Die SQL-Syntax zum Erstellen und Verwalten von Gruppen wurde geändert, obwohl die bisherige Syntax mit GRANT und REVOKE weiterhin unterstützt wird. Die Zuordnung der nicht mehr empfohlenen Syntax zur neuen Syntax finden Sie unter „Änderungen der REVOKE-Anweisungssyntax“ auf Seite 1396 und „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391.

Die folgende Tabelle zeigt die Systembenutzer und Gruppen sowie die Rollen, in die sie konvertiert werden.

Gruppe vor Version 16.0	Rolle	Beschreibung
dbo	dbo	Diese Rolle ist Eigentümer von vielen gespeicherten Systemprozeduren, Ansichten und Tabellen, die für UltraLite und MobiLink verwendet werden.
DIAGNOSTICS	DIAGNOSTICS	Diese Rolle ist Eigentümer der Diagnosetabellen und -ansichten und kann darin Vorgänge ausführen.
PUBLIC	PUBLIC	Diese Rolle hat die SELECT-Berechtigung für die Systemtabellen. Jeder neuen Benutzer-ID wird automatisch die PUBLIC-Rolle erteilt.
SA_DEBUG	SA_DEBUG	Diese Rolle ermöglicht es Benutzern, den SQL Anywhere-Debugger zu verwenden.
SYS	SYS	Diese Rolle ist Eigentümer der Systemtabellen und -ansichten (Katalog) für die Datenbank und kann darin Vorgänge ausführen.
SYS_SPATIAL_ADMIN_ROLE	SYS_SPATIAL_ADMIN_ROLE	Diese Rolle ermöglicht es Benutzern, räumliche Objekte zu erstellen, zu ändern oder zu löschen.

**Siehe auch**

- „Gruppen“ auf Seite 1346
- „Rollen“ auf Seite 1271

## Änderung des Konzepts eines Superusers (DBA-Berechtigung)

In Datenbanken vor Version 16.0 konnten Sie einen Superuser durch Erteilen der DBA-Berechtigung erstellen. Benutzer mit DBA-Berechtigung konnten jede mit Privilegien verbundene Aufgabe im System ausführen. Beim Upgrade Ihrer Datenbank wird Benutzern, die die DBA-Berechtigung hatten, die SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle erteilt und sie erhalten automatisch Ausübungs- und Administrationsrechte für alle Rollen und Privilegien, die zum Zeitpunkt des Upgrades vorhanden sind.

Außerdem gilt: Wenn Sie eine neue Rolle erstellen und bei der Erstellung keinen Administrator angeben, können Benutzer mit MANAGE ROLES-Systemprivileg (globale Administratoren) die Rolle verwalten.

Wenn Sie jedoch eine neue Rolle erstellen und im Rahmen der Erstellung Administratoren zuordnen, werden die Administrationsrechte auf die Berechtigungsempfänger beschränkt, denen sie gegeben wurden. Deshalb müssen Sie Ihrem Superuser die Administrationsrechte für die neue Rolle ggf. explizit erteilen.

**Siehe auch**

- „Superuser“ auf Seite 1295
- „Rollenadministratoren“ auf Seite 1293

**Änderungen der GRANT-Anweisungssyntax**

Wenn Sie Anwendungen haben, die die GRANT-Anweisungssyntax aus Datenbanken vor Version 16.0 für Berechtigungen und Gruppen verwenden, sollten Sie diese auf die aktualisierte Syntax für Rollen und Privilegien umstellen. Die folgende Tabelle zeigt, wie die Anweisungen geändert werden müssen. Die Verwendung der alten GRANT-Syntax für Berechtigungen und Gruppen wird zwar noch unterstützt, aber nicht mehr empfohlen.

**Vererbungsverhalten für frühere Berechtigungen auf Datenbankebene**

In Datenbanken vor Version 16.0 waren die Berechtigungen DBA, REMOTE DBA, BACKUP und RESOURCE und VALIDATE nicht vererbbar, wenn sie einem als Gruppe fungierenden Benutzer zugeordnet waren. Mitglieder dieser Gruppe konnten nicht die Funktionen der Berechtigung erben.

Beim Upgrade einer Datenbank vor Version 16.0 wird automatisch die äquivalente Rolle erteilt (z.B. SYS\_AUTH\_BACKUP\_ROLE statt der BACKUP-Berechtigung) und die WITH NO SYSTEM PRIVILEGE INHERITANCE-Klausel wird angegeben, um sicherzustellen, dass das Vererbungsverhalten mit früheren Versionen übereinstimmt. Mitglieder der Gruppe erben nicht die Privilegien, die die Rolle bereitstellt.

Ebenso gilt: Wenn Sie weiterhin die nicht mehr empfohlene GRANT-Syntax verwenden, um DBA, REMOTE DBA, BACKUP, RESOURCE und VALIDATE zu erteilen, wird das alte Verhalten der Nichtvererbung beibehalten. Das bedeutet, die äquivalente Rolle wird erteilt und die WITH NO SYSTEM PRIVILEGE INHERITANCE-Klausel wird angegeben. Dies geschieht automatisch.

In Datenbanken vor Version 16.0 konnten Benutzer, denen die Berechtigung DBA oder REMOTE DBA erteilt wurde, diese automatisch anderen erteilen. Die WITH ADMIN OPTION-Klausel in der unten empfohlenen neuen Syntax gewährleistet, dass das Verhalten der Administrationsrechte mit früheren Versionen übereinstimmt.

Nicht mehr empfohlene Syntax	Neue Syntax
<b>GRANT CONNECT TO</b> <i>username</i> [ <b>IDENTIFIED BY</b> ] <i>pwd</i>	Keine Änderung.
<b>GRANT GROUP TO</b> <i>user</i>	<b>CREATE OR REPLACE ROLE</b> <i>groupname</i> <b>FOR USER</b> <i>userid</i>
<b>GRANT MEMBERSHIP IN GROUP</b> <i>groupname</i> [...] <b>TO</b> <i>grantee</i> [...]	<b>GRANT ROLE</b> <i>groupname</i> [...] <b>TO</b> <i>grantee</i> [...]

Nicht mehr empfohlene Syntax	Neue Syntax
<b>GRANT DBA TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_DBA_ROLE TO</b> <i>grantee</i> [...] <b>WITH ADMIN OPTION</b> <b>WITH NO SYSTEM PRIVILEGE INHERITANCE</b>
<b>GRANT REMOTE DBA TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_RUN_REPLICATION_ROLE TO</b> <i>grantee</i> [...] <b>WITH ADMIN OPTION</b> <b>WITH NO SYSTEM PRIVILEGE INHERITANCE</b>
<b>GRANT BACKUP TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_BACKUP_ROLE TO</b> <i>grantee</i> [...] <b>WITH NO SYSTEM PRIVILEGE INHERITANCE</b>
<b>GRANT RESOURCE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_RESOURCE_ROLE TO</b> <i>grantee</i> [...] <b>WITH NO SYSTEM PRIVILEGE INHERITANCE</b>
<b>GRANT VALIDATE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_VALIDATE_ROLE TO</b> <i>grantee</i> [...] <b>WITH NO SYSTEM PRIVILEGE INHERITANCE</b>
<b>GRANT PROFILE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_PROFILE_ROLE TO</b> <i>grantee</i> [...]
<b>GRANT READCLIENTFILE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_READCLIENTFILE_ROLE TO</b> <i>grantee</i> [...]
<b>GRANT READFILE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_READFILE_ROLE TO</b> <i>grantee</i> [...]
<b>GRANT WRITECLIENTFILE TO</b> <i>grantee</i> [...]	<b>GRANT ROLE SYS_AUTH_WRITECLIENTFILE_ROLE TO</b> <i>grantee</i> [...]
<b>GRANT PUBLISH TO</b> <i>grantee</i>	Keine Änderung. Sie können jedoch auch die neue PUBLIC-Option <code>db_publisher</code> setzen:  <b>SET OPTION PUBLIC.db_publisher=grantee</b>
<b>GRANT</b> <i>permission</i> [...] <b>ON</b> <i>[owner.]object-name</i> <b>TO</b> <i>grantee</i> [...]  <i>permission</i> : <b>ALL [ PRIVILEGES ]</b> <b>ALTER</b> <b>DELETE</b> <b>INSERT</b> <b>REFERENCES [ ( column-name, ... ) ]</b> <b>SELECT [ ( column-name, ... ) ]</b> <b>UPDATE [ ( column-name, ... ) ]</b>	Keine Änderung.

Nicht mehr empfohlene Syntax	Neue Syntax
<b>GRANT EXECUTE ON</b> [ <i>owner</i> . ] { <i>proc</i>   <i>user-def-funct</i> } <b>TO</b> <i>grantee</i> [...]	Keine Änderung.
<b>GRANT INTEGRATED LOGIN TO</b> <i>user-profile-name</i> [...] <b>AS USER</b> <i>user</i>	Keine Änderung.
<b>GRANT KERBEROS LOGIN TO</b> <i>userid</i> [...] <b>AS USER</b> <i>user</i>	Keine Änderung.
<b>GRANT CREATE ON</b> <i>dbspacename</i> [...] <b>TO</b> <i>grantee</i> [...]	Keine Änderung.

**Siehe auch**

- „GRANT-Anweisung (Berechtigungen und Gruppen) (nicht mehr empfohlen)“ auf Seite 1393
- Hinweise zum Anzeigen der neuen GRANT-Anweisungssyntax finden Sie unter „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- Hinweise zum Anzeigen der Zuordnung von Berechtigungen auf Datenbankebene zu Kompatibilitätsrollen finden Sie unter „Kompatibilitätsrollen“ auf Seite 1275.
- Hinweise dazu, wie Sie ermitteln können, für welche Rollen Sie Administrationsrechte haben, finden Sie unter „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343 oder „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344.
- Hinweise zur GRANT-Anweisungssyntax in SQL Anywhere 12.0.1 finden Sie unter <http://dcx.sybase.com/index.html#1201/en/dbreference/grant-statement.html>

**GRANT-Anweisung (Berechtigungen und Gruppen) (nicht mehr empfohlen)**

Diese Syntax wird zwar noch unterstützt, aber nicht mehr empfohlen. Verwenden Sie stattdessen die neue GRANT-Syntax zum Erteilen von Rollen und Privilegien.

**Syntax 1 - Berechtigungen erteilen**

```
GRANT authority, ...
TO userid, ...
```

```
authority :
BACKUP
| DBA
| PROFILE
| READCLIENTFILE
| READFILE
| [ RESOURCE | ALL ]
```

| **VALIDATE**  
| **WRITECLIENTFILE**

## Syntax 2 - Einem Benutzer Gruppenstatus oder die Mitgliedschaft in einer Gruppe erteilen

```
GRANT { GROUP | MEMBERSHIP IN GROUP userid, ... }  
TO userid, ...
```

### Parameter

#### *Berechtigung*

##### **Hinweis**

Wenn Sie Berechtigungen auf Datenbankebene mit der alten, nicht mehr empfohlenen GRANT-Syntax erteilen, konvertiert der Datenbankserver die Berechtigung in die äquivalente Kompatibilitätsrolle. Für den Benutzer, dem die äquivalente Kompatibilitätsrolle erteilt wird, gehen keine Funktionen verloren.

- **BACKUP-Berechtigung** Konvertiert in das Erteilen der SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle.
- **DBA-Berechtigung** Konvertiert in das Erteilen der Kompatibilitätsrollen SYS\_AUTH\_DBA\_ROLE, SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE.
- **PROFILE-Berechtigung** Konvertiert in das Erteilen der SYS\_AUTH\_PROFILE\_ROLE-Kompatibilitätsrolle.
- **READ\_CLIENT\_FILE-Privileg** Konvertiert in das Erteilen der SYS\_AUTH\_READCLIENTFILE\_ROLE-Kompatibilitätsrolle.
- **READ FILE-Privileg** Konvertiert in das Erteilen der SYS\_AUTH\_READFILE\_ROLE-Kompatibilitätsrolle.
- **RESOURCE- oder ALL-Berechtigung** Konvertiert in das Erteilen der SYS\_AUTH\_RESOURCE\_ROLE-Kompatibilitätsrolle.
- **VALIDATE-Berechtigung** Konvertiert in das Erteilen der SYS\_AUTH\_VALIDATE\_ROLE-Kompatibilitätsrolle.
- **WRITECLIENTFILE-Berechtigung** Konvertiert in das Erteilen der SYS\_AUTH\_WRITECLIENTFILE\_ROLE-Kompatibilitätsrolle.

**GROUP-Klausel** Durch Erteilen wird nun der Benutzer in eine benutzererweiterte Rolle konvertiert, die anderen erteilt werden kann.

**MEMBERSHIP IN GROUP-Klausel** Durch Erteilen erhält der Berechtigungsempfänger alle Rollen und Privilegien der betreffenden benutzererweiterten Rolle (Gruppe).

### Bemerkungen

Die Syntax zum Erteilen von Berechtigungen auf Datenbankebene wird nicht mehr empfohlen, jedoch aus Gründen der Abwärtskompatibilität unterstützt. Das Erteilen einer Berechtigung führt zum Erteilen der äquivalenten Kompatibilitätsrolle, die ab Version 16.0 bereitgestellt wird. Wenn Sie jedoch Ihre

Kompatibilitätsrollen migriert haben, schlägt das Erteilen einer Berechtigung mit der nicht mehr empfohlenen Syntax fehl. Wenn Sie beispielsweise die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle in eine benutzerdefinierte Rolle migrieren (wobei die Kompatibilitätsrolle nach Abschluss der Migration gelöscht wird) und anschließend GRANT BACKUP TO UserA ausführen, schlägt die Anweisung fehl, weil die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle in der Datenbank nicht mehr vorhanden ist. Sie können dieses Problem lösen, indem Sie die Kompatibilitätsrolle wiederherstellen (CREATE ROLE SYS\_AUTH\_BACKUP\_ROLE) oder Ihre Anwendungen auf die neue Syntax umstellen und die neue, durch die Migration erstellte benutzerdefinierte Rolle referenzieren.

#### **Vererbungsverhalten für frühere Berechtigungen auf Datenbankebene**

In Datenbanken vor Version 16.0 waren die Berechtigungen DBA, REMOTE DBA, BACKUP und RESOURCE und VALIDATE nicht vererbbar, wenn sie einem als Gruppe fungierenden Benutzer zugeordnet waren. Mitglieder dieser Gruppe konnten nicht die Funktionen der Berechtigung erben.

Beim Upgrade einer Datenbank vor Version 16.0 wird automatisch die äquivalente Rolle erteilt (z.B. SYS\_AUTH\_BACKUP\_ROLE statt der BACKUP-Berechtigung) und die WITH NO SYSTEM PRIVILEGE INHERITANCE-Klausel wird angegeben, um sicherzustellen, dass das Vererbungsverhalten mit früheren Versionen übereinstimmt. Mitglieder der Gruppe erben nicht die Privilegien, die die Rolle bereitstellt.

Ebenso gilt: Wenn Sie weiterhin die nicht mehr empfohlene GRANT-Syntax verwenden, um DBA, REMOTE DBA, BACKUP, RESOURCE und VALIDATE zu erteilen, wird das alte Verhalten der Nichtvererbung beibehalten. Das bedeutet, die äquivalente Rolle wird erteilt und die WITH NO SYSTEM PRIVILEGE INHERITANCE-Klausel wird angegeben. Dies geschieht automatisch.

## **Privilegien**

Sie benötigen Administrationsrechte für die zu erteilende äquivalente Rolle. Wenn Sie beispielsweise die Möglichkeit zum Sichern von Datenbanken gewähren und die GRANT BACKUP-Syntax verwenden, müssen Sie Administrationsrechte für die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle haben.

## **Siehe auch**

- „Änderungen der GRANT-Anweisungssyntax“ auf Seite 1391
- Hinweise zum Anzeigen der neuen GRANT-Anweisungssyntax finden Sie unter „GRANT-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- Hinweise zum Anzeigen der Zuordnung von Berechtigungen auf Datenbankebene zu Kompatibilitätsrollen finden Sie unter „Kompatibilitätsrollen“ auf Seite 1275.
- Hinweise dazu, wie Sie ermitteln können, für welche Rollen Sie Administrationsrechte haben, finden Sie unter „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343 oder „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344.
- Hinweise zur GRANT-Anweisungssyntax in SQL Anywhere 12.0.1 finden Sie unter <http://dcx.sybase.com/index.html#1201/en/dbreference/grant-statement.html>.

## Änderungen der REVOKE-Anweisungssyntax

Wenn Sie Anwendungen haben, die die REVOKE-Anweisungssyntax aus Datenbanken vor Version 16.0 für Berechtigungen und Gruppen verwenden, sollten Sie diese auf die aktualisierte Syntax für Rollen und Privilegien umstellen. Die folgende Tabelle zeigt, wie die Anweisungen geändert werden müssen. Die Verwendung der alten REVOKE-Syntax für Berechtigungen und Gruppen wird zwar noch unterstützt, aber nicht mehr empfohlen.

Syntax vor Version 16.0	Neue Syntax
<b>REVOKE CONNECT FROM</b> <i>userid</i>	Keine Änderung.
<b>REVOKE GROUP FROM</b> <i>userid</i>	<b>DROP ROLE</b> <i>rolename</i> <b>FROM USER</b> <i>user</i> <b>WITH REVOKE</b>
<b>REVOKE MEMBERSHIP IN GROUP</b> <i>groupname</i> [...] <b>FROM</b> <i>grantee</i> [...]	<b>REVOKE ROLE</b> <i>groupname</i> [...] <b>FROM</b> <i>grantee</i> [...]
<b>REVOKE</b> <i>authority</i> <b>FROM</b> <i>grantee</i> [...]  <i>authority</i> : <b>DBA</b>   <b>REMOTE DBA</b>   <b>BACKUP</b>   <b>RESOURCE</b>   <b>VALIDATE</b>   <b>PROFILE</b>   <b>READCLIENTFILE</b>   <b>READFILE</b>   <b>WRITECLIENTFILE</b>	<b>REVOKE ROLE</b> <i>rolename</i> [...] <b>FROM</b> <i>userid</i> [...]  <i>role</i> : <b>SYS_AUTH_DBA_ROLE</b>   <b>SYS_RUN_REPLICATION_ROLE</b>   <b>SYS_AUTH_BACKUP_ROLE</b>   <b>SYS_AUTH_RESOURCE_ROLE</b>   <b>SYS_AUTH_VALIDATE_ROLE</b>   <b>SYS_AUTH_PROFILE_ROLE</b>   <b>SYS_AUTH_READCLIENTFILE_ROLE</b>   <b>SYS_AUTH_READFILE_ROLE</b>   <b>SYS_AUTH_WRITECLIENTFILE_ROLE</b>
<b>REVOKE PUBLISH FROM</b> <i>grantee</i>	Keine Änderung. Sie können jedoch auch die neue PUBLIC-Option <i>db_publisher</i> setzen:  <b>SET OPTION PUBLIC.db_publisher=grantee</b>
<b>REVOKE</b> <i>permission</i> [...] <b>ON</b> [ <i>owner.</i> ] <i>object-name</i> <b>FROM</b> <i>grantee</i> [...]  <i>permission</i> : <b>ALL [ PRIVILEGES ]</b>   <b>ALTER</b>   <b>DELETE</b>   <b>INSERT</b>   <b>REFERENCES [ ( column-name, ... ) ]</b>   <b>SELECT [ ( column-name, ... ) ]</b>   <b>UPDATE [ ( column-name, ... ) ]</b>	Keine Änderung außer der Namenskonvention. Berechtigungen auf Objektebene sind nun Privilegien auf Objektebene.
<b>REVOKE EXECUTE ON</b> [ <i>owner.</i> ] { <i>procedure-name</i>   <i>user-defined-function</i> } <b>FROM</b> <i>grantee</i> [...]	Keine Änderung.

Syntax vor Version 16.0	Neue Syntax
<b>REVOKE INTEGRATED LOGIN FROM</b> <i>user-profile-name</i> [...]	Keine Änderung.
<b>REVOKE KERBEROS LOGIN FROM</b> <i>userid</i> [...] <b>AS USER</b> <i>user</i>	Keine Änderung.
<b>REVOKE CREATE ON</b> <i>dbspacename</i> [...] <b>FROM</b> <i>grantee</i> [...]	Keine Änderung.

**Siehe auch**

- „REVOKE-Anweisung (Berechtigungen und Gruppen) (nicht mehr empfohlen)“ auf Seite 1397
- Hinweise zum Anzeigen der neuen REVOKE-Anweisungssyntax finden Sie unter „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- Hinweise zum Anzeigen der Zuordnung von Berechtigungen auf Datenbankebene zu Kompatibilitätsrollen finden Sie unter „Kompatibilitätsrollen“ auf Seite 1275.
- Hinweise dazu, wie Sie ermitteln können, für welche Rollen Sie Administrationsrechte haben, finden Sie unter „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343 oder „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344.
- Hinweise zur REVOKE-Anweisungssyntax in SQL Anywhere 12.0.1 finden Sie unter <http://dcx.sybase.com/index.html#1201/en/dbreference/revoke-statement.html>.

**REVOKE-Anweisung (Berechtigungen und Gruppen) (nicht mehr empfohlen)**

Diese Syntax wird zwar noch unterstützt, aber nicht mehr empfohlen. Verwenden Sie stattdessen die äquivalente GRANT-Syntax. Entzieht die Mitgliedschaft in Gruppen (benutzererweiterten Rollen) und entzieht Berechtigungen (Privilegien) für angegebene Benutzer.

**Hinweis**

Wenn Sie Berechtigungen auf Datenbankebene mit der alten, nicht mehr empfohlenen REVOKE-Syntax entziehen, konvertiert der Datenbankserver die Entziehung in die äquivalente Kompatibilitätsrolle.

**Syntax 1 - Entziehen von Berechtigungen**

**REVOKE** *privilege*, ... **FROM** *userid*, ...

*permission* :

**BACKUP**  
**CONNECT**  
**CREATE ON** *dbspace*  
**DBA**  
**GROUP**  
**INTEGRATED LOGIN**

**KERBEROS LOGIN**  
**MEMBERSHIP IN GROUP** *userid, ...*  
**PROFILE**  
**READCLIENTFILE**  
**READFILE**  
**[ RESOURCE | ALL ]**  
**VALIDATE**  
**WRITECLIENTFILE**

## Parameter

### *Berechtigung*

#### **Hinweis**

Wenn Sie Berechtigungen auf Datenbankebene mit der alten, nicht mehr empfohlenen REVOKE-Syntax entziehen, konvertiert der Datenbankserver die Berechtigung in die äquivalente Kompatibilitätsrolle.

- **BACKUP-Berechtigung** Konvertiert in das Entziehen der SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle.
- **DBA-Berechtigung** Konvertiert in das Entziehen der Kompatibilitätsrollen SYS\_AUTH\_DBA\_ROLE, SYS\_AUTH\_SA\_ROLE und SYS\_AUTH\_SSO\_ROLE.
- **PROFILE-Berechtigung** Konvertiert in das Entziehen der SYS\_AUTH\_PROFILE\_ROLE-Kompatibilitätsrolle.
- **READ\_CLIENT\_FILE-Privileg** Konvertiert in das Entziehen der SYS\_AUTH\_READCLIENTFILE\_ROLE-Kompatibilitätsrolle.
- **READ FILE-Privileg** Konvertiert in das Entziehen der SYS\_AUTH\_READFILE\_ROLE-Kompatibilitätsrolle.
- **RESOURCE- oder ALL-Berechtigung** Konvertiert in das Entziehen der SYS\_AUTH\_RESOURCE\_ROLE-Kompatibilitätsrolle.
- **VALIDATE-Berechtigung** Konvertiert in das Entziehen der SYS\_AUTH\_VALIDATE\_ROLE-Kompatibilitätsrolle.
- **WRITECLIENTFILE-Berechtigung** Konvertiert in das Entziehen der SYS\_AUTH\_WRITECLIENTFILE\_ROLE-Kompatibilitätsrolle.

**GROUP-Klausel** Konvertiert eine benutzererweiterte Rolle (Gruppe) in einen normalen Benutzer zurück, sodass er nicht mehr als Gruppe fungiert, der Benutzer hinzugefügt werden können.

**MEMBERSHIP IN GROUP-Klausel** Entzieht die Mitgliedschaft in einer benutzererweiterten Rolle (Gruppe).

## Bemerkungen

REVOKE GROUP entzieht automatisch allen Gruppenmitgliedern MEMBERSHIP IN GROUP.

Wenn Sie einen Benutzer zu einer Gruppe hinzufügen, erbt der Benutzer alle dieser Gruppe zugeordneten Privilegien. SQL Anywhere lässt nicht zu, dass Sie eine Teilmenge der Privilegien entziehen, die ein

Benutzer als Mitglied einer Gruppe erbt, weil Sie nur Privilegien entziehen können, die explizit mit einer GRANT-Anweisung erteilt wurden. Wenn Sie für verschiedene Benutzer unterschiedliche Privilegien benötigen, erstellen Sie unterschiedliche Gruppen mit den entsprechenden Privilegien oder erteilen Sie jedem Benutzer explizit die erforderlichen Privilegien.

Wenn Sie einem Benutzer ein Privileg entziehen und dieser auch WITH GRANT OPTION für dieses Privileg hatte, wird das Privileg auch allen Benutzern entzogen, denen es von diesem Benutzer erteilt wurde. Nehmen Sie beispielsweise an, Sie haben UserA das SELECT...WITH GRANT OPTION-Privileg für eine Tabelle erteilt und UserA hat anschließend UserB das SELECT-Privileg für die Tabelle erteilt. Wenn Sie UserA das SELECT-Privileg entziehen, wird es auch UserB entzogen.

## Privilegien

Sie benötigen Administrationsrechte für die zu entziehende äquivalente Rolle. Wenn Sie beispielsweise die Möglichkeit zum Sichern von Datenbanken entziehen und die REVOKE BACKUP-Syntax verwenden, müssen Sie Administrationsrechte für die SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle haben.

## Siehe auch

- „Änderungen der REVOKE-Anweisungssyntax“ auf Seite 1396
- Hinweise zum Anzeigen der neuen REVOKE-Anweisungssyntax finden Sie unter „REVOKE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- Hinweise zum Anzeigen der Zuordnung von Berechtigungen auf Datenbankebene zu Kompatibilitätsrollen finden Sie unter „Kompatibilitätsrollen“ auf Seite 1275.
- Hinweise dazu, wie Sie ermitteln können, für welche Rollen Sie Administrationsrechte haben, finden Sie unter „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (Sybase Central)“ auf Seite 1343 oder „Rollen und Privilegien für einen Benutzer oder eine Rolle anzeigen (SQL)“ auf Seite 1344.
- Hinweise zur REVOKE-Anweisungssyntax in SQL Anywhere 12.0.1 finden Sie unter <http://dcx.sybase.com/index.html#1201/en/dbreference/revoke-statement.html>.

## Änderungen von REMOTE DBA

In Datenbanken vor Version 16.0 konnte ein Benutzer mit REMOTE DBA-Berechtigung Replikations- und Synchronisationsvorgänge mit dbremote und dbmlsync ausführen.

Die REMOTE DBA-Berechtigung wurde durch die SYS\_RUN\_REPLICATION\_ROLE-Systemrolle ersetzt. Ändern Sie Ihre Anwendungen so, dass sie statt REMOTE DBA diese Rolle erteilen. Die GRANT REMOTE DBA-Anweisungssyntax wird zwar weiterhin unterstützt, aber nicht mehr empfohlen.

Im Zusammenhang mit der Replikation wurde eine weitere Rolle eingeführt: die SYS\_REPLICATION\_ADMIN\_ROLE-Systemrolle. Diese Rolle ermöglicht es Benutzern, die Replikation zu verwalten.

### Siehe auch

- „GRANT ROLE SYS\_RUN\_REPLICATION\_ROLE-Anweisung [MobiLink] [SQL Remote]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „GRANT ROLE SYS\_REPLICATION\_ADMIN\_ROLE-Anweisung [MobiLink] [SQL Remote]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273

## GRANT REMOTE DBA-Anweisung (nicht mehr empfohlen)

Erteilt die SYS\_RUN\_REPLICATION\_ROLE-Systemrolle, die erforderlich ist, um das Dienstprogramm dbremote für die Replikation und das Dienstprogramm dbmlsync für die Synchronisation ausführen zu können.

### Syntax

```
GRANT REMOTE DBA
TO userid, ...
[ IDENTIFIED BY password ]
```

### Parameter

**IDENTIFIED BY-Klausel** Die IDENTIFIED BY-Klausel ist bei dieser Anweisung optional. Wenn sie verwendet wird, ändert sie das Kennwort des Benutzer.

### Bemerkungen

Durch Ausführen dieser Anweisung wird die SYS\_RUN\_REPLICATION\_ROLE-Systemrolle erteilt. Die REMOTE DBA-Berechtigung wird nicht mehr empfohlen.

### Siehe auch

- „GRANT ROLE SYS\_RUN\_REPLICATION\_ROLE-Anweisung [MobiLink] [SQL Remote]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Systemrollen im Zusammenhang mit der Replikation“ auf Seite 1273

## Änderungen des Vererbungsverhaltens für einige Berechtigungen, die zu Rollen geworden sind

Wenn Sie in Datenbanken vor Version 16.0 die Berechtigungen DBA, REMOTE DBA, BACKUP, RESOURCE und VALIDATE einer Gruppe erteilt haben, wurden die zugrunde liegenden Berechtigungen *nicht* von den Mitgliedern der Gruppe geerbt.

Nun ist jedoch das Standardverhalten beim Erteilen *jeder* Rolle (einschließlich SYS\_AUTH\_DBA\_ROLE, SYS\_RUN\_REPLICATION\_ROLE, SYS\_AUTH\_BACKUP\_ROLE, SYS\_AUTH\_RESOURCE\_ROLE und SYS\_AUTH\_VALIDATE\_ROLE) an eine benutzerdefinierte Rolle, dass diejenigen, denen die benutzerdefinierte Rolle erteilt wird, die diesen Rollen zugrunde liegenden Systemprivilegien erben.

Angenommen, Sie haben einen Benutzer, UserA. Sie erteilen UserA das ALTER ANY OBJECT-Systemprivileg. Danach beschließen Sie, UserA zu einer Rolle zu erweitern, und erteilen diese Rolle

anschließend UserB. Nun möchten Sie UserA die SYS\_AUTH\_DBA\_ROLE-Systemrolle erteilen, möchten aber nicht, dass UserB alle Privilegien erbt, die die SYS\_AUTH\_DBA\_ROLE-Systemrolle gewährt. Deshalb erteilen Sie die SYS\_AUTH\_DBA\_ROLE-Systemrolle folgendermaßen:

```
GRANT ROLE SYS_AUTH_DBA_ROLE TO userA WITH NO SYSTEM PRIVILEGE INHERITANCE;
```

In diesem Szenario erbt UserB nur das ALTER ANY OBJECT-Systemprivileg von UserA.

Um das Nichtvererbungsverhalten dieser Rollen während des Upgrades beizubehalten, verfügt SQL Anywhere über eine WITH NO SYSTEM PRIVILEGE INHERITANCE Klausel in der GRANT ROLE-Anweisung. Wenn Sie Anwendungen haben, die Sie auf die neue GRANT-Syntax umstellen, müssen Sie diese Klausel ebenfalls angeben. Diese Klausel ist nur für die Verwendung mit diesen bestimmten Rollen vorgesehen.

#### Siehe auch

- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Kompatibilitätsrollen erteilen (Sybase Central)“ auf Seite 1280
- „Kompatibilitätsrollen erteilen (SQL)“ auf Seite 1281
- „Kompatibilitätsrollen“ auf Seite 1275

## Änderungen der Administration für Publikationseigentümer von Datenbanken

In Datenbanken vor Version 16.0 wurde der Publikationseigentümer der Datenbank durch Erteilen der PUBLISH-Berechtigung mithilfe der Anweisungen GRANT PUBLISH und REVOKE PUBLISH gesteuert. Der aktuelle Publikationseigentümer konnte durch Abfragen des CURRENT PUBLISHER-Spezialwerts ermittelt werden.

Die PUBLISH-Berechtigung wurde durch die PUBLIC.db\_publisher-Datenbankoption ersetzt, für die das SET ANY SYSTEM OPTION-Systemprivileg festgelegt werden muss. Sie können den Publikationseigentümer durch Ändern der Datenbankoption ändern. Aus Gründen der Abwärtskompatibilität können Sie jedoch weiterhin GRANT PUBLISH und REVOKE PUBLISH verwenden. Außerdem können Sie weiterhin den CURRENT PUBLISHER-Wert abfragen, um den aktuellen Publikationseigentümer zu ermitteln.

#### Siehe auch

- „db\_publisher-Option“ auf Seite 602
- „GRANT PUBLISH-Anweisung [SQL Remote]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „REVOKE PUBLISH-Anweisung [SQL Remote]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Änderungen für Systemprozeduren, die mit Privilegien verbundene Vorgänge ausführen

In Datenbanken vor Version 16.0 wurden Systemprozeduren, die mit Privilegien verbundene Vorgänge ausführen, standardmäßig mit den Privilegien des Eigentümers, in der Regel dbo oder SYS, ausgeführt und die SQL SECURITY-Klausel in den Prozedurdefinitionen war auf DEFINER (den Eigentümer) gesetzt.

In Version 16.0 ist die SQL SECURITY-Klausel für diese Systemprozeduren standardmäßig auf INVOKER gesetzt. Das bedeutet, dass die mit Privilegien verbundenen Vorgänge mit den Privilegien des Aufrufers ausgeführt werden statt mit denjenigen des Definierers.

Nun können Sie beim Erstellen bzw. beim Upgrade einer Datenbank festlegen, ob Systemprozeduren, die mit Privilegien verbundene Vorgänge ausführen, mit den Privilegien des Eigentümers oder des Aufrufers ausgeführt werden. Die CREATE DATABASE-Anweisung, die ALTER DATABASE UPGRADE-Anweisung, das Dienstprogramm Initialisierung (dbinit), und das Dienstprogramm zum Upgrade (dbupgrad) wurden um diese Wahlmöglichkeit erweitert.

Wenn bei einer neuen Datenbank keine Angabe gemacht wurde, wird der Aufrufer für diese Systemprozeduren ausgewählt. Wenn bei einem Upgrade keine Angabe gemacht wurde, wird standardmäßig die bereits vorhandene Einstellung für die betreffende Datenbank übernommen.

### Siehe auch

- „Prozeduren und Funktionen zum Ausführen mit Eigentümer- oder Aufruferprivilegien einrichten“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „ALTER DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Dienstprogramm zum Upgrade (dbupgrad)“ auf Seite 1017

## Datensicherheit

Da Datenbanken geschützte, vertrauliche oder private Daten enthalten können, ist es wichtig, Datenbank und Daten so planen, dass die Sicherheit gewährleistet ist.

SQL Anywhere bietet mehrere Funktionen, die Sie dabei unterstützen, eine sichere Umgebung für Ihre Daten einzurichten:

- **Benutzer-Identifizierung und -Authentifizierung** Mit diesen Elementen wird kontrolliert, wer Zugriff auf die Datenbank hat.
- **Frei bestimmbare Zugriffssteuerung** Diese Funktionen steuern die Aktionen, die ein Benutzer durchführen kann, während er mit der Datenbank verbunden ist.
- **Auditing** Diese Funktion unterstützt Sie dabei, die Aktionen in der Datenbank aufzuzeichnen.
- **Datenbankserveroptionen** Mit diesen Funktionen können Sie steuern, wer Verwaltungsvorgänge durchführen kann (z.B. Datenbanken laden). Diese Optionen werden festgelegt, wenn Sie den Datenbankserver starten. Siehe „[Privilegien über die Befehlszeile steuern](#)“ auf Seite 170.
- **Ansichten und gespeicherte Prozeduren** Mit diesen Funktionen können Sie die Daten festlegen, auf die ein Benutzer Zugriff hat, und definieren, welche Vorgänge von einem Benutzer ausgelöst werden dürfen.
- **Datenbank- und Tabellenverschlüsselung** Sie können Ihre Datenbank entweder mit einfacher Verschlüsselung oder mit starker Verschlüsselung chiffrieren. Einfache Verschlüsselung entspricht

der Verschleierung. Bei starker Verschlüsselung wird ohne den Chiffrierschlüssel der Zugriff auf die Datenbank vollständig verwehrt.

Tabellenverschlüsselungsfunktionen ermöglichen es Ihnen, statt der gesamten Datenbank einzelne Tabellen zu verschlüsseln.

- **Transportschichtssicherheit** Sie können die Transportschichtssicherheit verwenden, um die Kommunikation zwischen Clientanwendungen und dem Datenbankserver zu authentifizieren. Die Transportschichtssicherheit nutzt RSA-Verschlüsselungstechnologie.

#### Hinweis

Wenn Sie Bedenken haben, dass andere Prozesse auf dem Computer, der den Datenbankserver ausführt, auf den Inhalt Ihrer Client/Server-Kommunikation zugreifen können, wird empfohlen, dass Sie Verschlüsselung verwenden.

#### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

- **Gesicherte Funktionen** Sie können Funktionen bei allen Datenbanken deaktivieren, die auf einem Datenbankserver laufen.
- **Unterstützung für SELinux** SELinux-Richtlinien steuern den Zugriff einer Anwendung auf Systemressourcen. SQL Anywhere verfügt über eine Richtlinie, die die Anwendung unter Red Hat Enterprise Linux 5 sichert.

Weitere Informationen zum Kompilieren und Installieren der SQL Anywhere SELinux-Richtlinie finden Sie in `$SQLANY16/selinux/readme`.

#### Siehe auch

- „Benutzer“ auf Seite 1340
- „Audits von Datenbankaktivitäten“ auf Seite 1416
- „Sicherheit: Mit Ansichten und Prozeduren die Daten einschränken, auf die Benutzer Zugriff haben“ auf Seite 1403
- „Datenbankverschlüsselung und -entschlüsselung“ auf Seite 1424
- „Tabellenverschlüsselung“ auf Seite 1437
- „Transportschichtssicherheit“ auf Seite 1444

## Sicherheit: Mit Ansichten und Prozeduren die Daten einschränken, auf die Benutzer Zugriff haben

Bei Datenbanken, die eine hohe Sicherheitsstufe erfordern, unterliegt das Erteilen eines direkten Zugriffs auf Tabellen gewissen Einschränkungen. Jedes Privileg, das einem Benutzer für eine Tabelle erteilt wird,

betrifft die ganze Tabelle. Es gibt viele Fälle, in denen Privilegien von Benutzern genauer als nur tabellenweise festgelegt werden müssen. Zum Beispiel:

- Es ist nicht wünschenswert, Benutzern, die auf Teile der Tabelle zugreifen müssen, den Zugriff auf personenbezogene oder vertrauliche Daten in einer Mitarbeitertabelle zu gestatten.
- Sie können Handelsvertretern Privilegien zum Aktualisieren einer Tabelle erteilen, die Beschreibungen ihrer Verkaufsgespräche enthält, jedoch diese Privilegien auf die eigenen Gespräche beschränken.

Während Ansichten den Zugriff auf die Daten einschränken, schränken Prozeduren die Aktionen ein, die ein Benutzer ausführen kann. Ein Benutzer kann das EXECUTE-Privileg für eine Prozedur haben, ohne Privilegien für die Tabelle bzw. Tabellen zu haben, in denen die Prozedur ausgeführt wird.

Bei strenger Sicherheitsstufe können Sie jeglichen Zugriff auf die Basistabellen deaktivieren und Benutzern oder Gruppen Privilegien erteilen, bestimmte gespeicherte Prozeduren auszuführen. Bei diesem Ansatz wird genau definiert, wie Daten in der Datenbank geändert werden können.

### Beispiele

Der Sales Manager muss in der Datenbank Zugriff auf die Daten der Mitarbeiter seiner Abteilung haben. Jedoch gibt es keinen Grund, warum er Zugriff auf die Daten von Mitarbeitern in anderen Abteilungen haben sollte.

In diesem Beispiel wird beschrieben, wie eine Benutzer-ID für den Sales Manager erstellt wird, wie Ansichten mit den benötigten Daten erstellt werden und wie der Benutzer-ID des Sales Managers die geeigneten Privilegien erteilt werden.

1. Stellen Sie eine Verbindung her und erstellen Sie die neue Benutzer-ID mit der GRANT-Anweisung:

```
CONNECT DBA IDENTIFIED by sql;  
CREATE USER SalesManager  
IDENTIFIED BY sales;
```

2. Richten Sie folgendermaßen eine Ansicht ein, mit der nur Mitarbeiter des Verkaufs angezeigt werden:

```
CREATE VIEW EmployeeSales AS  
SELECT EmployeeID, GivenName, Surname  
FROM Employees  
WHERE DepartmentID = 200;
```

Der Bezug auf die Tabelle sollte mit dem Eigentümer qualifiziert sein, um eine mehrdeutige Referenzierung von Tabellen mit identischem Namen zu vermeiden.

3. Erteilen Sie SalesManager das Privileg, die Ansicht anzuzeigen:

```
GRANT SELECT ON EmployeeSales TO SalesManager;
```

Verwenden Sie genau dieselbe Anweisung zum Erteilen von Privilegien für Ansichten und für Tabellen.

Im nächsten Beispiel wird eine Ansicht erstellt, mit der der Sales Manager eine Zusammenfassung der Aufträge einsehen kann. Diese Ansicht benötigt Daten aus mehr als einer Tabelle:

1. Erstellen Sie die Ansicht.

```
CREATE VIEW OrderSummary AS
  SELECT OrderDate, Region, SalesRepresentative, CompanyName
  FROM SalesOrders
  KEY JOIN Customers;
```

2. Erteilen Sie dem Sales Manager das Privileg, diese Ansicht anzuzeigen.

```
GRANT SELECT
ON OrderSummary
TO SalesManager;
```

3. Um zu überprüfen, ob der Vorgang ordnungsgemäß funktioniert hat, stellen Sie eine Verbindung mit der Benutzer-ID "SalesManager" her und sehen Sie sich die Ansichten an, die Sie erstellt haben:

```
CONNECT SalesManager
IDENTIFIED BY sales;
SELECT *
FROM DBA.EmployeeSales;
SELECT *
FROM DBA.OrderSummary;
```

Dem Sales Manager wurden keine Privilegien zum Anzeigen der Basistabellen erteilt. Die folgenden Anweisungen führen zu Privilegfehlern.

```
SELECT * FROM GROUP0.Employees;
SELECT * FROM GROUP0.SalesOrders;
```

## Sicherheit: Prozeduren und Trigger

Prozeduren und Trigger bieten Sicherheit, da sie den Benutzern begrenzten Zugriff auf Daten in Tabellen gewähren, auf die sie sonst keinen direkten Zugriff zum Lesen oder Verändern hätten.

Trigger werden beispielsweise mit den Tabellenprivilegien des Eigentümers der zugeordneten Tabelle ausgeführt, können aber von allen Benutzern ausgelöst werden, die Privilegien haben, um Zeilen in der Tabelle einzufügen, zu aktualisieren oder zu löschen. Ebenso werden Prozeduren (einschließlich benutzerdefinierter Funktionen) mit den Privilegien des Prozedureigentümers ausgeführt, können aber von allen Benutzern mit den entsprechenden Privilegien aufgerufen werden. Das bedeutet, dass Prozeduren oder Trigger andere Privilegien haben können (und in der Regel auch haben) als der Benutzer, der sie aufruft.

### Prozeduren

In Hochsicherheitssystemen sollten Sie erwägen, den Zugriff für alle Basistabellen zu verbieten und stattdessen den Zugriff auf Daten und Aufgaben durch Prozeduren zu ermöglichen. Zugriff mithilfe von Prozeduren einschränken

1. Erstellen Sie eine Rolle für jede Gruppe von autorisierten Aufgaben, die ausgeführt werden müssen, und erteilen Sie der Rolle die betreffenden Systemprivilegien.
2. Erteilen Sie alle diese Rollen einer einzelnen gemeinsamen Rolle.
3. Erteilen Sie der betreffenden Rolle EXECUTE-Privilegien für die Prozedur, die die autorisierten Aufgaben ausführt.

4. Wenn ein neuer Benutzer erstellt wird, erteilen Sie diesem nur die Rollen, die für die von ihm auszuführenden Aufgaben erforderlich sind.

#### Siehe auch

- „sp\_proc\_priv-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE PROCEDURE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Dienstprogramm zum Upgrade (dbupgrad)“ auf Seite 1017

## Allgemeine Sicherheitstipps

Sie können viele Maßnahmen ergreifen, um die Sicherheit Ihrer Daten zu verbessern.

- **Wählen Sie Kennwörter mit Umsicht** Führen Sie kein Deployment von Datenbanken durch, die die Standard-Benutzer-ID und das Standard-Kennwort verwenden. Siehe „[Hinweise zur Sicherheit: Kennwörter](#)“ auf Seite 1410.
- **Setzen Sie Superuser sparsam ein** Vermeiden Sie Erstellen und Erteilen von Rollen, die alle Privilegien, Rollen und Administrationsrechte besitzen (d.h., vermeiden Sie Superuser). Erstellen Sie stattdessen Rollen mit logischen Gruppierungen von Privilegien und Rechten und erteilen Sie diese Rollen umsichtig. Wenn Sie Superuser erstellen, verwenden Sie sie nur, wenn es absolut notwendig ist, und speichern Sie ihre Kennwörter an einem sicheren Ort, z.B. in einem Datensafe, um sie bei Bedarf abrufen zu können. Siehe „[Superuser](#)“ auf Seite 1295.

Erwägen Sie, Ihren Datenbankadministratoren zwei Benutzer-IDs zuzuweisen: eine mit allen Privilegien und eine mit eingeschränkten Privilegien. Dann haben die Administratoren die Möglichkeit, sich nur dann mit allen Privilegien anzumelden, wenn dies notwendig ist.

- **Gesicherte Datenbankfunktionen verwenden** Mit der Datenbankserveroption -sf können Sie Funktionen bei allen auf einem Datenbankserver laufenden Datenbanken aktivieren und deaktivieren. Die Funktionen, die Sie deaktivieren können, sind die Verwendung von externen gespeicherten Prozeduren, von Java und des Ferndatenzugriffs sowie die Fähigkeit, die Einstellungen des Anforderungsprotokolls zu ändern. Siehe „[Datenbankserveroption -sf](#)“ auf Seite 280 und „[Schlüssel für gesicherte Funktionen erstellen](#)“ auf Seite 1415.
- **Externe Systemfunktionen löschen** Die folgenden externen Funktionen sind ein mögliches Sicherheitsrisiko:
  - „xp\_cmdshell-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]  
Mit der Prozedur xp\_cmdshell können Benutzer Betriebssystembefehle oder Programme ausführen.
  - „xp\_startmail-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)],
  - „xp\_startsmtp-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

- „xp\_sendmail-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „xp\_stopmail-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „xp\_stopsmtplib-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

Mit den E-Mail-Systemprozeduren können Benutzer selbst erstellte E-Mails über den Datenbankserver senden. Böswillige Benutzer könnten entweder E-Mail- oder Shell-Prozeduren verwenden, um Betriebssystemaufgaben mit anderen Berechtigungen als denjenigen auszuführen, die ihnen das Betriebssystem zugewiesen hat. In einer Betriebsumgebung, in der die Datensicherheit gewahrt bleiben soll, sollten diese Funktionen nicht verfügbar gemacht werden.

Hinweise zum Löschen von Prozeduren finden Sie unter „[DROP PROCEDURE-Anweisung](#)“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)].

- **Schützen Sie Ihre Datenbankdateien** Schützen Sie Datenbankdatei, Logdateien und DBSpace-Dateien vor nicht autorisiertem Zugriff. Speichern Sie sie nicht in einem gemeinsam genutzten Verzeichnis oder auf einem gemeinsam genutzten Volume.
- **Schützen Sie Ihre Datenbank-Software** Schützen Sie Ihre SQL Anywhere-Software vor nicht autorisiertem Zugriff. Geben Sie den Benutzern nur Zugriff auf die Anwendungen, DLLs und Ressourcen, die sie benötigen.
- **Datenbankserver als Dienst oder Daemon ausführen** Sie können verhindern, dass nicht autorisierte Benutzer die Datenbank- oder Logdateien herunterfahren oder sich Zugriff darauf verschaffen, indem Sie den Datenbankserver als Windows-Dienst ausführen. Unter Unix dient das Ausführen des Servers als Daemon ähnlichen Zwecken. Siehe „[Datenbankserver als Dienst oder Daemon ausführen](#)“ auf Seite 180.
- **Setzen Sie die SATMP-Umgebungsvariable auf ein eindeutiges Verzeichnis (Unix)** Um den Datenbankserver auf Unix-Plattformen zu sichern, setzen Sie SATMP auf ein eindeutiges Verzeichnis und versehen Sie dieses Verzeichnis mit Lese-, Schreib- und Ausführungsschutz gegen alle anderen Benutzer. Damit werden alle anderen Verbindungen gezwungen, TCP/IP zu benutzen, wodurch eine bessere Sicherheit gewährleistet ist als bei einer Shared Memory-Verbindung.

Die Puffer des Shared Memorys, die zwischen dem Client und dem Server verwendet werden, werden aus dem Verzeichnisbaum entfernt, bevor tatsächliche Daten zwischen den beiden Seiten ausgetauscht werden. Das bedeutet, dass kein anderer Prozess die Kommunikationsdaten einsehen kann, weil der Shared Memory-Puffer bzw. die Shared Memory-Datei verborgen ist. Daher erhält kein Prozess einen Handle für die Daten. Siehe „[SATMP-Umgebungsvariable](#)“ auf Seite 475.

- **Datenbank stark verschlüsseln** Wenn Sie Ihre Datenbank stark verschlüsseln, kann nur mit dem Schlüssel darauf zugegriffen werden. Mit anderen Mitteln können Sie weder die Datenbank öffnen noch Datenbank- oder Transaktionslogdateien anzeigen. Siehe „[Datenbankserveroption -ep](#)“ auf Seite 233 und „[Datenbankoption -ek](#)“ auf Seite 326.
- **Passen Sie den HTTP-Code der Serveroption -xs und die MaxRequestSize-Protokolloption an** Passen Sie den HTTP-Code der Serveroption -xs an { TO, KTO und MaxRequestSize-Protokolloption }. Siehe „[Datenbankserveroption -xs](#)“ auf Seite 310.

- **Setzen Sie request\_timeout, um zu gewährleisten, dass keine einzelne Anforderung Serverressourcen unbegrenzt verbrauchen kann** Setzen Sie die request\_timeout-Datenbankoption, um zu gewährleisten, dass keine einzelne Anforderung Serverressourcen unbegrenzt verbrauchen kann. Siehe „request\_timeout-Option“ auf Seite 664.
- **Sichern Sie die Sandboxing-Funktion** Wenn Sandboxing aktiviert ist, werden die Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse. Siehe:
  - „Sandboxing“ auf Seite 1411
  - „Datenbankserveroption -sbx “ auf Seite 279
  - „Datenbankoption -sbx “ auf Seite 330
  - „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- **Datenbanken starten und stoppen** Wenn ein Personal Datenbankserver (dbeng16) verwendet wird, kann standardmäßig jeder Benutzer eine zusätzliche Datenbank auf einem laufenden Server starten.

Auf Netzwerk-Datenbankservern (dbsrv16) ist standardmäßig das SERVER OPERATOR-Systemprivileg erforderlich, um eine Datenbank auf einem laufenden Datenbankserver starten zu können. Mit der Datenbankoption -gd können Sie den Zugriff auf diese Option auf Benutzer beschränken, die bestimmte Privilegien in der Datenbank haben, mit der sie bereits verbunden sind.

- **Datenbanken erstellen und löschen** Wenn ein Personal Datenbankserver (dbeng16) ausgeführt wird, kann standardmäßig jeder Benutzer die CREATE DATABASE-Anweisung verwenden, um eine Datenbankdatei zu erstellen.

Auf Netzwerk-Datenbankservern (dbsrv16) ist zum Erstellen von Datenbanken standardmäßig das SERVER OPERATOR-Systemprivileg erforderlich. Mit der Option -gu können Sie den Zugriff auf diese Option auf Benutzer beschränken, die bestimmte Privilegien in der Datenbank haben, mit der sie bereits verbunden sind.

- **Server stoppen** Das Dienstprogramm dbstop stoppt einen Datenbankserver. Dies ist in Batchdateien nützlich oder in anderen Fällen, in denen das interaktive Stoppen des Servers (über die Schaltfläche **Herunterfahren** im Meldungsfenster des Datenbankservers) nicht praktikabel erscheint.

Auf Personal Datenbankservern (dbeng16) kann standardmäßig jeder Benutzer dbstop ausführen, um einen Server herunterzufahren.

Auf Netzwerk-Datenbankservern (dbsrv16) ist zum Stoppen eines Datenbankservers laut Standardeinstellung das SERVER OPERATOR-Systemprivileg erforderlich. Mit der Option -gk können Sie den Zugriff auf diese Option auf Benutzer beschränken, die bestimmte Privilegien in der Datenbank haben.

- **Daten laden und entladen** Die Anweisungen LOAD TABLE, UNLOAD TABLE und UNLOAD greifen alle auf das Dateisystem auf dem Datenbankserver-Computer zu. Mithilfe der Datenbankserveroption -gl können Sie steuern, welche Datenbankprivilegien zum Laden und Entladen von Daten erforderlich sind. Die Standardeinstellung ist **all** für Personal Datenbankserver (dbeng16) unter Nicht-Unix-Betriebssystemen. Die Standardeinstellung DBA gilt für den Netzwerk-Datenbankserver und für den Personal Server unter Unix. Wenn Sie den Personal Datenbankserver

ausführen, haben Sie bereits Zugriff auf das Dateisystem und dies stellt kein Sicherheitsproblem dar. Wenn Sie den Netzwerk-Datenbankserver ausführen, kann ein unbefugter Zugriff auf das Dateisystem ein Sicherheitsproblem darstellen.

- **Transportschichtsicherheit zum Verschlüsseln der Client/Server-Kommunikation einsetzen** Um Netzwerkpakete besser zu schützen, können Sie die Transportschichtsicherheit einsetzen, um die Kommunikation zwischen Clientanwendungen und dem Datenbankserver zu authentifizieren. Die Transportschichtsicherheit nutzt RSA-Verschlüsselungstechnologie.
- **Datenbankfunktionen deaktivieren** Die Datenbankserveroption -sf gibt eine Liste von Funktionen an, die für auf dem Datenbankserver laufende Datenbanken deaktiviert sind und deshalb für Clientanwendungen oder gespeicherte Prozeduren, Trigger oder innerhalb der Datenbank definierte Ereignisse nicht zur Verfügung stehen. Das kann nützlich sein, wenn Sie eine Datenbank starten, die nicht Ihnen gehört und möglicherweise unerwünschte Aktionen enthält, z.B. Viren oder Trojaner.

## Hinweise zur Sicherheit: Benutzer-IDs

Durch die Zuweisung von Benutzer-IDs und Kennwörtern steuert der Datenbankadministrator den Zugriff der Benutzer auf eine Datenbank. Indem er jeder Benutzer-ID Privilegien erteilt, steuert der Datenbankadministrator, welche Aufgaben die einzelnen Benutzer ausführen können, wenn sie mit der Datenbank verbunden sind.

### Das Privilegienschema basiert auf Benutzer-IDs

Wenn sich ein Benutzer bei einer Datenbank anmeldet, kann er auf alle Objekte der Datenbank zugreifen, für die eines der folgenden Kriterien zutrifft:

- Objekte, die der Benutzer erstellt hat
- Objekte, für die der Benutzer explizit Privilegien erhalten hat
- Objekte, für die eine Gruppe, der der Benutzer angehört, explizit Privilegien erhalten hat

Der Benutzer kann nicht auf Datenbankobjekte zugreifen, die diesen Kriterien nicht entsprechen. Benutzer können also nur auf die Objekte zugreifen, deren Eigentümer sie sind oder für die sie explizit Zugriffsprivilegien erhalten haben.

### Rollen und Privilegien

Durch Erteilen von Rollen und Privilegien können Sie steuern, welche Aufgaben Benutzer an Datenbankobjekten ausführen können (z.B. Erstellen, Ändern, Ausführen, Aktualisieren usw.) und welche Administrationsaufgaben (z.B. Sichern, Profilerstellung usw.) ein Benutzer ausführen kann.

Zum Erteilen von Rollen und Privilegien verwenden Sie die GRANT-Anweisung.

Die REVOKE-Anweisung ist das Gegenteil der GRANT-Anweisung: Alle Berechtigungen, die mit GRANT explizit erteilt wurden, können mit REVOKE wieder entzogen werden. Wenn einem Benutzer CONNECT entzogen wird, entfernt dies den Benutzer mit allen Objekten, die ihm gehören, aus der Datenbank.

## Integrierte Logins

Mit integrierten Logins kann ein Benutzer seine Login-Kennung und sein Login-Kennwort verwenden, um sich in Windows und in einer Datenbank anzumelden. Ein externer Login-Name ist mit einer Benutzer-ID in der Datenbank verknüpft. Wenn Sie versuchen, ein integriertes Login durchzuführen, melden Sie sich beim Betriebssystem an, indem Sie einen Login-Namen und ein Kennwort angeben. Das Betriebssystem teilt dem Server dann mit, wer Sie sind, und der Server meldet Sie mit der zugeordneten Datenbankbenutzer-ID an. Es ist kein weiterer Login-Name bzw. kein weiteres Kennwort erforderlich.

Wenn Sie integrierte Logins verwenden und das Benutzerprofil "Guest" aktiviert bleibt, kann dies zu unbeschränktem Zugriff auf eine Datenbank führen, die auf dem Server läuft, der integrierte Logins akzeptiert. Jeder beliebige Benutzer kann sich mit einer beliebigen Benutzer-ID und einem Kennwort beim Server anmelden, weil er standardmäßig mit dem Benutzerprofil "Guest" angemeldet wird.

## Siehe auch

- „CONNECT-Anweisung [ESQL] [Interactive SQL]“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „GRANT-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „REVOKE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Sicherheitsprobleme: Unbeschränkter Datenbankzugriff“ auf Seite 62
- „Integrierte Windows-Logins“ auf Seite 52
- „login\_mode-Option“ auf Seite 623

## Hinweise zur Sicherheit: Kennwörter

Kennwörter sind ein wichtiger Bestandteil des Systems zur Aufrechterhaltung der Datenbanksicherheit. Kennwörter sind nur dann sicher, wenn sie nur schwer zu erraten sind und nicht auf der Festplatte des Benutzers im Klartext gelesen werden können. SQL Anywhere-Kennwörter berücksichtigen immer die Groß- und Kleinschreibung. Sie können eine Funktion zur Kennwortauthentifizierung mit der Option `verify_password_function` angeben.

## Eine Login-Richtlinie implementieren

Verwenden Sie eine Login-Richtlinie, um die Häufigkeit der Kennwortänderungen zu steuern und um die Anzahl der zulässigen Login-Versuche anzugeben, nach denen ein Konto gesperrt wird.

## Standardwert für Benutzer-ID und Kennwort ändern

Die Standardbenutzer-ID und das Standard-Kennwort bei einer neu erstellten Datenbank sind **DBA** bzw. **sql**. Dieses Kennwort muss geändert werden, bevor Sie ein Deployment der Datenbank zur allgemeinen Verfügung vornehmen.

## Mindestlängen für Kennwörter implementieren

Standardmäßig müssen Kennwörter 3 Byte lang sein. Um die Sicherheit zu erhöhen, können Sie die erforderliche Mindestlänge für alle neuen Kennwörter ändern, um kurze (und daher leicht zu erratende) Kennwörter auszuschließen. Sie erreichen dies, indem Sie die Datenbankoption `min_password_length` auf einen Wert größer als Null setzen. Die folgende Anweisung erzwingt Kennwörter von mindestens 8 Stellen.

```
SET OPTION PUBLIC.min_password_length = 8;
```

Siehe [min\\_password\\_length-Verbindungseigenschaft](#) auf Seite 726.

### **Kennwortablauf implementieren**

Standardmäßig laufen Kennwörter niemals ab. Sie können eine Login-Richtlinie verwenden, um den Kennwortablauf zu implementieren.

### **Keine Kennwörter in ODBC-Datenquellen einschließen**

Kennwörter sind der Schlüssel für den Datenbankzugriff. In einer auf Sicherheit bedachten Systemumgebung sollten sie nicht ohne Autorisierung zugänglich sein.

Wenn Sie eine ODBC-Datenquelle oder ein Sybase Central-Verbindungsprofil erstellen, können Sie optional ein Kennwort einbeziehen. Vermeiden Sie es, Kennwörter einzubeziehen, um zu gewährleisten, dass sie von nicht autorisierten Benutzern nicht angezeigt werden können.

### **Verschlüsselung von Konfigurationsdateien, die Kennwörter enthalten**

Wenn Sie eine Konfigurationsdatei erstellen, können Sie optional Kennwortinformationen aufnehmen. Um Ihre Kennwörter zu schützen, können Sie eine einfache Verschlüsselung der Inhalte der Konfigurationsdateien mit dem Dienstprogramm zum Verschleiern von Dateien [dbfhide] in Betracht ziehen.

### **Kennwortüberprüfung verwenden**

Sie können die Option `verify_password_function` verwenden, um eine Funktion anzugeben, die Kennwortregeln implementiert.

### **Siehe auch**

- „`verify_password_function`-Option“ auf Seite 704
- „Login-Richtlinien“ auf Seite 535
- „CREATE LOGIN POLICY-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`min_password_length`-Option“ auf Seite 637
- „ODBC-Datenquellen“ auf Seite 38
- „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922

## **Sandboxing**

Durch Aktivieren der Sandboxing-Einstellungen werden die Dateivorgänge der Datenbank mit Lese- und Schreibzugriff auf das Verzeichnis beschränkt, in dem sich die Hauptdatenbankdatei befindet, einschließlich der dazugehörigen Unterverzeichnisse. Diese Einschränkungen ermöglichen Benutzern das Ausführen von Dateivorgängen und verhindern gleichzeitig einen Zugriff auf Dateien, auf die Benutzer keinen Zugriff haben dürfen. Alle Datenbankbenutzer haben denselben Sandbox-Speicherort.

Wenn Sandboxing aktiviert ist, werden relative Pfadnamen als relativ zu dem Verzeichnis behandelt, in dem sich die Hauptdatenbankdatei (der System-DBSpace) befindet. Wenn Sandboxing nicht aktiviert ist, werden relative Pfadnamen als relativ zum Arbeitsverzeichnis des Datenbankservers angenommen.

Die sicherste Sandboxing-Einstellung hat immer Vorrang. Wenn eine Datenbank mit aktiviertem Sandboxing gestartet wird (angegeben durch eine der Serveroptionen mit -sbx, die START DATABASE-Anweisung oder die auf "On" gesetzte disk\_sandbox-Datenbankoption), läuft die Datenbank in einer Sandbox, unabhängig von anderen Einstellungen, die die Sandboxing-Funktion deaktivieren. Es gibt folgende Möglichkeiten, das Sandboxing zu aktivieren und zu deaktivieren:

Einstellung	Bereich	Beständigkeit	Hinweise
Datenbankserveroption -sbx	Alle auf dem Datenbankserver laufenden Datenbanken	Nur aktuelle Sitzung	<ul style="list-style-type: none"> <li>Durch die Einstellung der gesicherten Funktionen gesteuert</li> <li>Beim Starten eines Datenbankservers angegeben</li> </ul>
DiskSandbox-Option für die sa_server_option-Systemprozedur	Alle auf dem Datenbankserver laufenden Datenbanken	Nur aktuelle Sitzung	<ul style="list-style-type: none"> <li>Durch die Einstellung der gesicherten Funktionen gesteuert</li> <li>Nach dem Starten eines Datenbankservers angegeben</li> </ul>
Datenbankoption -sbx	Eine einzelne Datenbank, die auf dem Datenbankserver läuft	Nur aktuelle Sitzung	<ul style="list-style-type: none"> <li>Durch die Einstellung der gesicherten Funktionen gesteuert</li> <li>Beim Starten eines Datenbankservers angegeben</li> </ul>
sa_db_option-Systemprozedur	Eine einzelne Datenbank, die auf dem Datenbankserver läuft	Nur aktuelle Sitzung	<ul style="list-style-type: none"> <li>Durch die Einstellung der gesicherten Funktionen gesteuert</li> <li>Nach dem Starten eines Datenbankservers angegeben</li> </ul>
DISKSANDBOX-Klausel der START DATABASE-Anweisung	Eine einzelne Datenbank, die auf dem Datenbankserver läuft	Nur aktuelle Sitzung	<ul style="list-style-type: none"> <li>Durch die Einstellung der gesicherten Funktionen gesteuert</li> <li>Nach dem Starten eines Datenbankservers angegeben</li> </ul>
disk_sandbox-Datenbankoption	Die aktuelle Datenbank	Einstellung bleibt über Sitzungen hinweg bestehen	<ul style="list-style-type: none"> <li>Sie müssen das erforderliche Systemprivileg haben</li> <li>Für die Datenbank angegeben</li> </ul>

### Gesicherte Funktionen, die das Sandboxing steuern

Wenn Sie einen Datenbankserver starten, sind die gesicherten Funktionen `manage_disk_sandbox` und `disk_sandbox` standardmäßig aktiviert. Diese Einstellungen steuern, ob Benutzer das Sandboxing-Verhalten ändern können. Wenn Sie die gesicherte Funktion `manage_disk_sandbox` für eine einzelne Verbindung deaktivieren möchten, müssen Sie die `sp_use_secure_feature_key`-Systemprozedur verwenden.

## Datenbanksicherungen und Sandboxing

Wenn eine Datenbank in einer Sandbox läuft, können Sie clientseitige Sicherungen ohne Einschränkungen erstellen.

Wenn Sie eine serverseitige Sicherung erstellen und die Sicherung außerhalb des Sandbox-Verzeichnisses speichern möchten, müssen Sie den Schlüssel des Datenbankservers für gesicherte Funktionen für die Verbindung angeben, auf der die Sicherung ausgeführt wird. Siehe [„Serverseitige Sicherungen erstellen“](#) auf Seite 1027.

### Siehe auch

- [„Datenbankserveroption -sbx“](#) auf Seite 279
- [„Datenbankoption -sbx“](#) auf Seite 330
- [„disk\\_sandbox-Option“](#) auf Seite 608
- [„START DATABASE-Anweisung“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- [„Datenbankserveroption -sf“](#) auf Seite 280
- [disk\\_sandbox-Verbindungseigenschaft](#) auf Seite 719
- [DiskSandbox-Servereigenschaft](#) auf Seite 749
- [DiskSandbox-Datenbankeigenschaft](#) auf Seite 772
- [„sa\\_db\\_option-Systemprozedur“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- [„sa\\_server\\_option-Systemprozedur“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- [„sp\\_use\\_secure\\_feature\\_key-Systemprozedur“](#) [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Gesicherte Funktionen

Gesicherte Funktionen sind Funktionen, bei denen Sie den Zugriff durch Datenbanken sperren können, die auf einem Datenbankserver laufen. Wenn eine Funktion gesichert (nicht verfügbar) ist, kann sie nicht von Clientanwendungen, datenbankdefinierten gespeicherten Prozeduren, Triggern und Ereignissen verwendet werden. Einstellungen für gesicherte Funktion gelten für alle Datenbanken, die auf dem Datenbankserver laufen. Gesicherte Funktionen sind nützlich, wenn Sie eine Datenbank starten, die eingebettete Logik enthalten könnte, bei der Sie unsicher sind, z.B. einen Virus, oder wenn Sie den Datenbankserver sperren möchten, weil der Datenbankserver oder die Datenbank von einem Drittanbieter gehostet wird. Mit der Datenbankserveroption -sf können Sie angeben, welche Funktionen Sie für auf dem Datenbankserver laufende Datenbanken sichern möchten.

### Standardmäßig gesicherte Funktionen

Wenn Sie einen Server mit der Datenbankserveroption -sf starten, sind die folgenden Funktionen standardmäßig gesichert:

- `manage_security` (bestehend aus `manage_features`, `manage_keys` und `manage_disk_sandbox`)
- `Serversicherheit` (nur `disk_sandbox` ist standardmäßig gesichert, nicht aber `trace_system_event`)
- `manage_server` (bestehend aus `processor_affinity`)

### Schlüssel für gesicherte Funktionen

Ein **Schlüssel für gesicherte Funktionen** wird erstellt, wenn Sie beim Erstellen des Datenbankservers die Datenbankserveroption -sk angeben. Verwenden Sie bei laufendem Datenbankserver die `sa_server_option`-Systemprozedur, um zu ändern, welche Funktionen gesichert sind. Wenn Sie eine

Datenbank starten, ohne einen Systemschlüssel für gesicherte Funktionen anzugeben, sind die standardmäßig gesicherten Funktionen gesichert und Sie können die Einstellungen für gesicherte Funktionen weder für den Datenbankserver noch für darauf laufende Datenbanken ändern. Sie können den Systemschlüssel für gesicherte Funktionen nicht später erstellen, sondern müssen den Datenbankserver herunterfahren und beim Neustart einen Systemschlüssel für gesicherte Funktionen angeben.

Nach dem Erstellen eines Systemschlüssels für gesicherte Funktionen können Sie **benutzerdefinierte Schlüssel für gesicherte Funktionen** erstellen, die bestimmten Benutzern zugeordnet werden. Damit wird der Zugriff der Benutzer ausschließlich auf die Funktionen beschränkt, die der Administrator für diesen Schlüssel gesichert hat.

Der Schlüssel muss eine nicht leere Zeichenfolge aus mindestens sechs Zeichen sein und darf keine Anführungszeichen, Steuerzeichen (alle Zeichen unter 0x20) oder Backslashes enthalten. Die Anzahl der Schlüssel für gesicherte Funktionen ist auf 1000 pro Datenbankserver begrenzt.

### Hinweis

Der Systemschlüssel für gesicherte Funktionen kann nur gelöscht werden, wenn ein benutzerdefinierter Schlüssel für gesicherte Funktionen erstellt wurde, bei dem die gesicherten Funktionen `manage_features` und `manage_keys` aktiviert sind.

Benutzerdefinierte Schlüssel für gesicherte Funktionen werden mithilfe der folgenden Systemprozeduren verwaltet:

- `sp_create_secure_feature_key`-Systemprozedur
- `sp_alter_secure_feature_key`-Systemprozedur
- `sp_drop_secure_feature_key`-Systemprozedur
- `sp_list_secure_feature_keys`-Systemprozedur

### Siehe auch

- „Datenbankserveroption -sf “ auf Seite 280
- „Datenbankserveroption -sk “ auf Seite 288
- „`sa_server_option`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Schlüssel für gesicherte Funktionen erstellen“ auf Seite 1415
- „`sp_alter_secure_feature_key`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_create_secure_feature_key`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_drop_secure_feature_key`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_list_secure_feature_keys`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_use_secure_feature_key`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_copy_directory`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_copy_file`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_create_directory`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_delete_directory`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_delete_file`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_list_directory`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_move_directory`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „`sp_move_file`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Schlüssel für gesicherte Funktionen erstellen

Steuern Sie, welche Datenbankfunktionen Benutzern zur Verfügung stehen, indem Sie mithilfe der Datenbankserveroption für gesicherte Funktionen (-sf) die Funktionen angeben, auf die Benutzer auf dem Datenbankserver keinen Zugriff erhalten sollen. Mit der Datenbankserveroption -sk können Sie einen Systemschlüssel für gesicherte Funktionen erstellen und mit der `sp_create_secure_feature_key`-Systemprozedur einen benutzerdefinierten Schlüssel für gesicherte Funktionen.

### Voraussetzungen

Sie müssen das SERVER OPERATOR-Systemprivileg und Zugriff auf die `manage_keys`-Funktion haben.

### Kontext und Bemerkungen

Einstellungen für gesicherte Funktion gelten für alle Datenbanken, die auf einem Datenbankserver laufen.

Die Option für gesicherte Funktionen (-sf) steuert beispielsweise die Verfügbarkeit folgender Funktionen:

- Serverseitige Sicherungen
- Externe gespeicherte Prozeduren
- Ferndatenzugriff
- Webdienste

Die Option -sk gibt einen Systemschlüssel für gesicherte Funktionen an, mit dem der Zugriff auf gesicherte Funktionen für einen Datenbankserver verwaltet wird. Wenn Sie die Liste der gesicherten Funktionen bei laufendem Datenbankserver ändern möchten, verwenden Sie die `sa_server_option`-Systemprozedur. Wenn Sie einen benutzerdefinierten Schlüssel für gesicherte Funktionen bei laufendem Datenbankserver ändern möchten, verwenden Sie die `sp_alter_secure_feature_key`-Systemprozedur.

### Aufgabe

1. Starten Sie an einer Eingabeaufforderung den Datenbankserver mit den Optionen -sf und -sk.

Im folgenden Beispiel wird der Datenbankserver gestartet und alle Funktionen werden gesichert. Außerdem enthält der Befehl einen Schlüssel, der später verwendet werden kann, um Zugriff auf gesicherte Funktionen für eine Verbindung zu gewähren.

```
dbsrv16 -n secure_server -sf all -sk someSystemKey c:\mydemo.db
```

2. Stellen Sie eine Verbindung mit dem Datenbankserver her:

```
dbisql -c "UID=DBA;PWD=sql;Host=myhost;Server=secure_server;DBN=mydemo"
```

3. Rufen Sie die `sp_use_secure_feature_key`-Systemprozedur auf, um den Schlüssel für gesicherte Funktionen für die Verbindung anzugeben. In diesem Fall ist der Schlüssel für gesicherte Funktionen derselbe wie durch die Option -sk angegeben:

```
CALL sp_use_secure_feature_key ( 'system' , 'someSystemKey' );
```

4. Ändern Sie die gesicherten Funktionen im Systemschlüssel für gesicherte Funktionen, indem Sie die `sa_server_option`-Systemprozedur ausführen.

Zum Beispiel:

```
CALL sa_server_option( 'SecureFeatures', '-remote_data_access' );
```

5. Erstellen Sie einen benutzerdefinierten Schlüssel für gesicherte Funktionen für einen bestimmten Benutzer.

Erstellen Sie beispielsweise einen benutzerdefinierten Schlüssel für gesicherte Funktionen für Bob, mit dem er E-Mails senden kann:

```
CALL sp_create_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' ,  
  'sa_send_email' );
```

Nach dem Anmelden bei der Datenbank muss Bob den folgenden Befehl ausführen, um E-Mails zu senden:

```
CALL sp_use_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' );
```

Benutzer von Datenbanken, die auf dem Datenbankserver `secure_server` laufen, werden am Zugriff auf alle gesicherten Funktionen gehindert, mit Ausnahme der `remote_data_access`-Funktion. Der Benutzer Bob hat jedoch auch Zugriff auf die `sa_send_email`-Funktion.

### Ergebnisse

Es gibt nun eine gesicherte Systemfunktion für den Datenbankserver sowie eine benutzerdefinierte gesicherte Funktion, die einem bestimmten Benutzer zugeordnet wurde.

### Siehe auch

- „Datenbankserveroption -sf “ auf Seite 280
- „Datenbankserveroption -sk “ auf Seite 288
- „sa\_server\_option-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_alter\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_create\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_drop\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_list\_secure\_feature\_keys-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „sp\_use\_secure\_feature\_key-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Audits von Datenbankaktivitäten

Mit jeder Datenbank ist eine Transaktionslogdatei verbunden. Das Transaktionslog wird für die Wiederherstellung der Datenbank verwendet. Es ist ein Protokoll der Transaktionen, die in einer Datenbank ausgeführt wurden.

Das Transaktionslog speichert alle Datendefinitionsanweisungen und die ID des Benutzers, der sie ausgeführt hat. Es registriert auch alle Aktualisierungen, Löschungen, Einfügungen und die Namen der Benutzer, die diese Anweisungen ausgeführt haben. Für bestimmte Auditingzwecke reicht dies allerdings nicht aus. Standardmäßig enthält das Transaktionslog nicht die Zeit des Ereignisses, sondern nur die Reihenfolge, in der die Ereignisse eintraten. Es enthält keine fehlgeschlagenen Ereignisse, und auch keine Auswahlanweisungen.

**Auditing** verfolgt die in einer Datenbank ausgeführten Aktivitäten. Wenn Sie Auditing verwenden, werden zusätzliche Daten im Transaktionslog gespeichert, und zwar folgende:

- Alle Login-Versuche (erfolgreiche und fehlgeschlagene), einschließlich der Terminal-ID
- Präzise Zeitangaben für alle Ereignisse (bis auf Millisekunden)
- Alle Berechtigungsprüfungen (erfolgreiche und fehlgeschlagene), einschließlich des Objekts, für das die Prüfung erfolgte (wenn anwendbar)
- Alle Aktionen, die Systemprivilegien erfordern

Sie können die Verwendung eines Transaktionslogs nicht stoppen, während Auditing für eine Datenbank aktiviert ist. Wenn Sie das Transaktionslog deaktivieren möchten, müssen Sie zuerst das Auditing deaktivieren.

### Auditing von einzelnen Verbindungen

Wenn Sie Auditing bei einer Datenbank aktiviert haben, können Sie die temporäre Datenbankoption `conn_auditing` in der Datenbank-Login-Prozedur setzen, um verbindungsspezifisches Auditing zu aktivieren. Sie können Auditing basierend auf Informationen wie der IP-Adresse des Clientcomputers oder dem Verbindungstyp aktivieren.

Wenn Sie die Option `conn_auditing` in der Login-Prozedur nicht setzen, ist die Option standardmäßig auf "On".

Das folgende Beispiel zeigt einen Ausschnitt aus einer Login-Prozedur, die Auditing für alle Verbindungen zur Datenbank aktiviert, außer denjenigen, die vom DBA-Benutzer hergestellt werden:

```
DECLARE usr VARCHAR(128)
SELECT CONNECTION_PROPERTY( 'Userid' ) INTO usr;
IF usr != 'DBA' THEN
    SET TEMPORARY OPTION conn_auditing='On'
ELSE
    SET TEMPORARY OPTION conn_auditing='Off'
END IF;
```

### Audit-Kommentare

Sie können in den Audit-Trail Kommentare einfügen, indem Sie die Systemprozedur `sa_audit_string` verwenden. Sie übernimmt nur ein Argument, nämlich eine Zeichenfolge von bis zu 200 Byte. Zum Beispiel:

```
CALL sa_audit_string( 'Started audit testing here.' );
```

Dieser Kommentar wird im Transaktionslog als Audit-Anweisung gespeichert.

### Siehe auch

- „`sa_audit_string`-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Das Transaktionslog“ auf Seite 135

## Auditing-Aktionen außerhalb des Datenbankservers

Einige Datenbank-Dienstprogramme arbeiten direkt in der Datenbankdatei. In einer sicheren Umgebung sollten nur vertrauenswürdige Benutzer Zugriff auf die Datenbankdateien haben.

Um unter Windows oder Unix das Auditing von Aktionen verfügbar zu machen, generiert die Verwendung von "dbtran" oder "dblog" im selben Verzeichnis wie die Datenbankdatei eine Textdatei mit der Erweiterung *.alg*. Beispiel: Bei *demo.db* wird die Datei *demo.alg* genannt. Aufzeichnungen, die den Toolnamen, den Windows- oder Unix-Benutzernamen und Datum/Uhrzeit enthalten, werden an diese Datei angehängt. Aufzeichnungen werden der *.alg*-Datei nur hinzugefügt, wenn die Option auditing auf "On" gesetzt ist.

### Siehe auch

- „auditing-Option“ auf Seite 582
- „Dienstprogramm zur Logkonvertierung (dbtran)“ auf Seite 948
- „Transaktionslog-Dienstprogramm (dblog)“ auf Seite 998

## Auditing konfigurieren (Sybase Central)

Sie können Sybase Central verwenden, um Auditing für sicherheitsbezogene Daten im Transaktionslog zu konfigurieren. Auditing ist standardmäßig deaktiviert.

### Voraussetzungen

Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Auditing** und wählen Sie eine der folgenden Optionen:
  - **Keine Audit-Informationen für diese Datenbank sammeln** Es werden keine Audit-Daten gesammelt. Diese Option deaktiviert Auditing, indem die Datenbankoption "Auditing" auf "Off" gesetzt wird.
  - **Alle Audit-Informationen für diese Datenbank sammeln** Alle Arten von Audit-Daten werden für diese Datenbank gesammelt. Diese Option aktiviert Auditing, indem die Datenbankoption "Auditing" auf "On" gesetzt wird.

Das Transaktionslog kann signifikant zunehmen, wenn diese Option ausgewählt ist.

- **Folgende Arten von Audit-Informationen für diese Datenbank sammeln** Damit können Sie angeben, welche Audit-Daten Sie sammeln möchten. Sie könnten beispielsweise festlegen, nur DLL-Änderungen zu sammeln.

Das Auswählen dieser Option ändert die Einstellung der auditing\_options-Datenbankoption.

4. Klicken Sie auf **OK**.

## Ergebnisse

Das Auditing-Verhalten wird konfiguriert.

## Siehe auch

- „auditing-Option“ auf Seite 582
- „sa\_enable\_auditing\_type-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „auditing\_options-Option (für die Verwendung durch das System reserviert)“ auf Seite 583

## Auditing konfigurieren (Interactive SQL)

Sie können Interactive SQL verwenden, um Auditing für sicherheitsbezogene Daten im Transaktionslog zu konfigurieren. Auditing ist standardmäßig deaktiviert.

## Voraussetzungen

Sie müssen das SET ANY SECURITY OPTION-Systemprivileg haben.

## Aufgabe

1. Stellen Sie eine Verbindung mit Ihrer Datenbank her.
2. Führen Sie die folgende Anweisung aus, um Auditing zu aktivieren:

```
SET OPTION PUBLIC.auditing = 'On';
```

Um anzugeben, welche Arten von Audit-Daten Sie sammeln möchten, verwenden Sie die folgende Systemprozedur:

```
CALL sa_enable_auditing_type( 'all' );
```

Sie können die Art der gesammelten Audit-Daten steuern, indem Sie **all** durch die Arten von Auditing ersetzen, die Sie aktivieren möchten.

3. Führen Sie die folgende Anweisung aus, um Auditing zu deaktivieren:

```
SET OPTION PUBLIC.auditing = 'Off';
```

Um anzugeben, welche Arten von Audit-Daten Sie deaktivieren möchten, verwenden Sie die folgende Systemprozedur:

```
CALL sa_disable_auditing_type( 'all' );
```

Sie können das Sammeln bestimmter Arten von Audit-Daten stoppen, indem Sie **all** durch die Arten von Auditing ersetzen, die Sie deaktivieren möchten.

## Ergebnisse

Das Auditing-Verhalten wird konfiguriert.

### Siehe auch

- „login\_procedure-Option“ auf Seite 625
- „conn\_auditing-Option“ auf Seite 592
- „auditing-Option“ auf Seite 582
- „auditing-Option“ auf Seite 582
- „sa\_enable\_auditing\_type-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „auditing\_options-Option (für die Verwendung durch das System reserviert)“ auf Seite 583

## Audit-Daten (Sybase Central)

Sie können Sybase Central verwenden, um Audit-Daten aus dem Transaktionslog abzurufen.

### Voraussetzungen

Sie müssen das BACKUP DATABASE-Systemprivileg haben, um Audit-Daten von einem laufenden Datenbankserver abrufen zu können. Es sind keine Privilegien erforderlich, um Audit-Daten aus einer Datenbank-Transaktionslogdatei abzurufen.

### Aufgabe

1. Stellen Sie in Sybase Central eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
2. Wählen Sie im linken Fensterausschnitt die Datenbank aus.
3. Klicken Sie im rechten Fensterausschnitt auf die Registerkarte **Auditing**.
4. Klicken Sie auf **Audit-Meldungen abrufen**.

Ein Fenster wird eingeblendet, das die dbtran-Meldungen anzeigt. Ignorieren Sie die Warnung über die chronologisch gereihte Ausgabe.

5. Klicken Sie auf **Schließen**.

Die Audit-Daten werden auf der Registerkarte **Auditing** angezeigt.

6. Verwenden Sie die Filteroptionen, um zu steuern, welche Audit-Daten angezeigt werden sollen.

Sie können wählen, ob alle Audit-Daten angezeigt werden sollen, nur Fehler oder nur Audit-Meldungen, die den von Ihnen angegebenen Text enthalten. Klicken Sie auf **Übernehmen**, um die Filteroptionen zu übernehmen.

7. Wählen Sie einen Eintrag aus der Tabelle der Audit-Einträge, um Details dazu anzuzeigen.
8. Wenn Sie aktuelle Audit-Daten abfragen möchten, drücken Sie F5 und wiederholen Sie diesen Vorgang.

### Ergebnisse

Audit-Daten werden abgerufen.

**Siehe auch**

- „Auditing-Beispiele“ auf Seite 1422

## Audit-Daten abrufen (Dienstprogramm dbtran)

Das Dienstprogramm dbtran verwendet das angegebene Transaktionslog, um ein SQL-Skript zu erzeugen. Dieses enthält alle Transaktionen sowie Angaben dazu, welche Benutzer die einzelnen Befehle ausgeführt haben.

**Voraussetzungen**

Sie müssen das BACKUP DATABASE-Systemprivileg haben, um Audit-Daten von einem laufenden Datenbankserver abrufen zu können. Es sind keine Privilegien erforderlich, um Audit-Daten aus einer Datenbank-Transaktionslogdatei abzurufen.

**Kontext und Bemerkungen**

Wenn Sie die Datenbankserveroption -g verwenden, bezieht dbtran zusätzliche Kommentare mit Audit-Daten ein. Die Option -g entspricht dem Angeben der Datenbankserveroptionen -d, -t und -a.

**Aufgabe**

1. Stellen Sie eine Verbindung mit der Datenbank her.
2. Sie können das Dienstprogramm dbtran auf einem laufenden Datenbankserver oder in einer Datenbank-Transaktionslogdatei ausführen.

Option	Aktion
Audit-Daten von einem laufenden Datenbankserver abrufen	Führen Sie den folgenden Befehl aus:  <code>dbtran -g -c connection-string -n SQL-file</code>
Audit-Daten aus einer Transaktionslogdatei abrufen	Fahren Sie den Datenbankserver herunter, um zu gewährleisten, dass die Transaktionslogdatei verfügbar ist. Führen Sie den folgenden Befehl aus:  <code>dbtran -g transaction-log SQL-file</code>

**Ergebnisse**

Audit-Daten werden abgerufen und in einer SQL-Skriptdatei gespeichert.

**Beispiel**

In dem Beispiel werden die Audit-Daten in der Datei *demo.sql* gespeichert und die Datei enthält Informationen zur Beispieldatenbank.

```
dbtran -g -c "UID=DBA;PWD=sql;DBN=demo" -n demo.sql
```

Im folgenden Beispiel werden die Audit-Daten aus der Transaktionslogdatei *demo.log* in der Datei *demo.sql* platziert.

```
dbtran -g demo.log demo.sql
```

#### Siehe auch

- „Verbindungsparameter“ auf Seite 337
- „Dienstprogramm zur Logkonvertierung (dbtran)“ auf Seite 948

## Auditing-Beispiele

Dieses Beispiel zeigt, wie die Auditing-Funktion Versuche aufzeichnet, entweder mit Sybase Central oder mit Interactive SQL Zugriff auf nicht autorisierte Daten zu erhalten.

### Auditing-Beispiel für Sybase Central

1. Starten Sie Sybase Central und stellen Sie eine Verbindung mit der Beispieldatenbank unter Verwendung der Datenquelle **SQL Anywhere 16 Demo** her.  
  
Dies verbindet Sie als Benutzer mit der SYS\_AUTH\_DBA\_ROLE-Systemrolle.
2. Auditing aktivieren:
  - a. Rechtsklicken Sie auf die Datenbank und klicken Sie auf **Eigenschaften**.
  - b. Klicken Sie auf die Registerkarte **Auditing**.
  - c. Klicken Sie auf **Alle Audit-Informationen für diese Datenbank sammeln**.
  - d. Klicken Sie auf **Übernehmen**.
  - e. Klicken Sie auf **OK**.
3. Fügen Sie einen Benutzer namens Test1 mit dem Kennwort "welcome" zur Beispieldatenbank hinzu und erteilen Sie dem Benutzer das MANAGE PROFILING-Systemprivileg:
  - a. Rechtsklicken Sie auf **Benutzer** und klicken Sie auf **Neu » Benutzer**.
  - b. Wenn Sie dazu aufgefordert werden, geben Sie den Benutzernamen **Test1** und das Kennwort **welcome** ein.
  - c. Klicken Sie auf **Fertig stellen**.
  - d. Wählen Sie den neuen Benutzer unter **Benutzer** aus und öffnen Sie die Registerkarte **Systemprivilegien**.
  - e. Rechtsklicken Sie auf die Registerkarte **Systemprivilegien** und klicken Sie auf **Neu » Erteilte Systemprivilegien**.
  - f. Wählen Sie **MANAGE PROFILING** aus und klicken Sie auf **OK**, um Test1 das MANAGE PROFILING-Systemprivileg zu erteilen.

- g. Klicken Sie im Sybase Central-Hauptmenü auf **Datei** und **Speichern**, um Ihre Änderungen zu speichern.
  - h. Klicken Sie im Sybase Central-Hauptmenü auf **Verbindungen** und **Trennen**, um die Verbindung mit der Beispieldatenbank zu trennen.
4. Unter Verwendung von Sybase Central stellen Sie eine Verbindung zur Beispieldatenbank als Test1 her und versuchen Sie, auf vertrauliche Informationen in der Employees-Tabelle zuzugreifen:
- a. Klicken Sie auf **Tabellen** und wählen Sie dann die Employees-Tabelle aus.
  - b. Klicken Sie auf die Registerkarte **Daten**.  
  
Sie werden in einer Fehlermeldung darauf hingewiesen, dass Sie keine SELECT-Berechtigung für die Employees-Tabelle haben. Siehe „[Berechtigung verweigert: %1](#)“ [[Fehlermeldungen](#)].
  - c. Klicken Sie auf **OK**.
  - d. Trennen Sie die Verbindung zur Beispieldatenbank.
5. Zeigen Sie die Audit-Daten zu dieser Aktivität an:
- a. Stellen Sie eine Verbindung zur Datenbank mithilfe des **SQL Anywhere 16**-Plug-Ins her.
  - b. Wählen Sie die Datenbank aus und klicken Sie auf die Registerkarte **Auditing** im rechten Fensterausschnitt.
  - c. Klicken Sie auf **Audit-Nachrichten abrufen**.
  - d. Klicken Sie auf **Schließen**.

Audit-Daten werden angezeigt.

- e. Verwenden Sie die Filteroptionen, um die Position des Fehlers in der Tabelle der Audit-Daten zu ermitteln. Sie können den Fehler für Test1 finden, indem Sie die Option **Nur Fehler** auswählen. Verwenden Sie die Datums- und Uhrzeitinformatoren, um den Fehler festzulegen. Beispiel: Wenn Test1 versucht hat, auf die Employees-Tabelle am 6. November 2007 um 10:07:14 zuzugreifen, sieht der Audit-Eintrag so ähnlich wie der folgende Eintrag aus:  
  

```
2007-11-06 10:07:14 | Permission
```
6. Setzen Sie die Beispieldatenbank in ihren ursprünglichen Zustand zurück:
- a. Rechtsklicken Sie auf die Datenbank und klicken Sie dann auf **Eigenschaften**.
  - b. Klicken Sie auf der Registerkarte **Auditing** auf **Keine Audit-Informationen für diese Datenbank sammeln**.
  - c. Klicken Sie auf **OK**.
  - d. Klicken Sie auf **Benutzer**.

Rechtsklicken Sie auf "Test1" und klicken Sie auf **Löschen**.

### Auditing-Beispiel für Interactive SQL

1. Starten Sie Interactive SQL und stellen Sie eine Verbindung mit der Beispieldatenbank unter Verwendung der Datenquelle **SQL Anywhere 16 Demo** her.

Dies verbindet Sie als Benutzer mit der SYS\_AUTH\_DBA\_ROLE-Systemrolle.

2. Schalten Sie Auditing ein, indem Sie die Anweisung SET OPTION folgendermaßen verwenden:

```
SET OPTION PUBLIC.auditing = 'On';
```

3. Fügen Sie einen Benutzer (Test1) der Beispieldatenbank unter Verwendung der Anweisung CREATE USER hinzu, und zwar folgendermaßen:

```
CREATE USER Test1  
IDENTIFIED BY welcome;
```

4. Öffnen Sie ein neues Interactive SQL-Fenster, stellen Sie für den Benutzer Test1 eine Verbindung mit der Beispieldatenbank her und versuchen Sie, auf vertrauliche Informationen in der Employees-Tabelle unter Verwendung der folgenden SELECT-Anweisung zuzugreifen:

```
SELECT Surname, Salary  
FROM GROUPO.Employees;
```

Sie werden in einer Fehlermeldung darauf hingewiesen, dass Sie keine SELECT-Berechtigung für die Employees-Tabelle haben. Siehe „[Berechtigung verweigert: %1](#)“ [[Fehlermeldungen](#)].

5. Führen Sie den folgenden Befehl aus, um die Audit-Daten zu dieser Aktivität anzuzeigen:

```
dbtran -g -c "DSN=SQL Anywhere 16 Demo" -n demo.sql
```

6. Setzen Sie die Beispieldatenbank in ihren ursprünglichen Zustand zurück:

- Verwenden Sie die Anweisung DROP USER, um den Benutzer Test1 aus der Datenbank zu entfernen:

```
DROP USER Test1;
```

- Schalten Sie Auditing aus, indem Sie die folgende Anweisung SET OPTION verwenden:

```
SET OPTION PUBLIC.auditing = 'Off';
```

## Datenbankverschlüsselung und -entschlüsselung

Sie können die Datenbankverschlüsselung einsetzen, damit es schwieriger wird, die Daten in Ihrer Datenbank zu entziffern. Sie können Ihre Datenbank entweder mit einfacher Verschlüsselung oder mit starker Verschlüsselung chiffrieren.

#### Hinweis

Wenn Ihre Datenbank verschlüsselt ist, ergibt die Komprimierung mit einem Programm wie WinZip nur eine geringfügig kleinere Datei als die Original-Datenbankdatei.

## Einfache Verschlüsselung und starke Verschlüsselung

### Einfache Verschlüsselung

Einfache Verschlüsselung ist gleichbedeutend mit einem Verschleiern und erschwert das Dechiffrieren der Daten in Ihrer Datenbank mithilfe eines Festplatten-Dienstprogramms. Bei der einfachen Verschlüsselung wird kein Schlüssel benötigt, um die Datenbank zu chiffrieren.

### Starke Verschlüsselung

Bei der starken Verschlüsselung wird die Datenbank ohne den entsprechenden Schlüssel (Kennwort) unbrauchbar. Ein Algorithmus kodiert die Informationen in Ihren Datenbank- und Transaktionslogdateien, damit sie nicht entschlüsselt werden können.

In SQL Anywhere kann der Datenbankadministrator vier Aspekte der starken Verschlüsselung steuern:

- Status der starken Verschlüsselung
- Chiffrierschlüssel
- Schutz des Chiffrierschlüssels
- Verschlüsselungsalgorithmus

### Unterstützte Algorithmen für die starke Verschlüsselung

Der zur Implementierung der starken SQL Anywhere-Verschlüsselung verwendete Algorithmus ist AES: ein Block-Verschlüsselungsalgorithmus, der als Advanced Encryption Standard (AES) für Block-Chiffren vom amerikanischen National Institute of Standards and Technology (NIST) ausgewählt wurde.

Sie können auch ein separates FIPS-genehmigtes AES-Modul für starke Verschlüsselung angeben, indem Sie den Typ AES\_FIPS (128 Bit) oder AES256\_FIPS (256 Bit) verwenden. Wenn der Datenbankserver mit der Option -fips gestartet wird, können Sie Datenbanken mit starker AES-, AES256-, AES\_FIPS- oder AES256\_FIPS-Verschlüsselung ausführen, jedoch keine Datenbanken mit einfacher Verschlüsselung. Unverschlüsselte Datenbanken können ebenfalls auf dem Server gestartet werden, wenn -fips angegeben wurde.

Die SQL Anywhere-Sicherheitsoption muss auf jedem Computer installiert sein, der verwendet wird, um eine mit AES\_FIPS oder AES256\_FIPS verschlüsselte Datenbank auszuführen.

Die FIPS-zertifizierte Verschlüsselung ist nicht auf allen Plattformen verfügbar. Eine Liste der unterstützten Plattformen finden Sie unter <http://www.sybase.com/detail?id=1061806>.

#### Hinweis

Erforderliche getrennt lizenzierte Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierte Komponenten“ [*SQL Anywhere 16 - Einführung*].

### Siehe auch

- „Datenbankserveroption -fips“ auf Seite 237
- „Neuladen einer Datenbank“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE ENCRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Methoden zur Datenbankverschlüsselung

- **Verschlüsselte Datenbanken erstellen** Sie können Folgendes verwenden:
  - Das Dienstprogramm Initialisierung (dbinit) in Kombination mit verschiedenen Optionen zum Aktivieren der starken Verschlüsselung.

Die Optionen -ep und -ek des Dienstprogramms dbinit erstellen eine Datenbank mit starker Verschlüsselung, wobei Sie den Chiffrierschlüssel in einem Dialogfeld oder in der Befehlszeile festlegen können. Die Option -ea des Dienstprogramms dbinit setzt den Verschlüsselungsalgorithmus auf AES oder AES256 (bzw. beim FIPS-zertifizierten Modul auf AES\_FIPS oder AES256\_FIPS).
  - CREATE DATABASE-Anweisung.
  - Den **Assistenten zum Erstellen einer Datenbank** in Sybase Central zum Erstellen einer stark verschlüsselten Datenbank.
- **Vorhandene Datenbanken verschlüsseln** Obwohl Sie die starke Verschlüsselung in einer vorhandenen Datenbank nicht einfach aktivieren oder deaktivieren können, haben Sie folgende Möglichkeiten, um die starke Verschlüsselung zu implementieren:
  - Bauen Sie eine vorhandene Datenbank neu auf (Entladen/Neuladen) und ändern Sie dabei den Verschlüsselungsstatus. Sie können eine Datenbank neu aufbauen, indem alle Daten und Schemata einer vorhandenen Datenbank entladen werden. Hierdurch wird eine neue Datenbank (an dieser Stelle können Sie eine Reihe von Einstellungen, einschließlich der starken Verschlüsselung, ändern) erstellt und die Daten in die neue Datenbank geladen. Sie müssen den Schlüssel kennen, um eine stark verschlüsselte Datenbank entladen zu können. Wählen Sie für den Neuaufbau (Entladen/Neuladen) einer Datenbank eine der folgenden Methoden:
    - Das Dienstprogramm zum Entladen (dbunload).

Das Dienstprogramm zum Entladen (dbunload) mit Optionen zum Erstellen einer neuen Datenbank mit starker Verschlüsselung. Die Option -an erstellt eine Datenbank. Um die starke Verschlüsselung und den Chiffrierschlüssel in einem Dialogfeld oder in der Befehlszeile einzugeben, benutzen Sie die Option -ek oder -ep. Die Option -ea setzt den Verschlüsselungsalgorithmus auf AES oder AES256 (bzw. beim FIPS-zertifizierten Modul auf AES\_FIPS oder AES256\_FIPS).
    - Die Anweisungen UNLOAD und RELOAD.

- Den **Assistenten zum Entladen einer Datenbank**. Siehe „Tipps zum Exportieren von Daten mit dem Assistenten zum Entladen einer Datenbank“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*].
- Sie können die CREATE ENCRYPTED DATABASE-Anweisung oder die CREATE ENCRYPTED FILE-Anweisung verwenden. Siehe „Vergleich von CREATE ENCRYPTED DATABASE und CREATE ENCRYPTED FILE“ auf Seite 1427.
- **Tabellen, Spalten und materialisierte Ansichten verschlüsseln** Siehe „Spalten- und Tabellenverschlüsselung“ auf Seite 1434.

#### Siehe auch

- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ENCRYPT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Dienstprogramm zum Entladen (dbunload)“ auf Seite 1000
- „UNLOAD-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Tipps zum Exportieren von Daten mit dem Assistenten zum Entladen einer Datenbank“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „CREATE ENCRYPTED DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE ENCRYPTED FILE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Vergleich von CREATE ENCRYPTED DATABASE und CREATE ENCRYPTED FILE

Verwenden Sie die Anweisung CREATE ENCRYPTED DATABASE, wenn eine Datenbank vorhanden ist, die Sie verschlüsseln möchten. Verwenden Sie die Anweisung CREATE ENCRYPTED FILE nur, wenn eine Datenbank vorhanden ist, die Sie zur Wiederherstellung verschlüsseln möchten.

Sie dürfen beim Ausführen der Anweisung nicht mit der Datenbank verbunden sein, die Sie verschlüsseln möchten.

Die Anweisungen CREATE ENCRYPTED FILE und CREATE ENCRYPTED DATABASE haben folgende Unterschiede:

- Die Anweisung CREATE ENCRYPTED FILE muss für alle Dateien, die zur Datenbank gehören (Transaktionslog, Transaktionslogspiegel, DBSpace, wenn vorhanden), getrennt durchgeführt werden. Mit der Anweisung CREATE ENCRYPTED DATABASE werden dagegen alle zur Datenbank gehörenden Dateien automatisch verschlüsselt.
- Die Anweisung CREATE ENCRYPTED DATABASE kann nicht für eine Datenbank verwendet werden, die eine Wiederherstellung benötigt, die Anweisung CREATE ENCRYPTED FILE hingegen schon.
- Die Anweisung CREATE ENCRYPTED DATABASE kann nicht in Prozeduren, Triggern oder Batches verwendet werden. Die Anweisung CREATE ENCRYPTED FILE hingegen schon.

- Die Anweisung CREATE ENCRYPTED DATABASE unterstützt den Verschlüsselungsalgorithmus SIMPLE, die Anweisung CREATE ENCRYPTED FILE hingegen nicht.

### Siehe auch

Weitere Informationen zu Chiffrierschlüsseln finden Sie unter „[Verbindungsparameter DatabaseKey \(DBKEY\)](#)“ auf Seite 353.

Unter Windows Mobile werden die AES\_FIPS- und AES256\_FIPS-Algorithmen nur mit ARM-Prozessoren unterstützt.

#### Hinweis

FIPS steht nicht auf allen Plattformen zur Verfügung. Eine Liste der unterstützten Plattformen finden Sie unter <http://www.sybase.com/detail?id=1061806>.

### Siehe auch

- „CREATE ENCRYPTED DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE ENCRYPTED FILE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verschlüsselte Kopien von vorhandenen Datenbanken erstellen (SQL)“ auf Seite 1430

## Verschlüsselte Datenbanken erstellen (SQL)

Sie können eine Datenbank während der Erstellung verschlüsseln, indem Sie die ENCRYPTED-Klausel mit der CREATE DATABASE-Anweisung verwenden.

### Voraussetzungen

Standardmäßig müssen Sie das SERVER OPERATOR-Systemprivileg haben. Die erforderlichen Privilegien können mithilfe der Datenbanksoption -gu geändert werden.

### Kontext und Bemerkungen

Diese Aufgabe unterscheidet sich vom Verschlüsseln einer vorhandenen Datenbank. Verwenden Sie zum Verschlüsseln einer vorhandenen Datenbank die CREATE ENCRYPTED DATABASE-Anweisung.

#### Vorsicht

Achten Sie bei stark verschlüsselten Datenbanken darauf, eine Kopie des Schlüssels an einem sicheren Ort zu verwahren. Wenn Sie den Chiffrierschlüssel verlieren, gibt es keine Möglichkeit, auf die Daten zuzugreifen, auch nicht mit Unterstützung durch den technischen Support. Sie müssen die Datenbank verwerfen und eine neue Datenbank erstellen.

### Aufgabe

1. Stellen Sie in Interactive SQL eine Verbindung mit einer vorhandenen Datenbank her.
2. Führen Sie eine CREATE DATABASE-Anweisung aus, die die ENCRYPTED-Klausel sowie die Optionen KEY und ALGORITHM enthält.

## Ergebnisse

Eine verschlüsselte Datenbank wird erstellt.

## Beispiel

Mit der folgenden Anweisung wird beispielsweise eine Datenbankdatei namens *myencrypteddb.db* im Verzeichnis *c:\temp\* erstellt, und zwar mit FIPS-zertifizierter 128-Bit-AES-Verschlüsselung. Außerdem wird die Benutzer-ID "DBA" mit dem Kennwort "sql" erstellt.

```
CREATE DATABASE 'c:\\temp\\myencrypteddb.db'
DBA USER 'DBA' DBA PASSWORD 'sql'
TRANSACTION LOG ON
ENCRYPTED ON
KEY '0kZ2o52AK#'
ALGORITHM 'AES_FIPS';
```

## Siehe auch

- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Datenbankserveroption -gu “ auf Seite 255

## Verschlüsselte Datenbanken erstellen (Dienstprogramm dbinit)

Sie können eine verschlüsselte Datenbank mit dem Dienstprogramm dbinit erstellen.

## Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

## Kontext und Bemerkungen

### Vorsicht

Achten Sie bei stark verschlüsselten Datenbanken darauf, eine Kopie des Schlüssels an einem sicheren Ort zu verwahren. Wenn Sie den Chiffrierschlüssel verlieren, gibt es keine Möglichkeit, auf die Daten zuzugreifen, auch nicht mit Unterstützung durch den technischen Support. Sie müssen die Datenbank verwerfen und eine neue Datenbank erstellen.

## Aufgabe

- Führen Sie das Dienstprogramm dbinit aus, um eine Datenbank zu erstellen.
  - Wenn Sie die Datenbank mit einfacher Verschlüsselung verschlüsseln möchten, beziehen Sie die Option "-ea simple" ein.
  - Wenn Sie die Datenbank mit starker Verschlüsselung verschlüsseln möchten, beziehen Sie die Option -ek oder -ep ein, um den Chiffrierschlüssel anzugeben.

## Ergebnisse

Eine verschlüsselte Datenbank wird erstellt.

## Nächste Schritte

Beim Starten der Datenbank oder Herstellen einer Verbindung müssen Sie den Chiffrierschlüssel angeben.

## Beispiel

- Im folgenden Beispiel wird die Datenbank *test.db* mit einfacher Verschlüsselung erstellt und die Benutzer-ID "DBA" wird als DBA mit dem Kennwort "sql" konfiguriert:

```
dbinit -dba DBA,sql -ea simple test.db
```

- Der folgende Befehl erstellt eine stark verschlüsselte Datenbank mit Angabe des Chiffrierschlüssels und des Algorithmus.

```
dbinit -dba DBA,sql -ek "0kZ2o56AK#" -ea AES_FIPS "myencrypteddb.db"
```

Führen Sie zum Starten dieser Datenbank den folgenden Befehl aus:

```
dbsrv16 myencrypteddb.db -ek "0kZ2o56AK#"
```

## Siehe auch

- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Verschlüsselte Kopien von vorhandenen Datenbanken erstellen (SQL)

Mithilfe der CREATE ENCRYPTED DATABASE-Anweisung können Sie eine verschlüsselte Kopie einer vorhandenen Datenbank erstellen. Diese Anweisung erstellt eine Kopie der Datei (in diesem Fall in verschlüsselter Form) und überschreibt nicht die ursprüngliche Datenbankdatei.

### Voraussetzungen

Standardmäßig benötigen Sie zum Ausführen der CREATE ENCRYPTED DATABASE-Anweisung das SERVER OPERATOR-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gu geändert werden.

Die Datenbank, die Sie verschlüsseln möchten, darf nicht laufen.

### Kontext und Bemerkungen

#### Vorsicht

Achten Sie bei stark verschlüsselten Datenbanken darauf, eine Kopie des Schlüssels an einem sicheren Ort zu verwahren. Wenn Sie den Chiffrierschlüssel verlieren, gibt es keine Möglichkeit, auf die Daten zuzugreifen, auch nicht mit Unterstützung durch den technischen Support. Sie müssen die Datenbank verwerfen und eine neue Datenbank erstellen.

## Aufgabe

1. Stellen Sie in Interactive SQL eine Verbindung mit einer anderen vorhandenen Datenbank her als derjenigen, die Sie verschlüsseln möchten.
2. Verschlüsseln Sie die Datenbank mit der CREATE ENCRYPTED DATABASE-Anweisung.

## Ergebnisse

Wenn Sie eine CREATE ENCRYPTED DATABASE-Anweisung ausführen, verschlüsseln (überschreiben) Sie die Datei nicht, sondern erstellen eine Kopie der Datei in verschlüsselter Form. Wenn der Datenbank Transaktionslogs, Transaktionslogspiegel oder DBSpaces zugeordnet sind, werden auch verschlüsselte Kopien dieser Dateien erstellt.

## Beispiel

Im folgenden Beispiel wird für die Datenbankdatei *temp.db* eine AES-verschlüsselte Kopie namens *encryptedtemp.db* erstellt.

```
CREATE ENCRYPTED DATABASE 'C:\temp\encryptedtemp.db'
FROM 'C:\temp\temp.db'
KEY 'abc'
ALGORITHM 'AES' ;
```

## Siehe auch

- „CREATE ENCRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Vergleich von CREATE ENCRYPTED DATABASE und CREATE ENCRYPTED FILE“ auf Seite 1427

## Datenbanken entschlüsseln (SQL)

Sie können eine Datenbank mit der CREATE DECRYPTED DATABASE-Anweisung entschlüsseln. Diese Anweisung erstellt eine Kopie der Datei (in entschlüsselter Form) und überschreibt nicht die ursprüngliche Datenbankdatei.

## Voraussetzungen

Standardmäßig benötigen Sie zum Ausführen der CREATE DECRYPTED TABLE DATABASE-Anweisung das SERVER OPERATOR-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gu geändert werden.

Die Datenbank, die Sie verschlüsseln möchten, darf nicht laufen.

## Kontext und Bemerkungen

Wenn Sie eine Datenbank, die wiederhergestellt werden muss, entschlüsseln möchten, um sie an den technischen Support zu senden, müssen Sie die CREATE DECRYPTED FILE-Anweisung verwenden. Alle zu der Datenbank gehörenden Dateien, z.B. Transaktionslogs und Transaktionslogspiegel sowie DBSpace-Dateien, müssen ebenfalls mit dieser Anweisung entschlüsselt werden.

## Aufgabe

1. Stellen Sie in Interactive SQL eine Verbindung mit einer anderen Datenbank her als derjenigen, die Sie entschlüsseln möchten.
2. Führen Sie eine CREATE DECRYPTED DATABASE-Anweisung aus.

## Ergebnisse

Wenn Sie eine CREATE DECRYPTED DATABASE-Anweisung ausführen, entschlüsseln (überschreiben) Sie die Datei nicht, sondern erstellen eine Kopie der Datei in entschlüsselter Form. Wenn der Datenbank Transaktionslogs, Transaktionslogspiegel oder DBSpaces zugeordnet sind, werden auch entschlüsselte Kopien dieser Dateien erstellt.

## Beispiel

Die erste Anweisung erstellt eine mit AES256 verschlüsselte Kopie der Datenbank *temp.db* mit dem Namen *encryptedtemp.db*. Die zweite Anweisung erstellt eine entschlüsselte Kopie von *encryptedtemp.db* mit dem Namen *decryptedtemp.db*.

```
CREATE ENCRYPTED DATABASE 'C:\temp\encryptedtemp.db'  
FROM 'C:\temp\temp.db'  
KEY 'abc'  
ALGORITHM 'AES256';  
CREATE DECRYPTED DATABASE 'C:\temp\decryptedtemp.db'  
FROM 'C:\temp\encryptedtemp.db'  
KEY 'abc';
```

## Siehe auch

- „CREATE DECRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Chiffrierschlüssel

Es empfiehlt sich, einen Chiffrierschlüsselwert auszuwählen, der nicht leicht zu erraten ist. Der Schlüssel kann von beliebiger Länge sein, im Allgemeinen gilt: Je länger der Schlüssel, desto schwieriger lässt er sich erraten. Auch das Kombinieren von Zahlen, Buchstaben und Sonderzeichen reduziert die Gefahr des Erratens.

Chiffrierschlüssel berücksichtigen immer die Groß-/Kleinschreibung und dürfen keine voran- bzw. nachgestellte Leerzeichen oder Semikola enthalten.

Sie müssen diesen Schlüssel immer dann angeben, wenn Sie die Datenbank starten wollen. Wenn Sie den Schlüssel verlieren, können Sie nie mehr auf die Datenbank zugreifen.

Der Chiffrierschlüssel kann entweder an einer Eingabeaufforderung (Standard) oder in ein Dialogfeld eingegeben werden. Wenn das System in einem Dialogfeld zur Eingabe des Schlüssels auffordert, ist eine höhere Sicherheitsstufe gewährleistet, weil der Schlüssel nie im Klartext erscheint. Clients müssen den Schlüssel immer angeben, wenn sie die Datenbank starten. Wenn der Datenbankadministrator die Datenbank startet, brauchen Clients keinen Zugriff auf den Schlüssel. Siehe „[Datenbankserveroption - ep](#)“ auf Seite 233.

**Vorsicht**

Achten Sie bei stark verschlüsselten Datenbanken darauf, eine Kopie des Schlüssels an einem sicheren Ort zu verwahren. Wenn Sie den Chiffrierschlüssel verlieren, gibt es keine Möglichkeit, auf die Daten zuzugreifen, auch nicht mit Unterstützung durch den technischen Support. Sie müssen die Datenbank verwerfen und eine neue Datenbank erstellen.

## Chiffrierschlüssel für Datenbanken ändern

Sie können den Chiffrierschlüssel für eine verschlüsselte Datenbank oder für eine Datenbank, in der die Tabellenverschlüsselung aktiviert ist, mithilfe der CREATE ENCRYPTED DATABASE-Anweisung ändern. Das Ändern des Chiffrierschlüssels überschreibt nicht die vorhandene Datei, sondern erstellt eine Kopie der Datei, die mit dem neuen Schlüssel verschlüsselt wird.

### Voraussetzungen

Standardmäßig benötigen Sie zum Ausführen der CREATE ENCRYPTED DATABASE-Anweisung das SERVER OPERATOR-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gu geändert werden.

### Aufgabe

- Ändern Sie den Chiffrierschlüssel für eine verschlüsselte Datenbank mit der CREATE ENCRYPTED DATABASE-Anweisung.

### Ergebnisse

Der Chiffrierschlüssel wird geändert.

### Beispiel

Im folgenden Beispiel wird eine Kopie der Datenbankdatei *encryptedtemp.db*, die mit dem Schlüssel "abc" verschlüsselt ist, unter dem Namen *mynewencryptedtemp.db* erstellt und mit dem Schlüssel "abc123" verschlüsselt. Andere zu der Datenbank gehörende Dateien (Transaktionslog, Transaktionslogspiegel und DBSpace-Dateien) werden ebenfalls mit dem neuen Chiffrierschlüssel erstellt.

```
CREATE ENCRYPTED DATABASE 'C:\temp\mynewencryptedtemp.db'
FROM 'C:\temp\encryptedtemp.db'
KEY 'abc123'
ALGORITHM 'AES'
OLD KEY 'abc';
```

### Siehe auch

- „CREATE ENCRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Sicherheits- und Performanceprobleme

Die Performance von SQL Anywhere ist langsamer, wenn die Datenbank verschlüsselt ist. Die Auswirkungen auf die Performance hängen davon ab, wie häufig Seiten vom Plattenspeicher gelesen bzw.

darauf geschrieben werden. Sie können minimiert werden, sofern gewährleistet ist, dass der Server eine angemessene Cachegröße benutzt.

Mit der Option -c können Sie beim Serverstart die Anfangsgröße für den Cache erhöhen. Bei Betriebssystemen, die die dynamische Cachegrößenanpassung unterstützen, kann die verwendete Cachegröße durch die verfügbare Speichergröße beeinträchtigt werden. Erhöhen Sie den verfügbaren Speicher, damit mehr Speicher zur Verfügung steht.

#### Siehe auch

- „Tipp: Performance durch den Einsatz des Cachespeichers steigern“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]
- „Datenbankserveroption -c “ auf Seite 217

## Spalten- und Tabellenverschlüsselung

Wenn Sie nur Teile Ihrer Datenbank verschlüsseln möchten, können Sie wählen, Spalten oder Tabellen zu verschlüsseln.

Die Spaltenverschlüsselung kann jederzeit für jede Spalte in jeder Tabelle vorgenommen werden. Die Tabellenverschlüsselung erfordert, dass die Tabellenverschlüsselungsoption für die Datenbank aktiviert ist. Die Tabellenverschlüsselungsoption wird bei der Erstellung der Datenbank (Initialisierung) aktiviert.

- **Tabellen verschlüsseln** Sie können Folgendes verwenden:
  - Dienstprogramm Initialisierung (dbinit;). Siehe „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927.
  - CREATE DATABASE-Anweisung. Siehe „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
  - ALTER DATABASE-Anweisung. Siehe „ALTER DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
  - CREATE ENCRYPTED TABLE DATABASE-Anweisung. Siehe „CREATE ENCRYPTED DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- **Spalten verschlüsseln** ENCRYPT-Funktion. Siehe „ENCRYPT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].
- **Materialisierte Ansichten verschlüsseln** ALTER MATERIALIZED VIEW-Anweisung. Siehe „ALTER MATERIALIZED VIEW-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

#### Siehe auch

- „Tabellenverschlüsselung in Datenbank aktivieren (Dienstprogramm dbinit)“ auf Seite 1440
- „Tabellenverschlüsselung in Datenbanken aktivieren (SQL)“ auf Seite 1438
- „Spaltenverschlüsselung“ auf Seite 1435
- „Ver- und Entschlüsseln einer materialisierten Ansicht“ [*SQL Anywhere Server - SQL-Benutzerhandbuch*]

## Spaltenverschlüsselung

Wenn Sie Spalten in Ihrer Datenbank verschlüsseln möchten, verwenden Sie die ENCRYPT-Funktion. Die ENCRYPT-Funktion verwendet den starken Verschlüsselungsalgorithmus AES, der bei der Datenbankverschlüsselung eingesetzt wird, um übergebene Werte zu verschlüsseln.

Verschlüsselte Daten können mit der DECRYPT-Funktion entschlüsselt werden. Sie müssen denselben Schlüssel verwenden, der in der ENCRYPT-Funktion angegeben wurde. Beide Funktionen geben LONG BINARY-Werte zurück. Wenn Sie einen anderen Datentyp benötigen, können Sie die CAST-Funktion verwenden, um den Wert in den erforderlichen Datentyp zu konvertieren.

Die Funktionen ENCRYPT und DECRYPT unterstützen auch RAW-Verschlüsselung. Sie können Daten im Datenbankserver in einem Format verschlüsseln, das exportiert und außerhalb des Servers entschlüsselt werden kann.

Wenn Datenbankbenutzer auf die Daten in entschlüsselter Form zugreifen müssen, Sie aber ihnen keinen Zugriff auf den Chiffrierschlüssel geben wollen, können Sie eine Ansicht erstellen, die die DECRYPT-Funktion verwendet. Dadurch können Benutzer auf die entschlüsselten Daten zugreifen, ohne den Chiffrierschlüssel zu kennen. Wenn Sie eine Ansicht oder gespeicherte Prozedur erstellen, die die Tabelle verwendet, können Sie den SET HIDDEN-Parameter der ALTER VIEW- und ALTER PROCEDURE-Anweisungen verwenden, um zu gewährleisten, dass Benutzer nicht auf den Chiffrierschlüssel zugreifen können, wenn sie die Views- oder Prozedurdefinition abrufen.

### Beispiel für Spaltenverschlüsselung

Im folgenden Beispiel werden Trigger verwendet, um eine Spalte zu verschlüsseln, die Kennwörter in einer Tabelle namens user\_info speichert. Die user\_info-Tabelle wird folgendermaßen festgelegt:

```
CREATE TABLE user_info (
    employee_ID INTEGER NOT NULL PRIMARY KEY,
    user_name CHAR(80),
    user_pwd CHAR(80) );
```

Zwei Trigger werden der Datenbank hinzugefügt, um den Wert in der user\_pwd-Spalte zu verschlüsseln, wenn entweder ein neuer Benutzer hinzugefügt oder das Kennwort eines vorhandenen Benutzers aktualisiert wird.

- Der Trigger encrypt\_new\_user\_pwd wird jedes Mal ausgelöst, wenn der user\_info-Tabelle eine neue Zeile hinzugefügt wird.

```
CREATE TRIGGER encrypt_new_user_pwd
BEFORE INSERT
ON user_info
REFERENCING NEW AS new_pwd
FOR EACH ROW
BEGIN
    SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
END;
```

- Der Trigger encrypt\_updated\_pwd wird jedes Mal ausgelöst, wenn die user\_pwd-Spalte in der user\_info-Tabelle aktualisiert wird.

```
CREATE TRIGGER encrypt_updated_pwd
BEFORE UPDATE OF user_pwd
ON user_info
```

```
REFERENCING NEW AS new_pwd
FOR EACH ROW
BEGIN
    SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
END;
```

Fügen Sie einen neuen Benutzer der Datenbank hinzu:

```
INSERT INTO user_info
VALUES ( '1', 'd_williamson', 'abc123');
```

Wenn Sie eine SELECT-Anweisung ausgeben, um die Informationen in der Tabelle user\_info anzuzeigen, ist der Wert in der Spalte user\_pwd binär (die verschlüsselte Form des Kennworts) und nicht der Wert "abc123", der in der INSERT-Anweisung angegeben wurde.

Wenn das Kennwort dieses Benutzers geändert wurde, wird der encrypt\_updated\_pwd-Trigger ausgelöst und in der user\_pwd-Spalte wird die verschlüsselte Form des neuen Kennworts angezeigt.

```
UPDATE user_info
SET user_pwd='xyz'
WHERE employee_ID='1';
```

Das ursprüngliche Kennwort kann abgefragt werden, indem die folgende SQL-Anweisung ausgegeben wird. Diese Anweisung verwendet die DECRYPT-Funktion und den Chiffrierschlüssel, um die Daten zu entschlüsseln, sowie die CAST-Funktion, um den Wert von einem LONG BINARY- in einen CHAR-Wert zu konvertieren:

```
SELECT CAST (
    DECRYPT( user_pwd, '8U3dkA' )
    AS CHAR(100))
FROM user_info
WHERE employee_ID = '1';
```

### Siehe auch

- „RAW-Verschlüsselung“ auf Seite 1436
- „CAST-Funktion [Datentypkonvertierung]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER PROCEDURE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER VIEW-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ENCRYPT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DECRYPT-Funktion [Zeichenfolge]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

### RAW-Verschlüsselung

Die RAW-Verschlüsselung ermöglicht es Ihnen, Daten im Datenbankserver in einem Format zu verschlüsseln, das exportiert und außerhalb des Datenbankservers entschlüsselt werden kann. Das verschlüsselte Format wird als **RAW** bezeichnet. Wenn Sie Daten im RAW-Format verschlüsseln möchten, müssen Sie den Chiffrierschlüssel angeben, den Initialisierungsvektor und optional ein Format zum Auffüllen mit Zeichen. Zum Entschlüsseln der Daten müssen Sie dieselben Parameterwerte angeben.

Sie können auch die DECRYPT-Funktion verwenden, um die Daten im Datenbankserver zu entschlüsseln.

Die RAW-Verschlüsselung ist in folgenden Fällen nützlich:

- **Sie möchten Datenbankbenutzer am Zugriff auf die Daten hindern** Sie können mit der RAW-Verschlüsselung sensible Daten verschlüsseln, auf die sogar Ihre Datenbankadministratoren keinen Zugriff haben sollen, und anschließend die Daten mithilfe einer Clientanwendung entschlüsseln, ohne den Datenbankserver zu verwenden. Die RAW-Verschlüsselung ist nicht empfehlenswert, wenn die Daten nur durch den Datenbankserver verschlüsselt und entschlüsselt werden dürfen.
- **Sie können keine TLS-Verschlüsselung verwenden** Sie können RAW-Verschlüsselung statt TLS-Verschlüsselung verwenden. Im Gegensatz zur TLS-Verschlüsselung kann die RAW-Verschlüsselung jedoch keine Wiedergabe- oder Mittelsmannangriffe verhindern und auch keine Datenbankserver authentifizieren.

### Beispiel

Sie müssen Daten aus der `binary_data`-Spalte der Tabelle "SensitiveData" in Ihrer Datenbank an einen Client ohne Datenbanken senden. Da die Daten sensibel sind, verschlüsseln Sie die Daten mit der folgenden SQL-Anweisung im RAW-Format:

```
SELECT ENCRYPT( binary_data, 'TheEncryptionKey', 'AES(FORMAT=RAW)',
  'ThisIsTheIV' )FROM SensitiveData;
```

Sie kopieren die verschlüsselten Daten auf den Client, zusammen mit einer Anwendung zum Entschlüsseln des Inhalts. Außerdem geben Sie den Chiffrierschlüssel (TheEncryptionKey) und den Initialisierungsvektor (ThisIsTheIV) an, die der Client für die Anwendung verwenden soll. Der Client verwendet die Anwendung, um die Daten zu entschlüsseln und anzuzeigen.

### Siehe auch

- „[ENCRYPT-Funktion \[Zeichenfolge\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „[DECRYPT-Funktion \[Zeichenfolge\]](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Tabellenverschlüsselung

Mit der Tabellenverschlüsselung können Sie Tabellen oder materialisierte Ansichten mit vertraulichen Daten ohne jene Performanceauswirkungen verschlüsseln, die bei einer Verschlüsselung der gesamten Datenbank möglicherweise auftreten. Wenn die Tabellenverschlüsselung aktiviert ist, werden Tabellenseiten für die verschlüsselte Tabelle, die damit verbundenen Indexseiten und Seiten in temporären Dateien verschlüsselt. Die Transaktionslogseiten, die Transaktionen für verschlüsselte Tabellen enthalten, werden ebenfalls verschlüsselt.

Um Tabellen in Ihrer Datenbank zu verschlüsseln, muss die Tabellenverschlüsselung aktiviert sein. Die Aktivierung der Tabellenverschlüsselung wird während der Datenbankinitialisierung durchgeführt. Um zu bestimmen, ob die Tabellenverschlüsselung aktiviert ist, fragen Sie die Datenbankeigenschaft `EncryptionScope` unter Verwendung der `DB_PROPERTY`-Funktion folgendermaßen ab:

```
SELECT DB_PROPERTY( 'EncryptionScope' );
```

Wenn der Rückgabewert `TABLE` ist, ist die Tabellenverschlüsselung aktiviert.

Um den für die Tabellenverschlüsselung verwendeten Verschlüsselungsalgorithmus anzuzeigen, fragen Sie die Datenbankeigenschaft `Encryption` unter Verwendung der `DB_PROPERTY`-Funktion folgendermaßen ab:

```
SELECT DB_PROPERTY( 'Encryption' );
```

## Performance-Auswirkungen der Tabellenverschlüsselung

Bei verschlüsselten Tabellen werden die Tabellenseiten verschlüsselt, wenn sie auf die Festplatte geschrieben werden, und entschlüsselt, wenn sie von der Festplatte gelesen werden. Dieser Prozess ist für Anwendungen unsichtbar. Es können allerdings leichte Performance-Einbußen auftreten, wenn von verschlüsselten Tabellen gelesen bzw. in sie geschrieben wird. Das Verschlüsseln oder Entschlüsseln bestehender Tabellen kann, abhängig von der Größe der Tabelle, lange dauern.

Indexseiten für Indizes auf Spalten in einer verschlüsselten Tabelle werden ebenfalls verschlüsselt, wie auch Transaktionslogseiten, die Transaktionen der verschlüsselten Tabelle enthalten, und alle Seiten in der temporären Datei für die Datenbank. Alle anderen Datenbank- und Transaktionslogseiten sind unverschlüsselt.

Verschlüsselte Tabellen können komprimierte Spalten enthalten. In diesem Fall werden Daten komprimiert, bevor sie verschlüsselt werden.

Verschlüsselte Tabellen wirken sich nicht auf die Speicheranforderungen aus.

## Eine Datenbank mit aktivierter Tabellenverschlüsselung starten

Das Starten einer Datenbank, bei der Tabellenverschlüsselung aktiviert ist, entspricht dem Starten einer verschlüsselten Datenbank. Wenn die Datenbank z.B. mit der Option -ek gestartet wird, muss ein Schlüssel angegeben werden. Wenn die Datenbank mit der Option -ep gestartet wird, werden Sie zur Eingabe des Schlüssels aufgefordert.

## Siehe auch

- „Ver- und Entschlüsseln einer materialisierten Ansicht“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „Datenbankverschlüsselung und -entschlüsselung“ auf Seite 1424
- „Dienstprogramm Initialisierung (dbinit)“ auf Seite 927
- „Datenbankserveroption -ep“ auf Seite 233
- „Methoden zur Datenbankverschlüsselung“ auf Seite 1426
- „Datenbanken erstellen (Sybase Central)“ auf Seite 125
- „Datenbanken erstellen (Dienstprogramm dbinit)“ auf Seite 126
- „ALTER TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE ENCRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE DECRYPTED DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Tabellenverschlüsselung in Datenbanken aktivieren (SQL)

Erstellen Sie mithilfe der CREATE DATABASE-Anweisung eine Datenbank mit Tabellenverschlüsselung oder aktivieren Sie mithilfe der CREATE ENCRYPTED TABLE DATABASE-Anweisung die Tabellenverschlüsselung in einer vorhandenen Datenbank.

## Voraussetzungen

Standardmäßig benötigen Sie zum Ausführen der Anweisungen CREATE DATABASE und CREATE ENCRYPTED TABLE DATABASE das SERVER OPERATOR-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gu geändert werden.

## Kontext und Bemerkungen

Die Tabellenverschlüsselung muss bei der Datenbankerstellung aktiviert und konfiguriert werden. Wenn in Ihrer Datenbank die Tabellenverschlüsselung nicht aktiviert ist oder wenn eine Datenbankverschlüsselung in Kraft ist, erstellt die CREATE ENCRYPTED TABLE DATABASE-Anweisung eine Kopie der Datenbank mit aktivierter Tabellenverschlüsselung und überschreibt nicht die ursprüngliche Datenbankdatei.

## Aufgabe

- Erstellen Sie eine Datenbank mit Tabellenverschlüsselung oder aktivieren Sie die Tabellenverschlüsselung in einer vorhandenen Datenbank.

Option	Aktion
Datenbank mit Tabellenverschlüsselung erstellen	Erstellen Sie mit der CREATE DATABASE-Anweisung eine Datenbank und geben Sie einen Schlüssel und einen Verschlüsselungsalgorithmus an.
Tabellenverschlüsselung für eine vorhandene Datenbank aktivieren	Erstellen Sie mit der CREATE ENCRYPTED TABLE DATABASE-Anweisung eine Kopie der Datenbank und geben Sie einen Schlüssel an.

## Ergebnisse

Die Tabellenverschlüsselung wird aktiviert.

## Nächste Schritte

Sie erstellen eine verschlüsselte Tabelle mithilfe der CREATE TABLE-Anweisung oder durch entsprechendes Ändern einer vorhandenen Tabelle mithilfe der ALTER TABLE-Anweisung. Wenn Sie eine Tabelle verschlüsseln, wird der beim Aktivieren der Tabellenverschlüsselung angegebene Schlüssel bzw. Algorithmus verwendet.

## Beispiel

Der folgende Befehl erstellt die Datenbank *mynewdemo.db*, in der die starke Verschlüsselung für Tabellen aktiviert ist, wobei der Schlüssel "abc" und der AES256\_FIPS-Verschlüsselungsalgorithmus verwendet werden. Außerdem wird eine DBA-Benutzer-ID mit dem Kennwort "sql" erstellt.

```
CREATE DATABASE 'C:\temp\mynewdemo.db'  
  DBA USER 'DBA' DBA PASSWORD 'sql'  
  ENCRYPTED TABLE  
  KEY 'abc'  
  ALGORITHM 'AES256_FIPS';
```

Im folgenden Beispiel wird eine Datenbank namens "contacts2" aus der bestehenden Datenbank "contacts1" erstellt. Die neue Datenbank unterstützt verschlüsselte Tabellen.

```
CREATE ENCRYPTED TABLE DATABASE 'C:\temp\contacts2.db'  
FROM 'C:\temp\contacts1.db'  
KEY 'Sd8f6654'  
OLD KEY 'Sc8e5543';
```

### Siehe auch

- „CREATE DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE ENCRYPTED DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Tabellenverschlüsselung in Datenbank aktivieren (Dienstprogramm dbinit)

Sie können die Tabellenverschlüsselung während der Erstellung einer Datenbank mit der Befehlszeile aktivieren.

### Voraussetzungen

Die Tabellenverschlüsselung wird zum Zeitpunkt der Tabellenerstellung aktiviert und konfiguriert. Sie müssen die Datenbank mit aktivierter Tabellenverschlüsselung neu erstellen, wenn bei Ihrer Datenbank Tabellenverschlüsselung nicht aktiviert ist oder wenn eine Datenbankverschlüsselung vorhanden ist.

### Aufgabe

- Erstellen Sie eine Datenbank mit den dbinit-Optionen -et und -ek und geben Sie einen Schlüssel und einen Verschlüsselungsalgorithmus an.

### Ergebnisse

Die Tabellenverschlüsselung wird aktiviert.

### Beispiel

Der folgende Befehl erstellt die Datenbank *new.db*, in der die starke Verschlüsselung für Tabellen aktiviert ist, wobei der Schlüssel "abc" und der AES256\_FIPS-Verschlüsselungsalgorithmus verwendet werden, und setzt die DBA-Benutzer-ID auf "DBA" mit dem Kennwort "sql":

```
dbinit -dba DBA,sql new.db -et -ek abc -ea AES256_FIPS
```

Wenn Sie später eine Tabelle in dieser Datenbank verschlüsseln, werden der AES256\_FIPS-Algorithmus und der Schlüssel "abc" verwendet.

## Tabellen verschlüsseln

Sie können eine verschlüsselte Tabelle mit der CREATE TABLE-Anweisung erstellen oder eine vorhandene Tabelle mit der ALTER TABLE-Anweisung verschlüsseln.

## Voraussetzungen

Wenn Sie die CREATE TABLE-Anweisung verwenden möchten, müssen Sie eines der folgenden Systemprivilegien haben:

- CREATE TABLE
- CREATE ANY TABLE
- CREATE ANY OBJECT

Wenn Sie die ALTER TABLE-Anweisung verwenden möchten, müssen Sie Eigentümer der zu ändernden Tabelle sein oder eines der folgenden Privilegien haben:

- ALTER-Privileg für die Tabelle
- ALTER ANY TABLE
- ALTER ANY OBJECT

Um Tabellen in Ihrer Datenbank zu verschlüsseln, muss Verschlüsselung in der Datenbank bereits aktiviert sein.

## Kontext und Bemerkungen

Wenn Sie eine Tabelle verschlüsseln, werden der Verschlüsselungsalgorithmus und der Chiffrierschlüssel verwendet, die bei der Erstellung der Datenbank angegeben wurden.

## Aufgabe

- Sie können entweder eine Tabelle mit Verschlüsselung erstellen oder eine vorhandene Tabelle verschlüsseln.

Option	Aktion
Tabelle mit Verschlüsselung erstellen	Erstellen Sie eine Tabelle unter Verwendung der ENCRYPTED-Klausel der CREATE TABLE-Anweisung.
Vorhandene Tabelle verschlüsseln	Verschlüsseln Sie eine Tabelle mit der ENCRYPTED-Klausel der ALTER TABLE-Anweisung.

## Ergebnisse

Die Tabelle wird verschlüsselt.

## Beispiel

Der folgende Befehl erstellt eine verschlüsselte Tabelle namens MyEmployees:

```
CREATE TABLE MyEmployees (
  MemberID CHAR(40),
  CardNumber INTEGER )
ENCRYPTED;
```

Die folgenden Anweisungen erstellen eine Tabelle namens "MyEmployees2" und verschlüsseln sie.

```
CREATE TABLE MyEmployees2 (  
    MemberID CHAR(40),  
    CardNumber INTEGER );  
ALTER TABLE MyEmployees2  
    ENCRYPTED;
```

#### Siehe auch

- „Tabellenverschlüsselung in Datenbanken aktivieren (SQL)“ auf Seite 1438
- „Tabellenverschlüsselung in Datenbank aktivieren (Dienstprogramm dbinit)“ auf Seite 1440
- „CREATE TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER TABLE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Datenbanksicherheit unter Windows Mobile

Viele der SQL Anywhere-Sicherheitsfunktionen für Windows PC-Plattformen werden von Windows Mobile unterstützt, wie die Datenbankdateiverschlüsselung und die einfache Kommunikationsverschlüsselung, oder sie verfügen über eine modifizierte Unterstützung, wie das Dienstprogramm zur Logkonvertierung.

Unter Windows Mobile laufende Datenbanken verwenden dieselben Funktionen zur Benutzeridentifizierung und -autorisierung wie Datenbanken auf Windows-Desktop-Plattformen. Diese Funktionen steuern, wer auf die Datenbank zugreifen kann und welche Aktionen diese Benutzer ausführen können.

### Sicherheit von Windows Mobile-Geräten

Wenn Sie vertrauliche Daten auf Ihrem Windows Mobile-Gerät speichern, sollten Sie die Sicherheitsfunktionen verwenden, die für Ihr Windows Mobile-Gerät zur Verfügung stehen.

Weitere Informationen zu verfügbaren Sicherheitsfunktionen finden Sie im Bedienerhandbuch, das mit Ihrem Windows Mobile-Gerät mitgeliefert wird.

### Datenbankserveroptionen

Mit den Serveroptionen können Sie steuern, wer bestimmte Aktionen auf dem Server durchführen kann.

Diese Optionen werden im Dialogfeld **Server-Startoptionen** im Feld "Optionen" festgelegt, wenn Sie die Datenbank auf Ihrem Windows Mobile-Gerät starten.

### Auditing

Diese Funktion benutzt das Transaktionslog, um eine detaillierte Aufzeichnung aller in der Datenbank durchgeführten Vorgänge zu führen.

Das Dienstprogramm zur Logkonvertierung (dbtran) wird verwendet, um die im Transaktionslog enthaltenen Informationen, darunter auch Audit-Daten, zu übersetzen. Das Dienstprogramm dbtran wird unter Windows Mobile nicht unterstützt. Daher können Sie ein auf einem Windows Mobile-Gerät gespeichertes Log nicht konvertieren. Kopieren Sie die Transaktionslogdatei auf Ihren PC, um dieses Dienstprogramm zu benutzen.

## Datenbankverschlüsselung unter Windows Mobile

Mit diesen Funktionen können Sie die Stufe der Datenbankverschlüsselung wählen. Sie können Ihre Datenbank entweder mit einfacher Verschlüsselung oder mit starker Verschlüsselung chiffrieren. SQL Anywhere unterstützt unter Windows Mobile sowohl die einfache als auch die starke Verschlüsselung.

**Einfache Verschlüsselung** Diese Art der Verschlüsselung ist gleichbedeutend mit einem Verschleiern und erschwert das Dechiffrieren der Daten in Ihrer Datenbank mithilfe eines Festplatten-Dienstprogramms. Bei der einfachen Verschlüsselung wird kein Schlüssel benötigt, um die Datenbank zu chiffrieren.

Die Technologie der einfachen Verschlüsselung wird in früheren Versionen von SQL Anywhere unterstützt.

**Starke Verschlüsselung** Bei dieser Art der Verschlüsselung werden die Daten in Ihren Datenbank- und Transaktionslogdateien verschleiert, damit sie nicht direkt von der Festplatte gelesen werden können. Bei starker Verschlüsselung wird ohne den Schlüssel der Zugriff auf die Datenbank vollständig verwehrt. Unter Windows Mobile werden die AES\_FIPS- und AES256\_FIPS-Algorithmen nur mit ARM-Prozessoren unterstützt.

## Verschlüsselung der Kommunikation und Windows Mobile

Sie können die Client/Server-Kommunikation verschlüsseln und damit während der Übertragung im Netzwerk eine erhöhte Sicherheit gewährleisten. SQL Anywhere stellt zwei Typen von Kommunikationsverschlüsselung zur Verfügung: einfache und starke.

Bei der einfachen Kommunikationsverschlüsselung werden Kommunikationspakete angenommen, die mit der einfachen Verschlüsselung chiffriert wurden. Diese Stufe der Kommunikationsverschlüsselung wird von allen Plattformen unterstützt, einschließlich Windows Mobile und früheren Versionen von SQL Anywhere.

Die starke Kommunikationsverschlüsselung ist unter Windows Mobile nicht verfügbar.

## Siehe auch

- [„Hinweise zur Sicherheit: Benutzer-IDs“ auf Seite 1409](#)
- [„Privilegien über die Befehlszeile steuern“ auf Seite 170](#)
- [„Serveroptionen unter Windows Mobile“ auf Seite 451](#)
- [„Audits von Datenbankaktivitäten“ auf Seite 1416](#)
- [„Datenbankverschlüsselung und -entschlüsselung“ auf Seite 1424](#)
- [„Verbindungsparameter Encryption \(ENC\)“ auf Seite 359](#)

# Transportschichtsicherheit

## Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

Transportschichtsicherheit ist ein IETF-Standardprotokoll, das die Client/Server-Kommunikation mithilfe von digitalen Zertifikaten und Verschlüsselung mit öffentlichen Schlüsseln schützt. Transportschichtsicherheit aktiviert Verschlüsselung, Manipulationserkennung und Zertifikat-basierte Authentifizierung.

Sie können die Transportschichtsicherheit für folgende Aufgaben verwenden:

- Die Kommunikation zwischen dem SQL Anywhere-Datenbankserver und Clientanwendungen sichern
- Die Kommunikation zwischen dem MobiLink-Server und MobiLink-Clients sichern
- Einen sicheren SQL Anywhere-Webserver einrichten

Eine sichere Kommunikation beginnt mit einem Austausch von Meldungen (einem Handshake), wie:

- **Serverauthentifizierung** Transportschichtsicherheit verwendet Serverzertifikate, um eine sichere Verbindung einzurichten und aufrecht zu erhalten. Sie erstellen eindeutige Zertifikatsdateien für jeden Server. Sie können die Serverauthentifizierung für die SQL Anywhere Server-/Client-Kommunikation oder für die MobiLink-Synchronisation verwenden:
  - Bei der SQL Anywhere Server-/Client-Kommunikation verifiziert ein Datenbankclient die Identität eines SQL Anywhere-Datenbankservers.
  - Bei der MobiLink-Synchronisation verifiziert ein MobiLink-Client (SQL Anywhere oder UltraLite) die Identität eines MobiLink-Servers.

## Wirkungsgrad

Das Transportschichtsicherheits-Protokoll verwendet eine Kombination der Verschlüsselungsmethoden mit öffentlichen Schlüsseln und mit symmetrischen Schlüsseln. Die Verschlüsselung mit öffentlichen Schlüsseln bietet bessere Authentifizierungstechniken, wirkt sich jedoch auf die Performance aus. Sobald eine sichere Verbindung hergestellt ist, verwenden der Client und der Server für den Rest ihrer Kommunikation eine äußerst effiziente Chiffre mit einer 128-Bit-Schlüsselgröße.

## Zertifikate

Verwenden Sie das Dienstprogramm zum Erstellen von Zertifikaten (createcert), um X.509-Zertifikatsdateien für die Transportschichtsicherheit zu erstellen. Wenn Sie allerdings die Existenz von Zertifikaten von Drittanbietern verifizieren müssen oder sicherere Zertifikate benötigen, müssen Sie die Zertifikate von den entsprechenden Zertifizierungsstellen erwerben.

## Verschlüsselung der Datenbankdatei

Hinweise zur Verschlüsselung einer Datenbankdatei finden Sie unter:

- „Datenbankverschlüsselung und -entschlüsselung“
- „Datenbanksicherheit“ [*UltraLite - Datenbankverwaltung*]

## TLS-Unterstützung

### Hinweis

Erforderliche getrennt lizenzierbare Komponenten.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Alle Technologien für starke Verschlüsselungen unterliegen Exportbestimmungen.

Siehe „Getrennt lizenzierbare Komponenten“ [*SQL Anywhere 16 - Einführung*].

In diesem Thema wird die Unterstützung für RSA-Verschlüsselung und FIPS-zertifizierte Verschlüsselung beschrieben. Die TLS-Versionen 1.0 und 1.1 werden unterstützt.

### RSA-Verschlüsselung

Die RSA-Verschlüsselung wird mit SQL Anywhere mitgeliefert und kann für die Client/Server-Kommunikation, die Synchronisation und für Webdienste verwendet werden. Die kostenlose Version ist nicht FIPS-zertifiziert. Um eine FIPS-zertifizierte RSA-Verschlüsselung zu implementieren, benötigen Sie eine getrennte Lizenz.

Eine Liste der unterstützten Plattformen für RSA finden Sie unter <http://www.sybase.com/detail?id=1061806>.

### FIPS-zertifizierte Verschlüsselung

FIPS-zertifizierte Verschlüsselung ist nur für RSA-Verschlüsselung verfügbar.

FIPS-zertifizierte Verschlüsselung erfordert eine separate Lizenz. Siehe „Getrennt lizenzierbare Komponenten“ [*SQL Anywhere 16 - Einführung*].

Eine Liste der FIPS-zertifizierten Komponenten finden Sie unter <http://www.sybase.com/detail?id=1061806>.

## FIPS-zertifizierte Verschlüsselungstechnologie

Sie können mit FIPS-zertifizierten Sicherheitsalgorithmen Ihre Datenbankdateien bzw. Datenbankclient/Server- und Webdienste- sowie MobiLink-Client/Server-Kommunikation verschlüsseln.

FIPS 140-2 (Federal Information Processing Standard, FIPS) legt die Anforderungen für Sicherheitsalgorithmen fest. FIPS 140-2 wird von der amerikanischen und kanadischen Regierung durch das National Institute of Standards and Testing (NIST) und das Canadian Communication Security Establishment (CSE) erteilt.

SQL Anywhere verwendet für die Verschlüsselung ein FIPS-zertifiziertes Modul von Certicom. Unter Windows (Desktop und Windows Mobile) sowie Unix benutzt SQL Anywhere Certicom Security Builder GSE (FIPS Module v2.0). Dies ist Nummer 542 auf der Seite <http://csrc.nist.gov/cryptval/140-1/140val-all.htm>.

## FIPS erzwingen

Optional können Sie die Verwendung von FIPS-zertifizierter Verschlüsselung auf dem Client oder Server mit einer FIPS-Option erzwingen. Wenn Sie die FIPS-Option auf "On" setzen, muss die gesamte gesicherte Kommunikation FIPS-zertifiziert sein. Wenn ein Benutzer nicht FIPS-zertifizierte RSA-Verschlüsselung verwendet, wird die Verbindung automatisch auf FIPS-zertifizierte RSA-Verschlüsselung hochgestuft. Sie können die FIPS-Option auf dem Client oder Server setzen, auf dem FIPS-zertifizierte Verschlüsselung erzwungen werden soll. SQL Anywhere- und MobiLink-Server haben eine Befehlszeilenoption `-fips` und Clients haben eine `fips`-Option, die mit dem `encryption`-Verbindungsparameter gesetzt werden kann.

Hinweise zur Verschlüsselung von SQL Anywhere-Datenbankdateien mit FIPS-zertifizierter Verschlüsselung finden Sie unter „Einfache Verschlüsselung und starke Verschlüsselung“ auf Seite 1425.

## Transportschichtsicherheit einrichten

Die folgenden Abschnitte zeigen einen Überblick über die Aufgaben, die für die Einrichtung der Transportschichtsicherheit erforderlich sind.

### 1. Beziehen Sie digitale Zertifikate.

Sie benötigen Identitäts- und Zertifikatsdateien. Die Serveridentitätsdatei enthält den privaten Schlüssel des Servers und sollte gesichert auf dem Datenbankserver oder MobiLink-Server gespeichert werden. Sie verteilen die Zertifikatsdatei des Servers an Ihre Clients.

Sie können Zertifikate von einer Zertifizierungsstelle erwerben oder das Dienstprogramm zum Erstellen von Zertifikaten (`createcert`) verwenden. SQL Anywhere stellt auch eine Funktionalität zum Erstellen von Zertifikaten zu Verfügung, was besonders für das Entwickeln und Testen nützlich ist. Siehe „Digitale Zertifikate“ auf Seite 1447.

### 2. Wenn Sie die Transportschichtsicherheit für SQL Anywhere-Client/Server-Anwendungen einrichten, führen Sie Folgendes aus:

- **SQL Anywhere-Datenbankserver mit Transportschichtsicherheit starten** Mit der Datenbankserveroption `-ec` können Sie den Sicherheitstyp, den Namen der Serveridentitätsdatei und das Kennwort zum Schutz des privaten Schlüssels für den Server festlegen.

Wenn Sie auch unverschlüsselte Verbindungen über Shared Memory zulassen möchten, geben Sie die Option `-es` an.

Siehe „Datenbankserver mit Transportschichtsicherheit“ auf Seite 1454.

- **Clientanwendungen für die Transportschichtsicherheit konfigurieren** Geben Sie mithilfe des `encryption`-Verbindungsparameters `[ENC]` den Pfad und den Dateinamen für die vertrauenswürdigen Zertifikate an.

Siehe „[Konfigurieren der Clientanwendung für die Verwendung der Transportschichtssicherheit](#)“ auf Seite 1455.

3. Wenn Sie die Transportschichtssicherheit für SQL Anywhere-Webdienste einrichten, führen Sie Folgendes aus:

- **SQL Anywhere-Datenbankserver mit Transportschichtssicherheit starten** Mit der Datenbankserveroption -xs können Sie den Sicherheitstyp, den Serveridentitätsdateinamen und das Kennwort zum Schutz des privaten Serverschlüssels festlegen. Siehe „[Datenbankserveroption -xs](#)“ auf Seite 310.
- **Konfigurieren Sie Browser oder andere Webclients so, dass sie Zertifikaten vertrauen.** Verschlüsseln Sie SQL Anywhere-Webdienste.

Siehe „[Verschlüsselung für SQL Anywhere-Webdienste](#)“ auf Seite 1458.

4. Wenn Sie die Transportschichtssicherheit für die MobiLink-Synchronisation einrichten, führen Sie Folgendes aus:

- **Den MobiLink-Server mit Transportschichtssicherheit starten** Mit der mlsrv16-Option -x können Sie den Sicherheitsdatenstrom, den Namen der Serveridentitätsdatei und das Kennwort zum Schutz des privaten Schlüssels für den Server festlegen.

Siehe „[Den MobiLink-Server mit Transportschichtssicherheit starten](#)“ auf Seite 1460.

- **MobiLink-Clients für die Verwendung von Transportschichtssicherheit konfigurieren** Geben Sie die entsprechenden Sicherheits- bzw. Netzwerkprotokolloptionen mit dem MobiLink-Client-Synchronisationsprogramm (dbmlsync) oder der UltraLite-Anwendung an. Geben Sie den Sicherheitsdatenstrom und vertrauenswürdige Serverzertifikatsdateinamen an.

Siehe „[Konfigurieren von MobiLink-Clients für die Verwendung von Transportschichtssicherheit](#)“ auf Seite 1461.

## Digitale Zertifikate

Sie benötigen digitale Zertifikate, um Transportschichtssicherheit einzurichten. Sie können Zertifikate entweder von einer Zertifizierungsstelle beziehen oder mit dem Dienstprogramm zum Erstellen von Zertifikaten (createcert) erstellen.

### Dienstprogramm zum Erstellen von Zertifikaten

Sie können das Dienstprogramm zum Erstellen von Zertifikaten (createcert) verwenden, um X.509-Zertifikatsdateien mithilfe von RSA zu generieren. Siehe „[Dienstprogramm zum Erstellen von Zertifikaten \(createcert\)](#)“ auf Seite 894.

### Dienstprogramm zum Anzeigen von Zertifikaten

Sie können das Dienstprogramm zum Anzeigen von Zertifikaten (viewcert) verwenden, um X.509-Zertifikate mithilfe von RSA zu lesen. Siehe „[Dienstprogramm zum Anzeigen von Zertifikaten \(viewcert\)](#)“ auf Seite 903.

## Zertifikate für die Serverauthentifizierung

Mit demselben Prozess können Sie Zertifikatsdateien für die Serverauthentifizierung erstellen. Dabei erstellen Sie eine Identitäts- und eine Zertifikatsdatei.

Bei der Serverauthentifizierung erstellen Sie eine Serveridentitätsdatei und eine Zertifikatsdatei, die Sie an Clients verteilen. Siehe „[Unternehmensstammzertifikate](#)“ auf Seite 1451.

## Zertifikatskonfigurationen

Das Zertifikat kann selbstsigniert oder von einer kommerziellen bzw. Unternehmens-Zertifizierungsstelle signiert sein.

- **Selbstsignierte Zertifikate** In einfachen Setups können selbstsignierte Serverzertifikate verwendet werden. Siehe „[Selbstsignierte Stammzertifikate](#)“ auf Seite 1448.
- **Unternehmensstammzertifikate** Ein Unternehmensstammzertifikat kann verwendet werden, um die Datenintegrität und die Erweiterbarkeit zu verbessern, wenn mehrere Server eingesetzt werden.
  - Sie können den privaten Schlüssel, mit dem die Server-Zertifikate signiert werden, an einem sicheren zentralen Ort speichern.
  - Bei der Serverauthentifizierung können Sie MobiLink- oder Datenbankserver hinzufügen, ohne Clients neu zu konfigurieren.

Siehe „[Zertifikatketten](#)“ auf Seite 1449.

- **Kommerzielle Zertifizierungsstellen** Sie können anstelle eines Unternehmensstammzertifikats auch das Zertifikat der Zertifizierungsstelle eines Drittanbieters verwenden. Kommerzielle Zertifizierungsstellen besitzen dedizierte Einrichtungen, um private Schlüssel zu speichern und qualitativ hochwertige Serverzertifikate zu erstellen.

Siehe „[Zertifikatketten](#)“ auf Seite 1449 und „[Global signierte Zertifikate](#)“ auf Seite 1451.

## Selbstsignierte Stammzertifikate

Selbstsignierte Stammzertifikate können für einfache Setups mit nur einem MobiLink- oder Datenbankserver verwendet werden.

### Tipp

Verwenden Sie Zertifikatketten auf Unternehmensebene oder kommerzielle Zertifizierungsstellen, wenn Sie mehrere Serveridentitätsdateien benötigen. Zertifizierungsstellen bieten Erweiterbarkeit und eine höhere Zertifikatintegrität mit entsprechenden Einrichtungen, um private Stammschlüssel zu speichern.

Siehe „[Zertifikatketten](#)“ auf Seite 1449.

- **Certificate** Bei Serverauthentifizierungszertifikaten wird das selbstsignierte Zertifikat an Clients verteilt. Es ist ein elektronisches Dokument, das Identitätsinformationen, den öffentlichen Schlüssel des Servers und eine selbstsignierte digitale Unterschrift enthält.
- **Identitätsdatei** Bei Serverauthentifizierungszertifikaten wird die Identitätsdatei sicher auf einem MobiLink- oder Datenbankserver gespeichert. Sie besteht aus einer Kombination aus dem

selbstsignierten Zertifikat (das an Clients verteilt wird) und dem entsprechenden privaten Schlüssel. Der private Schlüssel ermöglicht es dem MobiLink- bzw. Datenbankserver, beim ersten Handshake vom Client gesendete Nachrichten zu entschlüsseln.

#### Siehe auch

- „Serverauthentifizierung“ auf Seite 1461
- „Datenbankserver mit Transportschichtssicherheit“ auf Seite 1454
- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894

## Zertifikatketten

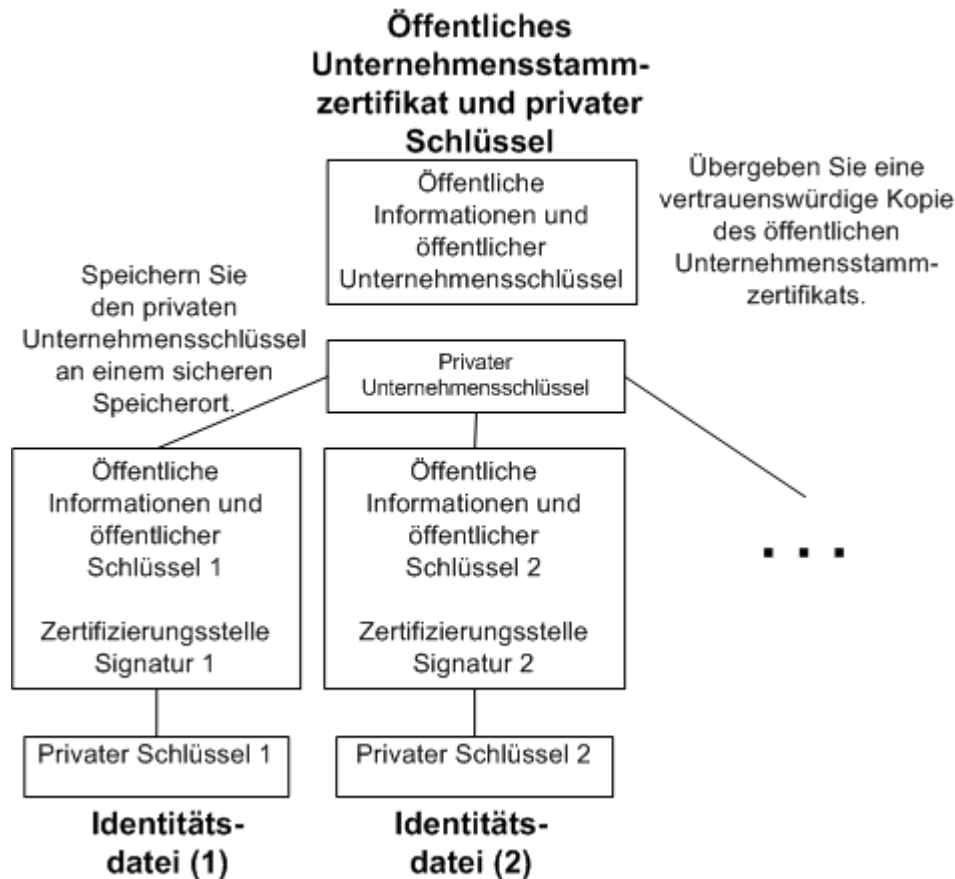
Wenn Sie mehrere Identitätsdateien benötigen, können Sie die Sicherheit und Erweiterbarkeit erhöhen, indem Sie anstelle von selbstsignierten Zertifikaten Zertifikatketten verwenden. Bei Zertifikatketten muss eine Zertifizierungsstelle oder ein Unternehmensstammzertifikat die Identitäten signieren.

#### Vorteile der Verwendung von Zertifikatketten

Zertifikatketten haben folgende Vorteile:

- **Erweiterbarkeit** Bei der Serverauthentifizierung können Sie Clients so konfigurieren, dass sie jedem Zertifikat vertrauen, das von einem Unternehmensstammzertifikat oder einer Zertifizierungsstelle signiert ist. Wenn Sie einen neuen MobiLink- oder Datenbankserver hinzufügen, benötigen die Clients keine Kopie des neuen Zertifikats.
- **Sicherheit** Der private Schlüssel des Unternehmensstammzertifikats befindet sich nicht in der Identitätsdatei. Dadurch, dass der private Schlüssel des Stammzertifikats an einem Hochsicherheitsstandort gespeichert ist bzw. eine Zertifizierungsstelle mit entsprechenden Einrichtungen verwendet wird, kann die Integrität der Serverauthentifizierung erhöht werden.

Im folgenden Diagramm ist die grundlegende Architektur für Unternehmensstammzertifikate dargestellt.



### Zertifikate in einer Umgebung mit mehreren Servern verwenden

Um Zertifikate für eine Umgebung mit mehreren Servern zu erstellen, müssen Sie Folgendes tun:

- Ein öffentliches Unternehmensstammzertifikat und einen privaten Unternehmensschlüssel erstellen.  
Speichern Sie den privaten Unternehmensschlüssel an einem sicheren Ort, vorzugsweise in einer dedizierten Einrichtung.  
Bei der Serverauthentifizierung verteilen Sie das öffentliche Unternehmensstammzertifikat an Clients.
- Verwenden Sie das Unternehmensstammzertifikat, um Identitäten zu signieren.  
Verwenden Sie das öffentliche Unternehmensstammzertifikat und einen privaten Unternehmensschlüssel, um jede Identität zu signieren. Bei der Serverauthentifizierung wird die Identitätsdatei für den Server verwendet.

Sie können auch das Zertifikat der Zertifizierungsstelle eines Drittanbieters verwenden, um Ihre Serverzertifikate zu signieren. Kommerzielle Zertifizierungsstellen besitzen dedizierte Einrichtungen, um private Schlüssel zu speichern und qualitativ hochwertige Serverzertifikate zu erstellen.

### Siehe auch

- „Selbstsignierte Stammzertifikate“ auf Seite 1448
- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894
- „Global signierte Zertifikate“ auf Seite 1451

## Unternehmensstammzertifikate

Unternehmensstammzertifikate verbessern die Datenintegrität und die Erweiterbarkeit, wenn mehrere Server eingesetzt werden.

- Sie können den privaten Schlüssel, mit dem die vertrauenswürdigen Zertifikate erstellt werden, in einer dedizierten Einrichtung speichern.
- Bei der Serverauthentifizierung können Sie Server hinzufügen, ohne Clients neu zu konfigurieren.

Um Unternehmensstammzertifikate einzurichten, erstellen Sie das Unternehmensstammzertifikat und den privaten Unternehmensschlüssel, mit denen Sie Identitäten signieren.

### Siehe auch

- „Signierte Identitätsdateien“ auf Seite 1451
- „Global signierte Zertifikate“ auf Seite 1451

## Signierte Identitätsdateien

Mit einem Unternehmensstammzertifikat können Sie Serveridentitätsdateien signieren.

Bei der Serverauthentifizierung generieren Sie Identitätsdateien für jeden Server. Da diese Zertifikate durch ein Unternehmensstammzertifikat signiert werden, verwenden Sie die createcert-Option -s.

### Siehe auch

- „Dienstprogramm zum Erstellen von Zertifikaten [createcert]“ auf Seite 894

## Global signierte Zertifikate

Eine kommerzielle Zertifizierungsstelle ist eine Organisation, die Zertifikate höchster Qualität erstellt und diese zum Signieren Ihrer Zertifikatanforderungen verwendet.

Global signierte Zertifikate bieten folgende Vorteile:

- Bei der Kommunikation zwischen Unternehmen kann das Vertrauen in eine außenstehende anerkannte Zertifizierungsstelle das Vertrauen in die Sicherheit des Systems verbessern. Eine Zertifizierungsstelle muss die Korrektheit der Identitätsinformationen in von ihr unterzeichneten Zertifikaten garantieren.
- Zertifizierungsstellen bieten kontrollierte Umgebungen und erweiterte Methoden zum Erstellen von Zertifikaten.

- Der private Schlüssel für das Stammzertifikat muss geheim gehalten werden. Ihr Unternehmen verfügt möglicherweise nicht über entsprechende Möglichkeiten, diese sensiblen Daten sicher zu speichern. Eine Zertifizierungsstelle hingegen kann entsprechende Einrichtungen aufbauen und warten.

### Global signierte Zertifikate einrichten

Sie richten global signierte Identitätsdateien mit folgenden Schritten ein:

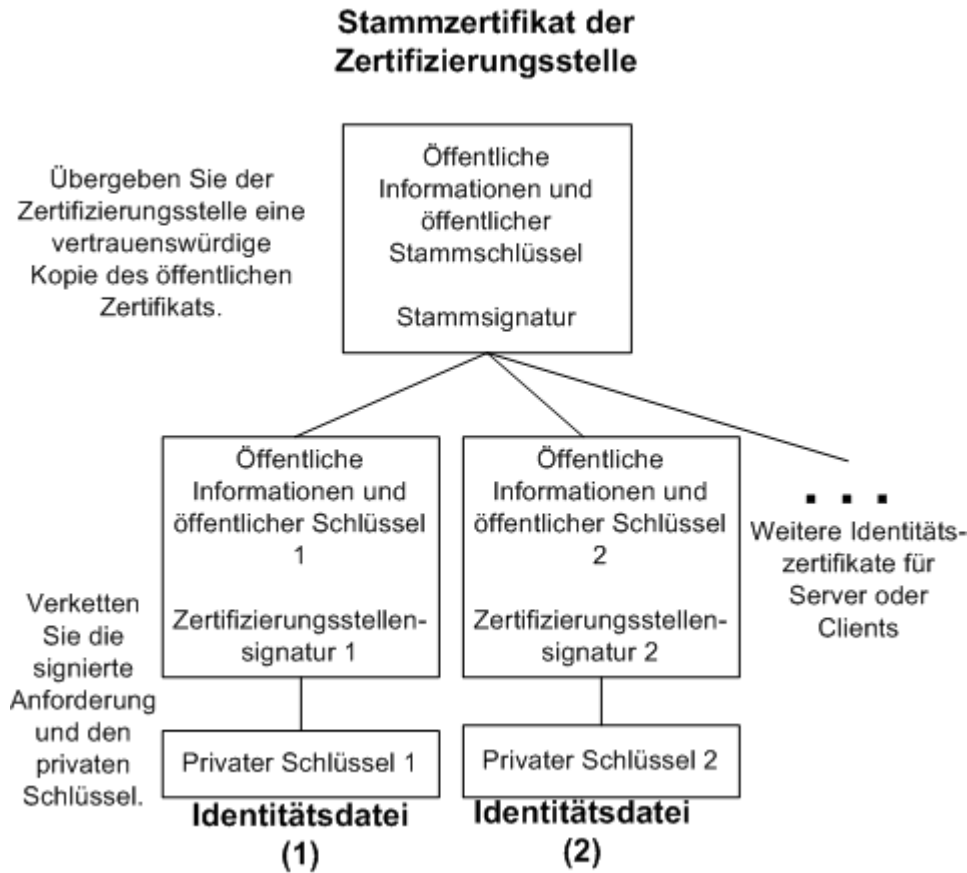
- Erstellen Sie eine Zertifikatanforderung, indem Sie das Dienstprogramm createcert mit der Option -r verwenden. Siehe „[Dienstprogramm zum Erstellen von Zertifikaten \[createcert\]](#)“ auf Seite 894.
- Verwenden Sie eine Zertifizierungsstelle, um jede Anforderung zu signieren. Sie können die signierte Anforderung mit dem entsprechenden privaten Schlüssel kombinieren, um die Serveridentitätsdatei zu erstellen.

#### Hinweis

Sie können möglicherweise auch ein Unternehmensstammzertifikat global signieren. Dies ist nur möglich, wenn Ihre Zertifizierungsstelle Zertifikate erstellt, die zum Signieren anderer Zertifikate verwendet werden können.

### Globale signierte Identitätsdateien

Sie können global signierte Zertifikate direkt als Serveridentitätsdateien verwenden. Im folgenden Diagramm wird die Konfiguration für mehrere Identitätsdateien dargestellt:



Sie referenzieren die Serveridentitätsdatei und das Kennwort für den privaten Schlüssel auf der dbsrv16- bzw. mlsrv16-Befehlszeile.

#### Siehe auch

- SQL Anywhere: „Datenbankserver mit Transportschichtssicherheit“ auf Seite 1454
- MobiLink: „Den MobiLink-Server mit Transportschichtssicherheit starten“ auf Seite 1460

### Vertrauenseinstellung von Clients für das Zertifikat der Zertifizierungsstelle

Bei der Serverauthentifizierung müssen Sie gewährleisten, dass Clients, die mit Ihrem Server Kontakt aufnehmen, dem Stammzertifikat in der Kette vertrauen. Bei global signierten Zertifikaten ist das Stammzertifikat das Zertifikat der Zertifizierungsstelle.

#### Hinweis

Bei der Verwendung von globalen Zertifikaten muss jeder Client Feldwerte überprüfen, um zu vermeiden, dass Zertifikaten vertraut wird, die dieselbe Zertifizierungsstelle für andere Clients signiert hat.

Siehe [Zertifikatsfelder überprüfen](#) auf Seite 1461.

#### Siehe auch

- „Konfigurieren von MobiLink-Clients für die Verwendung von Transportschichtsicherheit“ auf Seite 1461
- „Datenbankserver mit Transportschichtsicherheit“ auf Seite 1454
- „Global signierte Zertifikate“ auf Seite 1451

## Verschlüsselung der SQL Anywhere-Client/Server-Kommunikation

Sie können die SQL Anywhere Client/Server-Kommunikation unter Verwendung der Transportschichtsicherheit verschlüsseln.

#### Siehe auch

- „Verschlüsselung für SQL Anywhere-Webdienste“ auf Seite 1458

## Datenbankserver mit Transportschichtsicherheit

Um den Datenbankserver mit Transportschichtsicherheit zu starten, geben Sie den Namen der Serveridentitätsdatei und das Kennwort, mit dem der private Schlüssel des Servers geschützt ist, an.

Verwenden Sie die Datenbankserveroption `-ec`, um die Parameter `identity` und `identity_password` anzugeben. Wenn Sie unverschlüsselte Verbindungen über Shared Memory zulassen möchten, müssen Sie auch die Option `-es` angeben.

Folgendes ist die Syntax einer partiellen `dbsrv16`-Befehlszeile:

```
-ec tls(  
  identity=server-identity-filename;  
  identity_password=password )  
-x tcpip
```

- **Serveridentitätsdateiname** Der Pfad und der Dateiname der Serveridentitätsdatei. Wenn Sie FIPS-zertifizierte RSA-Verschlüsselung verwenden, müssen Sie Ihre Zertifikate mit dem RSA-Algorithmus generieren.

Eine Identitätsdatei enthält das öffentliche Zertifikat und seinen privaten Schlüssel. Für Zertifikate, die nicht selbst signiert sind, enthält die Identitätsdatei auch alle Signierzertifikate.

- **Kennwort** Das Kennwort für den privaten Schlüssel des Servers. Sie geben dieses Kennwort beim Erstellen des Serverzertifikats an.

Sie können den Datenbankserver auch mit einfacher Verschlüsselung starten. Die einfache Verschlüsselung erschwert es einem Eindringling, einen Datenpaketschnüffler einzusetzen, um die zwischen Client und Server transportierten Netzwerkpakete auszuspähen. Dabei wird aber weder die Datenintegrität noch eine Serverauthentifizierung garantiert.

Das TCP/IP-Protokoll wird mit der Datenbankserveroption `-x` angegeben.

### Siehe auch

- „Transportschichtssicherheit einrichten“ auf Seite 1446
- „Digitale Zertifikate“ auf Seite 1447
- „Datenbankserveroption -fips“ auf Seite 237
- „Datenbankserveroption -ec“ auf Seite 230
- „Datenbankserveroption -es“ auf Seite 234
- „Datenbankserveroption -x“ auf Seite 305

### Beispiel

Im folgenden Beispiel (in einer einzigen Zeile eingegeben) werden mit der Datenbankserveroption -ec der Sicherheitstyp RSA, die Serveridentitätsdatei und das Kennwort, das den privaten Schlüssel des Servers schützt, angegeben:

```
dbsrv16 -ec tls( identity=c:\test\srv1_rsa.id;identity_password=mypwd )
-x tcpip c:\test\secure.db
```

Sie können die Befehlszeilenoptionen, einschließlich Kennwörter, mit einer Konfigurationsdatei und dem Dienstprogramm zum Verschleiern von Dateien (dbfhide) verschleiern. Siehe „Dienstprogramm zum Verschleiern von Dateien (dbfhide)“ auf Seite 922 und „@data -Datenbankserveroption“ auf Seite 214.

## Konfigurieren der Clientanwendung für die Verwendung der Transportschichtssicherheit

Sie können SQL Anywhere-Clientanwendungen für die Verwendung von Transportschichtssicherheit konfigurieren. Mit einer Reihe von encryption-Verbindungsparametern geben Sie vertrauenswürdige Zertifikate, den Typ der Verschlüsselung und das Netzwerkprotokoll an.

### Siehe auch

- „Transportschichtssicherheit einrichten“ auf Seite 1446

## Serverauthentifizierung

Mithilfe der Serverauthentifizierung kann ein entfernter Client die Identität eines Datenbankservers überprüfen. Die Überprüfung von digitalen Signaturen und Zertifikatsfeldern ist für die Serverauthentifizierung erforderlich.

### Digitale Signaturen

Ein Zertifikat für einen Datenbankserver enthält eine oder mehrere digitale Signaturen, mit denen die Datenintegrität sichergestellt und vor unbefugten Zugriffen geschützt wird. Mit den folgenden Schritten erstellen Sie eine digitale Signatur:

- Wenn ein Algorithmus für ein Zertifikat ausgeführt wird, wird ein eindeutiger Wert oder Hash generiert.
- Der Hash wird mit dem privaten Schlüssel eines unterzeichnenden Zertifikats bzw. einer Zertifizierungsstelle verschlüsselt.

- Der verschlüsselte Hash, auch digitale Signatur genannt, wird in das Zertifikat eingebettet.

Eine digitale Signatur kann selbstsigniert oder durch ein Unternehmensstammzertifikat bzw. eine Zertifizierungsstelle signiert sein.

Wenn eine Clientanwendung einen Datenbankserver kontaktiert und beide für die Verwendung der Transportschichtssicherheit konfiguriert sind, sendet der Server dem Client eine Kopie seines Zertifikats. Der Client entschlüsselt die digitale Signatur des Zertifikats mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels des Servers, berechnet für das Zertifikat einen neuen Hash und vergleicht die beiden Werte. Wenn die Werte übereinstimmen, wird dadurch die Integrität des Serverzertifikats bestätigt.

Wenn Sie FIPS-zertifizierte RSA-Verschlüsselung verwenden, müssen Sie Ihre Zertifikate mit RSA generieren.

### Zertifikatsfelder überprüfen

Bei der Verwendung von globalen Zertifikaten muss jeder Client bestimmte Zertifikatsfelder überprüfen, um zu vermeiden, dass Zertifikaten vertraut wird, die von derselben Zertifizierungsstelle für andere Clients signiert wurden. Dieses Problem wird gelöst, indem Ihre Clients bestimmte Feldwerte im Identifizierungsabschnitt des Zertifikats überprüfen. Eine Zertifizierungsstelle muss die Korrektheit der Identitätsinformationen in von ihr unterzeichneten Zertifikaten garantieren.

Beim Erstellen eines Zertifikats mit dem Dienstprogramm createcert füllen Sie die Felder "Organisation", "Organisationseinheit" und "Name" aus. Sie können diese Felder mit den entsprechenden Client-Verbindungsparametern überprüfen. Wenn Sie die Zertifizierungsstelle eines Drittanbieters zum globalen Signieren von Zertifikaten verwenden, sollten Sie dringend die Zertifikatsfelder überprüfen.

- **Organisation** Das Feld "Organisation" entspricht der encryption-Protokolloption `certificate_company`.
- **Organisationseinheit** Das Feld "Organisationseinheit" entspricht der encryption-Protokolloption `certificate_unit`.
- **Name** Das Feld "Name" entspricht der encryption-Protokolloption `certificate_name`.

### Die trusted\_certificates-Protokolloption verwenden

Dies ist die einzige erforderliche Protokolloption, wenn TLS im Encryption-Verbindungsparameter angegeben wird. Mit der trusted\_certificates-Protokolloption geben Clients vertrauenswürdige Zertifikate für Datenbankserver an. Das vertrauenswürdige Zertifikat kann ein selbstsigniertes Zertifikat des Servers, ein öffentliches Unternehmensstammzertifikat oder ein Zertifikat einer kommerziellen Zertifizierungsstelle sein.

## Siehe auch

- „Selbstsignierte Stammzertifikate“ auf Seite 1448
- „Global signierte Zertifikate“ auf Seite 1451
- „certificate\_company-Protokolloption“ auf Seite 392
- „certificate\_unit-Protokolloption“ auf Seite 394
- „certificate\_name-Protokolloption“ auf Seite 393
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „trusted\_certificates-Protokolloption“ auf Seite 421
- „Digitale Zertifikate“ auf Seite 1447
- „Zertifikatketten“ auf Seite 1449

## Eine Clientverbindung mit Transportschichtssicherheit herstellen

Um Clientanwendungen für die Verwendung von Transportschichtssicherheit zu konfigurieren, verwenden Sie den encryption [ENC]-Verbindungsparameter in Ihrer Verbindungszeichenfolge. Die Verbindungszeichenfolge sieht dann wie folgt aus (muss in einer einzigen Zeile eingegeben werden):

```
Encryption=tls(
[ fips={ y | n }; ]
  trusted_certificates=public-certificate
[ certificate_company=organization; ]
[ certificate_name=common-name; ]
[ certificate_unit=organization-unit ] )
```

- **öffentliches\_Zertifikat** ist der Pfad und Dateiname einer Datei, die ein oder mehrere Zertifikate enthält. Wenn Sie FIPS-zertifizierte RSA-Verschlüsselung verwenden, müssen Sie Ihre Zertifikate mit RSA generieren.
- **Organisation** Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Feld "Organisation" auf dem Zertifikat mit diesem Wert übereinstimmt.
- **Common\_Name** Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Feld "Common Name" auf dem Zertifikat mit diesem Wert übereinstimmt.
- **Organisationseinheit** Zwingt den Client, Serverzertifikate nur zu akzeptieren, wenn das Feld "Organisationseinheit" auf dem Zertifikat mit diesem Wert übereinstimmt.

## Siehe auch

- „trusted\_certificates-Protokolloption“ auf Seite 421
- „certificate\_company-Protokolloption“ auf Seite 392
- „certificate\_name-Protokolloption“ auf Seite 393
- „certificate\_unit-Protokolloption“ auf Seite 394
- „Verbindungsparameter Encryption (ENC)“ auf Seite 359
- „Digitale Zertifikate“ auf Seite 1447
- Zertifikatsfelder überprüfen auf Seite 1456
- Die trusted\_certificates-Protokolloption verwenden auf Seite 1456

## Beispiel

Im folgenden Beispiel wird mit dem encryption-Verbindungsparameter `trusted_certificates` das Zertifikat `public_cert.crt` angegeben.

```
"UID=DBA;PWD=sql;Host=myhost;Server=myserver;  
ENC=tls(trusted_certificates=public_cert.crt) "
```

Im folgenden Beispiel wird mit dem encryption-Verbindungsparameter `trusted_certificates` das Zertifikat `public_cert.crt` angegeben. Außerdem werden Zertifikatfelder mit den encryption-Verbindungsparametern `certificate_unit` und `certificate_name` überprüft.

```
"UID=DBA;PWD=sql;Host=myhost;Server=myserver;  
ENC=tls(trusted_certificates=public_cert.crt;  
certificate_unit=test_unit;certificate_name=my_certificate) "
```

## Verschlüsselung für SQL Anywhere-Webdienste

Der SQL Anywhere-Webserver unterstützt HTTPS-Verbindungen mit SSL-Version 3.0 und den TLS-Versionen 1.0 und 1.1.

Um die Transportschichtssicherheit für SQL Anywhere-Webdienste einzurichten, führen Sie die folgenden Schritte aus:

- **Digitale Zertifikate beziehen** Sie benötigen Datenbankserver-Zertifikats- und Identitätsdateien. Zertifikate (bei denen es sich um Zertifikate einer Zertifizierungsstelle handeln kann), werden an Browser oder Webclients verteilt. Serveridentitätsdateien werden sicher auf Ihrem SQL Anywhere-Webserver gespeichert.
- **Webserver mit Transportschichtssicherheit starten** Mit der Datenbankserveroption `-xs` können Sie HTTPS, die Serveridentitätsdatei und das Kennwort zum Schutz des privaten Schlüssels festlegen.
- **Webclients konfigurieren** Konfigurieren Sie Browser oder andere Webclients so, dass sie Zertifikaten vertrauen. Bei den vertrauenswürdigen Zertifikaten kann es sich um ein selbstsigniertes Zertifikat, Unternehmensstammzertifikat oder um ein von einer Zertifizierungsstelle signiertes Zertifikat handeln.

### Siehe auch

- „Digitale Zertifikate“ auf Seite 1447
- „Datenbankserveroption `-fips`“ auf Seite 237
- „Datenbankserveroption `-xs`“ auf Seite 310
- „Identity-Protokolloption“ auf Seite 402
- „identity\_password-Protokolloption“ auf Seite 403

## Verschlüsselung der MobiLink-Client/Server-Kommunikation

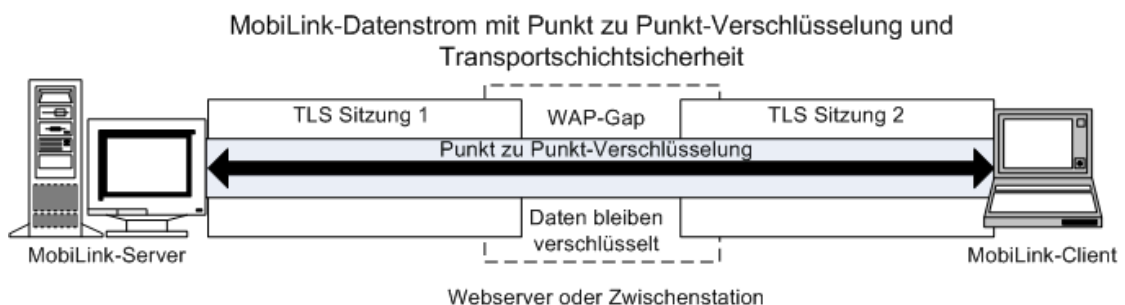
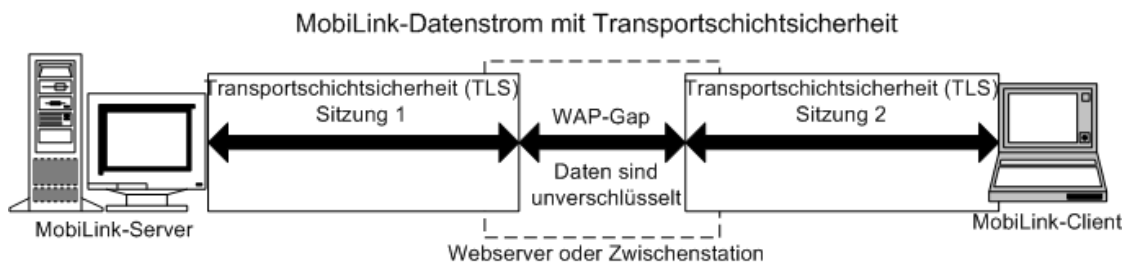
Sie können die MobiLink-Client/Server-Kommunikation unter Verwendung der Transportschichtssicherheit verschlüsseln.

## Ende-zu-Ende-Verschlüsselung

Von Punkt zu Punkt-Verschlüsselung spricht man, wenn Daten am Ursprung verschlüsselt und am Ziel entschlüsselt werden. Während der gesamten Übertragung sind die Daten zu keinem Zeitpunkt unverschlüsselt.

MobiLink TLS wird oft nur zur Verschlüsselung der Daten auf einer Teilstrecke (zum Beispiel bis zur Verschlüsselungs-/Entschlüsselungs-Hardware) zwischen Client und Server eingesetzt. Bei der Zwischenstation werden die Daten entschlüsselt und danach von der Zwischenstation für den Rest der Übertragung neuerlich verschlüsselt. Dies tritt vor allem dann ein, wenn eine Synchronisation über einen HTTPS-Webserver durchgeführt wird. Das kurze Intervall, wenn Daten an der Zwischenstation entschlüsselt werden, wird oft auch als Wireless Application Protocol-Lücke oder WAP Gap (also eine Lücke bei der Übermittlung über ein Drahtlosprotokoll) bezeichnet.

In einem Unternehmen ist ein WAP-Gap oft akzeptabel, wenn sich die Zwischenstation innerhalb des Unternehmens befindet. Bei einem von einem Provider zentral verwalteten System, in dem Daten von verschiedenen Unternehmen über dasselbe WAP-Gap geschleust werden, können schutzwürdige Daten gegebenenfalls dem externen Zugriff ausgesetzt sein. Die Punkt zu Punkt-Verschlüsselung hindert eine Zwischenstation daran, auf die Daten zuzugreifen, weil der Synchronisationsdatenstrom von Anfang bis Ende verschlüsselt ist und noch einmal mit TLS verschlüsselt werden kann.



### Siehe auch

- „mlsrv16-Option -x“ [[MobiLink - Serveradministration](#)]
- „e2ee\_public\_key“ [[MobiLink - Clientadministration](#)]
- „Schlüsselpaargenerator-Dienstprogramm (createkey)“ auf Seite 945

## Den MobiLink-Server mit Transportschichtsicherheit starten

Um den MobiLink-Server mit Transportschichtsicherheit zu starten, geben Sie die Identitätsdatei und das Identitätskennwort ein, mit denen der private Schlüssel des Servers geschützt ist.

### MobiLink-Server über TCP/IP und HTTPS sichern

Verwenden Sie die mlsrv16-Serveroption -x, um eine Identität und ein Identitätskennwort einzugeben. Folgendes ist eine partielle mlsrv16-Befehlszeile (muss in einer einzigen Zeile eingegeben werden):

```
-x protocol(  
  fips={ y | n };  
  identity=identity-file;  
  identity_password=password;... )
```

- **Protokoll** Das zu verwendende Protokoll. Kann **https** oder **tls** sein. Das **tls**-Protokoll ist TCP/IP mit TLS.
- **fips** Gibt an, ob FIPS-zertifizierte Verschlüsselung verwendet werden soll. Die fips-Option kann nur mit RSA-Verschlüsselung verwendet werden. RSA FIPS verwendet separate FIPS 140-2-bestätigte Software von Certicom. Server mit der fips-Option sind mit Clients ohne die fips-Option kompatibel und umgekehrt. RSA FIPS kann bei SQL Anywhere-Clients auf jeder unterstützten 32-Bit-Windows-Plattform und unter Solaris bzw. bei UltraLite-Clients unter Unix oder auf jeder unterstützten 32-Bit-Windows-Plattform, einschließlich Windows Mobile, verwendet werden.
- **Identitätsdatei** Pfad und Dateiname der Identitätsdatei, die den privaten Schlüssel des Servers, das Zertifikat des Servers und optional die von der Zertifikatsstelle signierten Zertifikate enthält.
- **Kennwort** Das Kennwort für den privaten Schlüssel des Servers. Sie geben dieses Kennwort beim Erstellen der Serveridentität an.

### Siehe auch

- „Transportschichtsicherheit einrichten“ auf Seite 1446
- „Digitale Zertifikate“ auf Seite 1447
- „mlsrv16-Option -x“ [*MobiLink - Serveradministration*]

### Beispiele

Im folgenden Beispiel wird der Typ der Sicherheit (RSA), die Serveridentitätsdatei und das Identitätskennwort, mit dem der private Schlüssel des Servers geschützt wird, in der mlsrv16-Befehlszeile angegeben:

```
mlsrv16 -c "dsn=my_cons"  
-x tls(identity=c:\test\serv_rsa1.crt;identity_password=pwd)
```

Das folgende Beispiel ist ähnlich dem vorherigen, mit dem Unterschied, dass der Name der Identitätsdatei ein Leerzeichen enthält:

```
mlsrv16 -c "dsn=my_cons"  
-x "tls(identity=c:\Program Files\test\serv_rsa1.crt;identity_password=pwd)"
```

Sie können die Befehlszeilenoptionen mit einer Konfigurationsdatei und dem Dienstprogramm zum Verschleiern von Dateien (dbfhide) ausblenden. Siehe „mlsrv16-Option @data“ [[MobiLink - Serveradministration](#)].

## Konfigurieren von MobiLink-Clients für die Verwendung von Transportschichtssicherheit

Sie können SQL Anywhere- oder UltraLite-Clients für die Verwendung von MobiLink-Transportschichtssicherheit konfigurieren. Für jeden Client geben Sie vertrauenswürdige Zertifikate, den Typ der Verschlüsselung und das Netzwerkprotokoll an.

### Serverauthentifizierung

Mithilfe der Serverauthentifizierung kann ein entfernter Client die Identität eines MobiLink-Servers überprüfen. Die Überprüfung von digitalen Signaturen und Zertifikatsfeldern ist für die Serverauthentifizierung erforderlich.

### Digitale Signaturen

Ein Zertifikat für einen MobiLink-Server enthält eine oder mehrere digitale Signaturen, mit denen die Datenintegrität sichergestellt und vor unbefugten Zugriffen geschützt wird. Mit den folgenden Schritten erstellen Sie eine digitale Signatur:

- Wenn ein Algorithmus für ein Zertifikat ausgeführt wird, wird ein eindeutiger Wert oder Hash generiert.
- Der Hash wird mit dem privaten Schlüssel eines unterzeichnenden Zertifikats bzw. einer Zertifizierungsstelle verschlüsselt.
- Der verschlüsselte Hash, auch digitale Signatur genannt, wird in das Zertifikat eingebettet.

Eine digitale Signatur kann selbstsigniert oder durch ein Unternehmensstammzertifikat bzw. eine Zertifizierungsstelle signiert sein.

Wenn ein MobiLink-Client einen MobiLink-Server kontaktiert und beide für die Verwendung der Transportschichtssicherheit konfiguriert sind, sendet der Server dem Client eine Kopie seines Zertifikats. Der Client entschlüsselt die digitale Signatur des Zertifikats mithilfe des im Zertifikat enthaltenen öffentlichen Schlüssels des Servers, berechnet für das Zertifikat einen neuen Hash und vergleicht die beiden Werte. Wenn die Werte übereinstimmen, wird dadurch die Integrität des Serverzertifikats bestätigt.

### Zertifikatsfelder überprüfen

Bei der Verwendung von globalen Zertifikaten muss jeder Client bestimmte Zertifikatsfelder überprüfen, um zu vermeiden, dass Zertifikaten vertraut wird, die von derselben Zertifizierungsstelle für andere Clients signiert wurden. Dieses Problem wird gelöst, indem Ihre Clients bestimmte Feldwerte im Identifizierungsabschnitt des Zertifikats überprüfen. Eine Zertifizierungsstelle muss die Korrektheit der Identitätsinformationen in von ihr unterzeichneten Zertifikaten garantieren.

Beim Erstellen eines Zertifikats mit dem Dienstprogramm createcert füllen Sie die Felder "Organisation", "Organisationseinheit" und "Name" aus. Sie können diese Felder mit den entsprechenden MobiLink-Client-Verbindungsparametern überprüfen.

- **Organisation** Das Feld "Organisation" entspricht dem MobiLink-Client-Verbindungsparameter certificate\_company.
- **Organisationseinheit** Das Feld "Organisationseinheit" entspricht dem MobiLink-Client-Verbindungsparameter certificate\_unit.
- **Name** Das Feld "Name" entspricht dem MobiLink-Client-Verbindungsparameter certificate\_name.

### Siehe auch

- „Transportschichtsicherheit einrichten“ auf Seite 1446
- „Selbstsignierte Stammzertifikate“ auf Seite 1448
- „Zertifikatketten“ auf Seite 1449
- „Global signierte Zertifikate“ auf Seite 1451
- „certificate\_company“ [*MobiLink - Clientadministration*]
- „certificate\_unit“ [*MobiLink - Clientadministration*]
- „certificate\_name“ [*MobiLink - Clientadministration*]
- „UltraLite-Clients für die Verwendung von Transportschichtsicherheit konfigurieren“ auf Seite 1464
- „Clientsicherheitsoptionen“ auf Seite 1462
- „Digitale Zertifikate“ auf Seite 1447

## Clientsicherheitsoptionen

MobiLink-Clients (SQL Anywhere und UltraLite) verwenden eine gemeinsame Gruppe von Verbindungsparametern zum Konfigurieren der Transportschichtsicherheit.

### trusted\_certificates-Protokolloption

Mit der trusted\_certificates-Protokolloption geben MobiLink-Clients vertrauenswürdige Zertifikate für MobiLink-Server an. Das vertrauenswürdige Zertifikat kann ein selbstsigniertes Zertifikat des Servers, ein öffentliches Unternehmensstammzertifikat oder das Zertifikat einer kommerziellen Zertifizierungsstelle sein.

Siehe:

- „trusted\_certificates“ [*MobiLink - Clientadministration*]
- „Digitale Zertifikate“ auf Seite 1447

### Zertifikatsfelder überprüfen

Mit den Protokolloptionen certificate\_company, certificate\_unit und certificate\_name werden Zertifikatsfelder überprüft. Hierbei handelt es sich um einen wichtigen Schritt bei der Serverauthentifizierung. Wenn Sie die Zertifizierungsstelle eines Drittanbieters zum globalen Signieren von Zertifikaten verwenden, sollten Sie dringend die Zertifikatsfelder überprüfen.

Siehe:

- [Zertifikatsfelder überprüfen auf Seite 1461](#)
- [„Global signierte Zertifikate“ auf Seite 1451](#)
- [„Serverauthentifizierung“ auf Seite 1461](#)

## Konfigurieren von SQL Anywhere-Clients für die Verwendung der Transportschichtssicherheit

### Transportschichtssicherheit über TCP/IP und HTTPS verwenden

Die MobiLink-Transportschichtssicherheit ist eine spezifische Funktion der MobiLink HTTPS- und TCP/IP-Protokolle. Wenn Sie die Transportschichtssicherheit über HTTPS verwenden möchten, geben Sie den `trusted_certificates`-Verbindungsparameter mit der erweiterten Option `ADR` an. Folgendes ist die Syntax einer partiellen `dbmlsync`-Befehlszeile:

```
-e "ctp=protocol;
    adr=[ fips={ y | n }; ]
    trusted_certificates=public-certificate;
    ..."
```

- **Protokoll** Das zu verwendende Protokoll. Kann **https** oder **tls** sein. Das **tls**-Protokoll ist TCP/IP mithilfe von Transportschichtssicherheit.
- **fips** Gibt an, ob FIPS-zertifizierte Verschlüsselung verwendet werden soll. FIPS-zertifizierte Verschlüsselung kann nur mit RSA-Verschlüsselung verwendet werden. FIPS-zertifiziertes HTTPS verwendet separate FIPS 140-2-zertifizierte Software von Certicom, ist aber mit MobiLink-Servern der Version 9.0.2 oder später kompatibel, die HTTPS verwenden.
- **öffentliches\_Zertifikat** Der Pfad und der Dateiname eines vertrauenswürdigen Zertifikats.

Bei HTTPS oder FIPS-zertifiziertem HTTPS müssen Sie mit RSA-Verschlüsselung erstellte Zertifikate verwenden.

### Siehe auch

- [„Clientsicherheitsoptionen“ auf Seite 1462](#)
- [„Digitale Zertifikate“ auf Seite 1447](#)
- [„Erweiterte Option CommunicationAddress \(adr\)“ \[MobiLink - Clientadministration\]](#)
- [„Netzwerkprotokolloptionen des MobiLink-Clients“ \[MobiLink - Clientadministration\]](#)
- [„CREATE SYNCHRONIZATION SUBSCRIPTION-Anweisung \[MobiLink\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)
- [„ALTER SYNCHRONIZATION SUBSCRIPTION-Anweisung \[MobiLink\]“ \[SQL Anywhere Server - SQL-Referenzhandbuch\]](#)

### Beispiele

Das folgende Beispiel gibt RSA-Sicherheit über HTTPS an. Es muss in einer einzigen Zeile eingegeben werden:

```
dbmlsync -c "server=reml;uid=DBA;pwd=mypwd"
-e "ctp=https;
```

```
adr='trusted_certificates=c:\temp\public_cert.crt;  
certificate_company=Sybase, Inc.;  
certificate_unit=IAS;  
certificate_name=MobiLink' "
```

Alternativ können Sie die erweiterte Option CommunicationAddress mit der Anweisung CREATE SYNCHRONIZATION SUBSCRIPTION oder ALTER SYNCHRONIZATION SUBSCRIPTION angeben. Diese Methode liefert dieselben Informationen, speichert sie jedoch in der Datenbank.

```
CREATE SYNCHRONIZATION SUBSCRIPTION  
TO publ  
FOR user1  
ADDRESS 'trusted_certificates=c:\temp\public_cert.crt;  
certificate_company=Sybase, Inc.;  
certificate_unit=IAS;  
certificate_name=MobiLink';
```

Das folgende Beispiel gibt RSA-Sicherheit und TCP/IP an. Es muss in einer einzigen Zeile eingegeben werden:

```
dbmlsync -c "server=rem1;uid=myuid;pwd=mypwd"  
-e "ctp=tls;  
adr='port=3333;  
trusted_certificates=c:\test\public_cert.crt;  
certificate_company=Sybase, Inc.;  
certificate_unit=IAS;  
certificate_name=MobiLink' "
```

Alternativ können Sie die erweiterte Option CommunicationAddress mit der Anweisung CREATE SYNCHRONIZATION SUBSCRIPTION oder ALTER SYNCHRONIZATION SUBSCRIPTION angeben:

```
CREATE SYNCHRONIZATION SUBSCRIPTION  
TO publ  
FOR user1  
ADDRESS 'port=3333;  
trusted_certificates=public_cert.crt;  
certificate_company=Sybase, Inc.;  
certificate_unit=IAS;  
certificate_name=MobiLink';
```

## UltraLite-Clients für die Verwendung von Transportschichtsicherheit konfigurieren

UltraLite-Clients können so konfiguriert werden, dass sie die Transportschichtsicherheit über ein TCP/IP- oder HTTPS-Protokoll verwenden.

### Voraussetzungen

Sie müssen ein TCP/IP- oder HTTPS-Protokoll verwenden.

### Kontext und Bemerkungen

Die MobiLink-Transportschichtsicherheit ist eine spezifische Funktion des MobiLink HTTPS-Protokolls. Wenn Sie HTTPS und UltraLite-Clients verwenden, können Sie vertrauenswürdige Zertifikate und Zertifikatfelder direkt als Netzwerkprotokolloptionen angeben. Es gibt zwei Möglichkeiten,

vertrauenswürdige Stammzertifikate anzugeben: mit dem UltraLite-Dienstprogramm zum Initialisieren einer Datenbank oder mit der trusted\_certificates-Protokolloption.

## Aufgabe

1. Geben Sie das TCP/IP- oder HTTPS-Protokoll für die Synchronisation an. Das Schlüsselwort für sicheres TCP/IP ist "tls".
2. Geben Sie TCP/IP- oder HTTPS-Protokolloptionen an.

Mithilfe der Protokolloptionen certificate\_company, certificate\_unit und certificate\_name werden Zertifikatfelder überprüft.

Wenn Sie die trusted\_certificates-Protokolloption für HTTPS angeben, werden alle in der UltraLite-Datenbank eingebetteten Informationen für vertrauenswürdige Zertifikate aufgehoben.

## Ergebnisse

Der UltraLite-Client wird so konfiguriert, dass er die Transportschichtssicherheit entweder über ein HTTPS- oder über ein TCP/IP-Protokoll verwendet.

## Beispiel

Das folgende Beispiel ist in C/C++ UltraLite. Um "tls" anzugeben, ändern Sie HTTPS in "tls".

```
auto ul_sync_info synch_info;
conn.InitSynchInfo( &synch_info );
synch_info.user_name = UL_TEXT( "50" );
synch_info.version = UL_TEXT( "ul_default" );
...
synch_info.stream = "https";
...

auto ul_sync_info synch_info;
...
synch_info.stream = "https";
synch_info.stream_parms = TEXT(
    "port=9999;
    certificate_company=Sybase, Inc.;
    certificate_unit=IAS;
    certificate_name=MobiLink");

auto ul_sync_info synch_info;
...
synch_info.stream = "https";
synch_info.stream_parms = TEXT(
    "port=9999;
    trusted_certificates=\\rsaroot.crt;
    certificate_company=Sybase, Inc.;
    certificate_unit=IAS;
    certificate_name=MobiLink");
```

**Siehe auch**

- „UltraLite-Netzwerkprotokolloptionen für dbmsync“ [[UltraLite - Datenbankverwaltung](#)]
- „UltraLite-Dienstprogramm zum Initialisieren einer Datenbank (ulinit)“ [[UltraLite - Datenbankverwaltung](#)]
- Zertifikatsfelder überprüfen auf Seite 1461

## Zertifikat-Dienstprogramme

Benutzer wenden sich üblicherweise an Dritthersteller, um Zertifikate zu erwerben. Diese Zertifizierungsstellen stellen ihre eigenen Tools zur Erstellung von Zertifikaten zur Verfügung. Die folgenden Tools sind möglicherweise bei der Erstellung von Zertifikaten für Entwicklungs- und Testzwecke besonders nützlich und können auch für Produktionszertifikate verwendet werden.

**Siehe auch**

- „Dienstprogramm zum Erstellen von Zertifikaten (createcert)“ auf Seite 894
- „Dienstprogramm zum Anzeigen von Zertifikaten (viewcert)“ auf Seite 903

---

# Hochverfügbarkeit und Scale-Out-Systeme mit Schreibschutz

SQL Anywhere unterstützt Datenbankspiegelung und Veritas Cluster Server, um eine hohe Verfügbarkeit zu gewährleisten. Beide Konfigurationen bieten alternative Datenbankserver, die Datenbanken ausführen können, falls einer der aktuell ausgeführten Datenbankserver ausfallen sollte.

Wenn Sie Arbeitslasten verteilen möchten, dann sollten Sie auch erwägen, ob Scale-Out mit Schreibschutz eine geeignete Lösung ist.

Außerdem können Sie Hochverfügbarkeit bzw. Scale-Out mit Schreibschutz für das Hosting von Webanwendungen einsetzen.

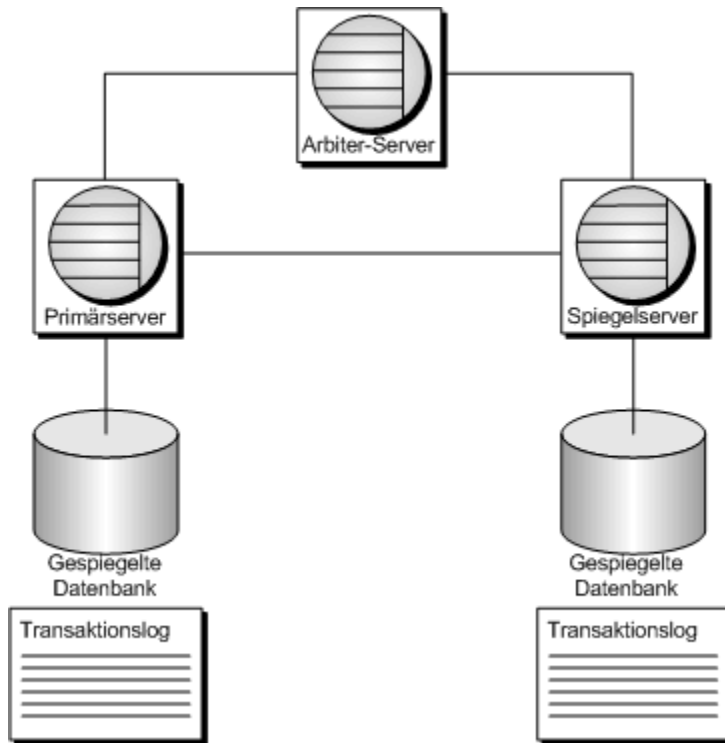
## Siehe auch

- [„SQL Anywhere-Scale-Out mit Schreibschutz“ auf Seite 1536](#)
- [„SQL Anywhere-Webdienste mit Hochverfügbarkeit und Scale-Out-Lösungen“ auf Seite 1540](#)

## Datenbankspiegelung

Die **Datenbankspiegelung** ist eine Konfiguration aus drei auf separaten Computern laufenden Datenbankservern, die zusammenarbeiten, um Kopien der Datenbank- und Transaktionslogdateien zu verwalten.

Der **Primärserver** und der **Spiegelserver** verwalten jeweils eine Kopie der Datenbankdateien und Transaktionslogdateien. Der Primärserver verfügt über die Kopie der Datenbank mit Lese-/Schreibzugriff, der Spiegeldatenbankserver über die schreibgeschützte Kopie der Datenbank. Die dritte Server, der sogenannte **Arbiterserver**, wird verwendet, wenn bestimmt werden muss, welcher der beiden anderen Server Eigentümer der Datenbank werden kann. Eigentümer der Datenbank ist der Server, auf dem sich die Kopie der Datenbank mit Lese-/Schreibzugriff befindet. Der Arbiterserver führt keine Kopie der Datenbank. Die Konfiguration der drei Datenbankserver (Primär-, Spiegel- und Arbiterserver) wird **Spiegelungssystem** genannt, und der Primär- und der Spiegelserver werden gemeinsam **Partnerserver** genannt.



Clients verbinden sich mit dem Primärserver, um auf die Datenbank zuzugreifen. Alle in der Datenbank gemachten Änderungen werden im Transaktionslog auf dem Primärserver aufgezeichnet. Wenn die Änderungen festgeschrieben werden, sendet der Primärserver die Transaktionslogseiten an den Spiegelserver, wo sie an einer Kopie (Spiegel) der Datenbank angewendet werden. Auf die Kopie der Datenbank auf dem Spiegelserver kann nur im schreibgeschützten Modus zugegriffen werden, während dieser Datenbankserver als Spiegelserver verwendet wird.

**Hinweis**

Datenbankspiegelung erfordert eine getrennte Lizenz. Siehe „[Getrennt lizenzierbare Komponenten](#)“ [[SQL Anywhere 16 - Einführung](#)].

**Siehe auch**

- „[Verbindungen mit Datenbank in Spiegelungssystemen herstellen](#)“ auf Seite 1472

## Arbiterserver

Der Arbiterserver löst Konflikte zwischen den Servern bei der Frage, welcher Server der Primärserver sein soll. Ohne Arbiterserver würde Folgendes geschehen: Wenn Server A in einem Spiegelungssystem gestartet wird, während Server B nicht verfügbar ist, kann Server A nicht ermitteln, ob seine Kopie der Datenbankdateien aktuell ist. Das Starten einer Datenbank mit nicht aktuellen Dateien führt zum Verlust von Transaktionen, die in der anderen Kopie der Datenbank bereits übernommen und festgeschrieben

wurden. Außerdem könnte die andere Kopie der Datenbank nicht für eine Spiegelung verwendet werden, wenn die beiden Partnerserver die Kommunikation wieder aufnehmen.

Neben der Lösung von Konflikten beim Start wird der Arbiterserver benötigt, wenn die Kommunikationsverbindung zwischen den beiden Servern unterbrochen wird, aber beide Server weiterhin laufen. Ohne einen Arbiterserver würden beide Server annehmen, dass sie Eigentümer der Datenbank sind. Dies würde wieder zu verlorenen Transaktionen und inkompatiblen Datenbanken führen. Mit einem Arbiterserver kann der Primärserver feststellen, dass er weiterhin Eigentümer der Datenbank ist und Clients weiterhin zur Verfügung stehen kann. Wenn der Primärserver die Verbindung sowohl zu dem Spiegel- als auch zu dem Arbiterserver verliert, muss er herunterfahren und darauf warten, dass einer der beiden wieder verfügbar wird.

Der als Arbiterserver ausgeführte Server kann als Arbitrer für mehr als ein Spiegelungssystem fungieren. Außerdem kann er als Datenbankserver für andere Datenbanken fungieren.

### Siehe auch

- [„Verwenden eines Kopieknottens als Arbitrer“ auf Seite 1485](#)

## Quorum in der Datenbankspiegelung

Bevor ein Server die Rolle eines Primärservers annehmen kann, muss er ein **Quorum** erhalten, d.h. dass zumindest ein weiterer Server zustimmen muss, dass der Server Datenbankeigentümer sein kann. Wenn der Spiegelserver ausfällt, während der Primär- und der Arbiterserver verbunden sind, gewährt der Primärserver weiter Zugriff auf die Datenbank. Wenn der Primärserver das Quorum verliert, ist er nicht mehr in der Lage, Zugriff auf die Datenbank zu ermöglichen. An dieser Stelle stoppt der Primärserver die gespiegelte Datenbank und versucht, sie neu zu starten. Anschließend wartet er auf das Erreichen des Quorums, bevor er die Datenbank verfügbar macht.

### Ablauf beim Starten eines Datenbankspiegelungssystems

Wenn Sie ein Datenbankspiegelungssystem starten, durchlaufen die Datenbankserver einen Startprozess, um das Quorum zu erreichen und Clientverbindungen zu akzeptieren. In den folgenden Schritten wird eine typische Ereignissequenz für diesen Prozess beschrieben. Annahmen: Server 1 und Server 2 sind Partner, die beide gestoppt wurden. (Server 2 war der Spiegelserver und wurde zuerst gestoppt und anschließend wurde Server 1 gestoppt.) Der Arbiterserver läuft.

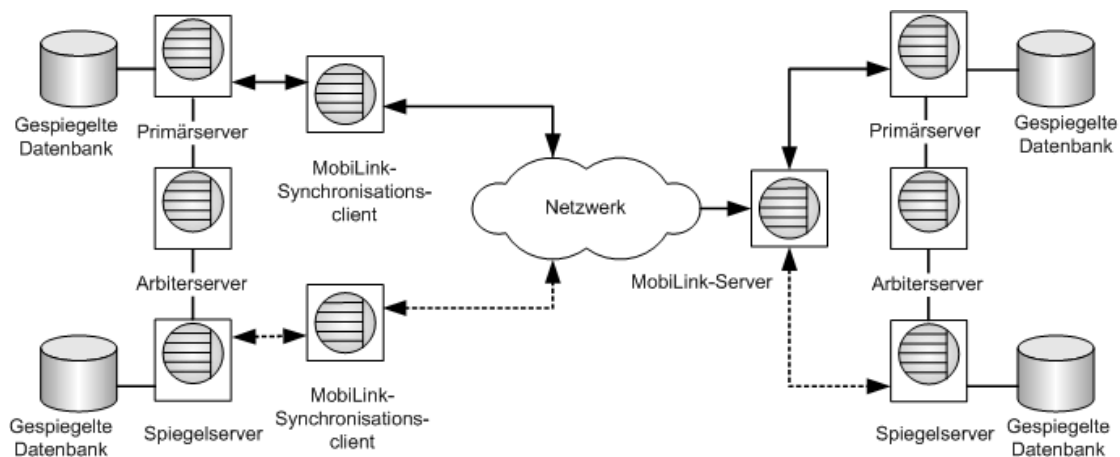
1. Der Arbiterserver wartet auf Verbindungen von Server 1 und Server 2.
2. Server 1 wird gestartet und versucht, sich mit Server 2 und dem Arbiterserver zu verbinden.
3. Server 1 verbindet sich mit dem Arbiterserver.
4. Server 1 kann sich nicht mit Server 2 verbinden, weil dieser nicht läuft.
5. Server 1 verhandelt mit dem Arbitrer, um zu ermitteln, ob Server 1 als Primär- oder Spiegelserver fungieren soll.

6. Das Quorum wird erreicht, wenn Arbiterserver und Server 1 vereinbaren, dass Server 1 die Rolle des Primärserver übernehmen soll. Der Arbitrer und die Statusdatei für Server 1 zeigen an, dass Server 1 der letzte Primärserver war, bevor die Partnerserver gestoppt wurden.
7. Server 1 beginnt, Verbindungen zu akzeptieren.
8. Server 2 wird gestartet und versucht, sich mit Server 1 und dem Arbitrer zu verbinden.
9. Server 2 verbindet sich mit dem Arbitrer und mit Server 1.
10. Server 2 verhandelt mit Server 1 und dem Arbitrer, um zu ermitteln, ob Server 2 als Primär- oder Spiegelserver fungieren soll.
11. Alle drei Server vereinbaren, dass Server 2 als Spiegelserver fungieren soll.
12. Server 2 beginnt, schreibgeschützte Verbindungen zu akzeptieren.
13. Server 2 beginnt, Logdatei-Seiten zu übernehmen, die er von Server 1 empfängt.

## Datenbankspiegelung und MobiLink

Konfigurieren Sie die MobiLink-Synchronisation für die Ausführung in einer Hochverfügbarkeitsumgebung, in der eine konsolidierte SQL Anywhere-Datenbank mit entfernten SQL Anywhere-Datenbanken verwendet wird. Sie können Ihr MobiLink-Synchronisationssystem zum Ausführen der konsolidierten Datenbank in einer Hochverfügbarkeitsumgebung konfigurieren oder die entfernte Datenbank für die Ausführung in einer Hochverfügbarkeitsumgebung konfigurieren oder beides.

Die folgende Grafik zeigt eine MobiLink-Synchronisation, die in einer Umgebung ausgeführt wird, in der sowohl die konsolidierte Datenbank als auch die entfernte Datenbank gespiegelt werden:



## Hochverfügbarkeit für konsolidierte SQL Anywhere-Datenbanken

Der **Primärserver** verwaltet die aktive Kopie der Datenbankdatei und der Transaktionslogs. Dieser Server akzeptiert aktive Verbindungen und verarbeitet Datenbanktransaktionen. Alle Transaktionen werden vom Primärserver an den Spiegelserver gesendet.

Der **Spiegelserver** empfängt alle Transaktionen, die auf den Primärserver angewendet wurden, direkt vom Primärserver. Der Spiegelserver wird zum Primärserver, wenn ein Failover auftritt.

Der **MobiLink-Server** stellt eine ODBC-Verbindung mit dem Primärserver her und verarbeitet den vom MobiLink-Client kommenden Upload-Datenstrom. Er generiert den Download-Datenstrom, der an die Clients gesendet wird. Der MobiLink-Server verbindet sich immer mit dem als Primärserver fungierenden Server, nie mit dem Spiegelserver.

## Hochverfügbarkeit für entfernte SQL Anywhere-Datenbanken

Die Datensynchronisation wird eingeleitet, wenn der **MobiLink-Client** eine Verbindung mit der entfernten Datenbank und dem MobiLink-Server herstellt. Der MobiLink-Client muss das aktive Transaktionslog und die Offline-Transaktionslogs durchsuchen. In einer Hochverfügbarkeitsumgebung ist jedoch nicht immer bekannt, welche Datenbank als Primärserver fungiert und wo sich das aktive Transaktionslog und die Offline-Transaktionslogs befinden. Wenn der Datenbank Offline-Transaktionslogs zugeordnet sind, müssen Sie beim Start des MobiLink-Clients **-e dir=Pfadname** angeben. Siehe „Erweiterte Option OfflineDirectory (dir)“ [[MobiLink - Clientadministration](#)].

Der MobiLink-Client generiert den an den MobiLink-Server zu sendenden Upload-Datenstrom aus dem Transaktionslog der entfernten Datenbank. Der Client verarbeitet und übernimmt anschließend den Download-Datenstrom.

## Wiederherstellen nach einem Primärserver-Ausfall

Um zu verhindern, dass Ihr Hochverfügbarkeits-Datensynchronisationssystem eine einzelne Schwachstelle aufweist, wird empfohlen, dass Sie mehrere MobiLink-Server und Lastausgleicher verwenden. In diesem Fall ist jede Komponente der Datensynchronisationsumgebung redundant und das System funktioniert auch dann, wenn in der Umgebung Hardware- oder Softwareausfälle eintreten. Weitere Hinweise zur Verwendung mehrerer MobiLink-Server finden Sie unter „MobiLink-Server in einer Serverfarm“ [[MobiLink - Serveradministration](#)] und „Getrennt lizenzierbare Komponenten“ [[SQL Anywhere 16 - Einführung](#)].

Ebenso gilt: Um zu vermeiden, dass die entfernte Datenbank eine einzelne Schwachstelle aufweist, kann über ein geplantes Ereignis, das sowohl in der Primärdatenbank als auch in der Spiegeldatenbank gespeichert ist, eine Implementierung ausgelöst werden, bei der eine externe Prozedur, z.B. die xp\_cmdshell-Systemprozedur, zum Aufrufen des MobiLink-Clients verwendet wird.

## Siehe auch

- „xp\_cmdshell-Systemprozedur“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Hochverfügbarkeit und Scale-Out-Systeme mit Schreibschutz“ auf Seite 1467
- „MobiLink-Servertechnologie“ [[MobiLink - Serveradministration](#)]

# Hinweise zur Anwendungsentwicklung bei Datenbankspiegelung

Wenn Sie eine Datenbankspiegelung verwenden, sollten Anwendungen in fast allen Fällen genauso laufen können wie bei Verbindungen mit nicht gespiegelten Datenbanken. Es gibt allerdings ein paar Hinweise, die zu berücksichtigen sind, wenn Sie Anwendungen für die Verwendung mit einer Datenbankspiegelung entwickeln.

## Verbindungen mit Datenbank in Spiegelungssystemen herstellen

Stellen Sie eine Verbindung mit der Datenbank auf dem Primär- oder Spiegelserver her, indem Sie den alternativen Namen für den betreffenden Server mit dem `ServerName`-Verbindungsparameter angeben sowie die Adressen für die beiden Partnerserver mit dem `Host`-Verbindungsparameter.

### Voraussetzungen

Die Partnerserver für die Spiegelung müssen laufen.

### Kontext und Bemerkungen

In einem Spiegelungssystem wissen Sie nicht unbedingt, welcher Datenbankserver als Primärserver fungiert und welcher als Spiegelserver.

Erstellen Sie Clients, die sich neu mit der Datenbank verbinden können (z.B. wenn der Benutzer bei einem Failover die Anwendung herunterfahren und neu starten muss).

### Aufgabe

- Wenn Sie eine Verbindung mit dem Primär- oder Spiegelserver der gespiegelten Datenbank herstellen möchten, muss die Verbindungszeichenfolge die folgenden Verbindungsparameter enthalten:
  - **Server**

**Mit dem Primärserver verbinden** Wählen Sie eine der folgenden Optionen:

Option	Aktion
ServerName-Verbindungsparameter	Geben Sie den alternativen Servernamen für den Primärdatenbankserver im Datenbankspiegelungssystem an. Dies ist der durch die Anweisung <code>CREATE MIRROR SERVER primary_alternate_server_name AS PRIMARY ...</code> definierte Name.
NodeType-Verbindungsparameter	Setzen Sie den NodeType-Verbindungsparameter (Node) in der Verbindungszeichenfolge auf <code>MIRROR</code> .

**Mit dem Spiegelserver verbinden** Wählen Sie eine der folgenden Optionen:

Option	Aktion
ServerName-Verbindungsparameter	Geben Sie den alternativen Servernamen für den Spiegeldatenbankserver im Datenbankspiegelungssystem an. Dies ist der durch die Anweisung <code>CREATE MIRROR SERVER mirror_alternate_server_name AS MIRROR ...</code> definierte Name.
NodeType-Verbindungsparameter	Setzen Sie den NodeType-Verbindungsparameter (Node) in der Verbindungszeichenfolge auf PRIMARY.

- **HOST** Geben Sie die Adressen und Ports für beide Partner an, um sicherzustellen, dass die Verbindung erfolgreich ist, unabhängig davon, welcher Partner gerade als Primärserver fungiert. Die Host- und Portinformationen für jeden der Partner werden in der Verbindungszeichenfolge der Anweisung `CREATE MIRROR SERVER partner_server_name AS PARTNER connection_string='SERVER=partner_server_name;host=host_name:port_number'` definiert.

Das Angeben des `RetryConnectionTimeout`-Verbindungsparameters kann sinnvoll sein, um zu steuern, wie lange Clients versuchen sollen, sich mit einem der Datenbankserver zu verbinden.

## Ergebnisse

Der Client stellt eine Verbindung mit dem angegebenen Server her.

## Beispiel

Wenn der primäre Datenbankserver zum Beispiel `myprimary` heißt, geben Clients in ihrer Verbindungszeichenfolge den Verbindungsparameter `"Server=myprimary"` an:

```
...UID=user12;PWD=x92H4pY;Server=myprimary;HOST=myhost1:6871,myhost2:6872...
```

## Siehe auch

- „[RetryConnectionTimeout-Verbindungsparameter \(RetryConnTO\)](#)“ auf Seite 382
- „[Verbindungsparameter NodeType \(NODE\)](#)“ auf Seite 375
- „[Verbindungen mit Datenbanken in Scale-Out-Systemen herstellen](#)“ auf Seite 1544

## Abfragen in der Spiegeldatenbank

In einem Datenbankspiegelungssystem können Sie über eine schreibgeschützte Verbindung auf die Datenbank zugreifen, die auf dem Spiegelserver läuft. Diese Funktion ist nützlich, wenn Sie Berichterstellungs- oder andere Vorgänge auslagern möchten, die einen schreibgeschützten Zugriff auf diese Datenbank erfordern.

Der Versuch, die Spiegeldatenbank zu ändern, führt zu einem Fehler, was dem Verhalten entspricht, wenn eine Datenbank mit der Option `-r` als schreibgeschützt gestartet wird. Sie können Vorgänge in temporären Tabellen ausführen.

Abfragen, die in der Spiegeldatenbank ausgeführt werden, können Sperren abhängig von der angegebenen Isolationsstufe einrichten. Wenn sich Sperren mit Vorgängen überlagern, die vom Primärserver

angewendet werden, werden die Transaktionen der Verbindungen, die die Sperren halten, zurückgesetzt und etwaige geöffnete Cursor für diese Verbindungen werden geschlossen. Anwendungen, die auf der Isolationsstufe 0 ausgeführt werden, fügen zwar keine Zeilensperren hinzu, setzen aber dennoch Schemasperren. Wenn die Schemasperren Vorgänge stören, die vom Primärserver angewendet werden, erfolgt einfach ein Rollback der Transaktionen in der Spiegeldatenbank.

Anwendungen, die eine konstante Ansicht der Datenbank erfordern (und daher nicht Isolationsstufe 0 verwenden können), sollten Snapshot-Isolation verwenden. Um dies zu tun, muss die Option `allow_snapshot_isolation` auf "On" gesetzt sein. Diese Option wird sowohl auf dem Primärserver als auch auf dem Spiegelserver wirksam. Daher müssen die mit der Snapshot-Isolation verbundenen Kosten berücksichtigt werden.

Verbindungen zur Spiegeldatenbank sind von Transaktionen im Primärserver betroffen, da diese Vorgänge anschließend abgearbeitet und durch den Spiegelserver angewendet werden. Es kann eine kleine Verzögerung zwischen dem Zeitpunkt, an dem ein Update auf dem Primärserver festgeschrieben wird, und dem Zeitpunkt auftreten, an dem das Update dem Spiegelserver zur Verfügung steht. Normalerweise ist diese Verzögerung nur kurz, aber Sie sollten sie berücksichtigen, wenn Sie auf die Datenbank zugreifen, die auf dem Spiegelserver läuft.

Verbindungen zur Spiegeldatenbank bleiben aufrecht, wenn ein Failover auftritt und der Spiegelserver zum Primärserver wird. Nach einem Failover kann eine Verbindung Änderungen an der Datenbank durchführen. Fragen Sie den Wert der `ReadOnly`-Datenbankeigenschaft ab, um zu ermitteln, ob die Datenbank, mit der Sie verbunden sind, aktualisierbar ist:

```
SELECT DB_PROPERTY( 'ReadOnly' );
```

Verbindungen mit einem Kopieknoten oder einer Spiegeldatenbank werden in manchen Fällen getrennt oder abgebrochen, wenn diese Verbindungen das Übernehmen des Transaktionslogs verhindern. Wenn beispielsweise eine Verbindung eine Prozedur verwendet, die das Transaktionslog zu ändern oder zu löschen versucht, wird die Verbindung getrennt, die das Übernehmen des Transaktionslogs blockiert, und eine Meldung wird in die Serverkonsole gedruckt.

### Siehe auch

- „Snapshot-Isolation“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]
- „`allow_snapshot_isolation`-Option“ auf Seite 574
- „`CREATE MIRROR SERVER`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „`ALTER MIRROR SERVER`-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- `ReadOnly`-Datenbankeigenschaft auf Seite 784
- „Ereignisausführung in einem Datenbankspiegelungssystem oder Scale-Out-System mit Schreibschutz“ auf Seite 1474

## Ereignisausführung in einem Datenbankspiegelungssystem oder Scale-Out-System mit Schreibschutz

Ereignisse können entweder nur auf dem Primärserver oder dem Stammserver ausgeführt werden oder sie können auf dem Primärserver, dem Spiegelserver und den Kopieknoten ausgeführt werden.

Standardmäßig werden Ereignisse nicht in der Spiegeldatenbank ausgelöst. Das Auslösen von Ereignissen beginnt erst nach einem Failover vom Primärserver auf den Spiegelserver.

Sie können beim Erstellen oder Ändern eines Ereignisses festlegen, wo das Ereignis ausgeführt werden kann. Verwenden Sie die FOR-Klausel der Anweisung CREATE EVENT oder ALTER EVENT, um festzulegen, wo ein Ereignis ausgelöst werden kann.

### DatabaseStart-Ereignistyp

Standardmäßig wird ein Ereignis mit dem DatabaseStart-Ereignistyp nur ausgeführt, wenn ein Server zum Primärserver für die Datenbank wird. Wenn Sie jedoch angegeben haben, dass das Ereignis auf dem Primärserver, dem Spiegelserver und den Kopieknoten ausgeführt werden kann, wird das Ereignis beim Starten jeder Datenbank ausgeführt. Wenn in einem Spiegelungssystem dieses Ereignis nicht beim Starten der Datenbank ausgeführt wurde (z.B. weil die Datenbank bereits vor dem Erstellen des Ereignisses lief), kann das Ereignis während eines Failovers ausgeführt werden.

Wenn Sie beispielsweise ein Datenbankspiegelungssystem starten, ein DatabaseStart-Ereignis mit der FOR ALL-Klausel erstellen und anschließend den Primärserver stoppen, verursachen Sie einen Failover. In diesem Beispiel wird das Ereignis auf dem neuen Primärserver ausgeführt. Das DatabaseStart-Ereignis wird bei nachfolgenden Failovers nicht mehr ausgeführt.

### Siehe auch

- „Systemereignisse“ auf Seite 1091
- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „EVENT\_PARAMETER-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Anforderungen und Einschränkungen für Datenbankspiegelungssysteme

Bei der Datenbankspiegelung gibt es keine besonderen Hardware- oder Software-Anforderungen, und die Datenbankserver können an örtlich verschiedenen Standorten ausgeführt werden. Datenbankserver, die an einem Datenbankspiegelungssystem teilnehmen, können gespiegelte wie auch ungespiegelte Datenbanken ausführen. Überdies kann der Arbiterserver der Arbiters bei mehreren Datenbankspiegelungssystemen sein.

Bei der Verwendung der Datenbankspiegelung gelten die folgenden Anforderungen und Einschränkungen:

- **Netzwerk-Datenbankserver erforderlich** Da eine Spiegelung Netzwerkkommunikation zwischen den Datenbankservern beinhaltet, müssen Sie den Netzwerk-Datenbankserver (dbsrv16) verwenden. Der Personal Server kann nicht verwendet werden.

Alle Datenbankserver in einem Datenbankspiegelungssystem müssen dieselbe Minor Release verwenden, können jedoch unterschiedliche Supportpakete ausführen.

- **TCP/IP erforderlich** Nur TCP/IP-Verbindungen sind zwischen gespiegelten Servern zulässig.
- **Transaktionslog-Einschränkungen** Bei Verwendung der Datenbankspiegelung können Sie das Transaktionslog auf dem Primärserver nicht kürzen, weil dies zum Verlust von Transaktionen führen kann. Sie können das Transaktionslog beliebig oft umbenennen. Weitere Hinweise zur Verwendung von Ereignissen zum Verwalten von Transaktionslogs in Spiegelungssystemen finden Sie unter „Verwaltung von Transaktionslogdateien in einem Datenbankspiegelungssystem“ auf Seite 1484.

- **Webserver** Bei gleichzeitiger Verwendung von SQL Anywhere als Webserver und in einem Spiegelungssystem ist es nicht möglich, die URL für eine Webanforderung so anzugeben, dass gewährleistet ist, dass die Anforderung zum aktuellen Primärserver geleitet wird. Wenn einer der Servercomputer in der URL genannt wird und dieser Server nicht aktiv ist, tritt ein Timeout für die Anforderung ein.
- **Regelmäßige Sicherungen weiterhin erforderlich** Die Datenbankspiegelung ist kein Ersatz für einen Sicherungs- und Wiederherstellungsplan. Implementieren Sie eine Sicherungs- und Wiederherstellungsstrategie für Ihre Datenbank. Siehe „[Sicherungen in Datenbankspiegelungssystemen](#)“ auf Seite 1487 und „[Sicherung und Datenwiederherstellung](#)“ auf Seite 1027.
- **DDL-Einschränkungen** Minimieren Sie die Anzahl von DDL-Anweisungen, die in der Primärdatenbank ausgeführt werden, während ein Objekt möglicherweise auf einem Kopieknoten oder dem Spiegelserver verwendet wird. Das Löschen oder Ändern eines Systemobjekts kann dazu führen, dass Benutzerverbindungen mit dem Spiegelserver oder den Kopieknoten getrennt werden, wenn diese Verbindungen das gelöschte bzw. geänderte Objekt verwenden.
- **Failover und geplante Ereignisse** Wenn für Ihre Datenbank Ereignisse geplant sind und ein Failover auftritt, muss der Failover vor dem Starten der Ereignisse abgeschlossen werden. Andernfalls werden die Ereignisse erst zum nächsten geplanten Zeitpunkt ausgeführt. Wenn der Spiegelserver zur Primärserver-Rolle wechselt, aber der Übergang noch nicht abgeschlossen wurde, wird das geplante Ereignis nicht ausgeführt. Die Ausführung erfolgt dann zum nächsten geplanten Zeitpunkt. Wenn ein Ereignis ausgeführt wird und der Primärserver die Verbindungen zum Spiegelserver und Arbiterserver verliert, werden die Ereignisverbindung und alle anderen Verbindungen getrennt. Wenn für den Zeitpunkt, nachdem der Spiegelserver die Primärserver-Rolle übernommen hat, die Ausführung eines Ereignisses geplant ist, wird dieses Ereignis auf dem neuen Primärserver ausgeführt.

### Siehe auch

- „[Verwendung von Datenbankspiegelungssystem-Ereignissen zum Senden von Benachrichtigungs-E-Mails bei Failover](#)“ auf Seite 1489
- „[Verwaltung von Transaktionslogdateien in einem Datenbankspiegelungssystem](#)“ auf Seite 1484
- „[Abfragen in der Spiegeldatenbank](#)“ auf Seite 1473
- „[SQL Anywhere-Webdienste mit Hochverfügbarkeit und Scale-Out-Lösungen](#)“ auf Seite 1540

## Hinweise zur Performance bei Datenbankspiegelungssystemen

- Die Computer, auf denen Primär- und Spiegelserver laufen, sollten mit ähnlicher Hardware (Prozessor, Festplatte, Speicher etc.) konfiguriert sein. Der auf einem der Computer laufende Datenbankserver kann jederzeit als Primärserver für die gespiegelte Datenbank fungieren. Die Auslastung des Spiegelservers ist normalerweise niedrig und hängt von der Häufigkeit der Aktualisierungen auf dem Primärserver ab und von der Verarbeitungslast, die durch schreibgeschützte Verbindungen mit dem Spiegelserver erzeugt wird.
- Die Performance von Transaktionen, die die Datenbank aktualisieren, hängt von der Größe der Transaktionen und der Häufigkeit von Festschreibungen ab. Wenn die Größe der Transaktionen oder der Häufigkeit der Festschreibungen erhöht wird, interagiert der Primärserver mehr mit dem

Spiegelserver, wodurch zusätzliche Möglichkeiten von Verzögerungen auf dem Primärserver entstehen und der Benutzer diese möglicherweise bemerkt.

- Die Abfrageperformance auf dem Primärserver wird von einer Spiegelung im Allgemeinen nicht beeinflusst. Wenn Ihre Anwendung mehr Lesevorgänge als Aktualisierungen hat und Auditing nicht aktiviert ist, werden Sie wahrscheinlich keine Veränderung der Performance des Primärservers feststellen. Wenn für die Datenbank das Auditing aktiviert ist, kann eine Veränderung der Performance feststellbar werden, weil beim Auditing zusätzliche Informationen in das Transaktionslog geschrieben werden.
- Die Performance Ihrer Clientanwendungen kann durch die Netzwerkverbindung zwischen den Servern im Spiegelungssystem beeinflusst werden, v. a. wenn sich die Server an verschiedenen Standorten befinden. Eine langsame Netzwerkverbindung zwischen den Servern kann die Performance Ihrer Clientanwendungen ebenfalls beeinträchtigen.
- Ein Spiegelungssystem, das im asynchronen oder Asynchron-Ganzseiten-Modus (asyncfullpage) läuft, veranlasst den Primärserver weniger häufig zu Wartephasen als wenn der synchrone Modus verwendet wird. Jedoch auch im asynchronen oder asyncfullpage-Modus muss bei gesendeten Nachrichten vom Primärserver an den Spiegelserver auf eine Bestätigung vom Spiegelserver gewartet werden, wodurch sich Verzögerungen ergeben könnten. Außerdem ist das Senden von Paketen an den Spiegelserver mit einem geringen Overhead verbunden. Der asynchrone Modus und der Asynchron-Ganzseiten-Modus werden nicht empfohlen, da Transaktionen verloren gehen können.
- Unvollständige Transaktionen müssen zurückgesetzt werden, wenn der Spiegelserver Eigentümer der Datenbank wird, und je länger eine Transaktion ist, desto länger dauert das Rollback. Die Wiederherstellungsgeschwindigkeit bei einem Failover hängt von der Anzahl der Clients und von der Länge ihrer Transaktionen ab, die zurückgesetzt werden müssen. Wenn die Wiederherstellungsgeschwindigkeit wichtig ist, sollten Sie Ihre Anwendung so planen, dass sie nach Möglichkeit kurze Transaktionen verwendet.

#### **Siehe auch**

- [„Datenbankspiegelungsmodi“ auf Seite 1477](#)

## **Datenbankspiegelungsmodi**

Es gibt drei Betriebsmodi, die steuern, wann und wie Transaktionen auf dem Spiegelserver erfasst werden. In fast allen Fällen wird der Standardmodus "synchronous", empfohlen, weil er der zuverlässigste ist.

Bei der Datenbankspiegelung gibt es drei Betriebsmodi:

- synchronous (Standardwert)
- asynchronous
- asyncfullpage

Diese Modi steuern, wann und wie Transaktionen auf dem Spiegelserver erfasst werden, und Sie legen sie fest, indem Sie mit der SET MIRROR OPTION-Anweisung den Wert der synchronization\_mode-Option setzen.

Das Senden von Logseiten an die Kopieknoten erfolgt immer asynchron, unabhängig vom gewählten Modus.

Beim Wählen eines Synchronisationsmodus für Ihr Datenbankspiegelungssystem müssen Sie bestimmen, ob bei einem Failover die Performance von Änderungen an der Primärdatenbank oder das Vermeiden des Verlusts von Transaktionen wichtiger ist.

Sie können den Datenbankspiegelungsmodus überprüfen, indem Sie den Wert der Datenbankeigenschaft `MirrorMode` abfragen.

```
SELECT DB_PROPERTY( 'MirrorMode' );
```

### Synchroner Modus (Standardeinstellung)

Im synchronen Modus werden festgeschriebene Transaktionen auf dem Spiegelserver garantiert aufgezeichnet. Sollte ein Fehler auf dem Primärserver auftreten, gehen nicht-festgeschriebene Transaktionen verloren, wenn der Spiegelserver übernimmt. In diesem Modus sendet der Primärserver Transaktionslogseiten an den Spiegel, wenn eine Transaktion festgeschrieben wird. Der Spiegelserver bestätigt die Übertragung, wenn er diese Seiten in seine Kopie des Transaktionslogs geschrieben hat. Der Primärserver antwortet der Anwendung erst, wenn er diese Bestätigung erhalten hat.

Die Verwendung des synchronen Modus bietet **Transaktionssicherheit**, weil sich die Partnerserver in einem synchronisierten Status befinden und an den Spiegelserver gesendete Änderungen zuerst bestätigt werden müssen, bevor der Primärserver fortfahren kann.

### Asynchroner Modus und Asynchron-Ganzseiten-Modus (nicht empfehlenswert)

Der asynchrone Modus und der Asynchron-Ganzseiten-Modus sind zwar schneller als der synchrone Modus, aber weniger zuverlässig. Standardmäßig gilt: Wenn der Primärserver unerwartet ausfällt, übernimmt der Spiegelserver nicht automatisch als Primärserver.

- **Asynchroner Modus** Im asynchronen Modus werden festgeschriebene Transaktionen auf dem Spiegelserver nicht garantiert aufgezeichnet. In diesem Modus sendet der Primärserver Transaktionslogseiten an den Spiegel, wenn eine Transaktion festgeschrieben wird. Er wartet nicht auf eine Bestätigung vom Spiegelserver, bevor er der Anwendung mitteilt, dass der COMMIT abgeschlossen wurde. Sollte ein Fehler auf dem Primärserver auftreten, können einige festgeschriebene Transaktionen verloren gehen, wenn der Spiegelserver übernimmt.
- **Asynchron-Ganzseiten-Modus** Im Asynchron-Ganzseiten-Modus (oder Seitenmodus) werden Seiten nicht bei einem COMMIT gesendet, sondern sie werden übermittelt, wenn die Seite voll ist. Diese Einstellung verringert das Verkehrsaufkommen zwischen den beiden Datenbankservern und verbessert die Performance des Primärservers. Wenn die aktuelle Logseite nicht innerhalb der im `pagetimeout`-Parameter angegebenen Anzahl von Sekunden an den Spiegelserver gesendet wurde, wird sie gesendet, auch wenn sie noch nicht voll ist. Der Standardwert für `pagetimeout` ist 5 Sekunden. Dieser Modus beschränkt die Zeitspanne, in der festgeschriebene Transaktionen verloren gehen können, wenn der Primärserver ausfällt und der Spiegelserver Eigentümer der Datenbank wird. Der Asynchron-Ganzseiten-Modus impliziert einen asynchronen Vorgang, daher wartet der Primärserver nicht auf eine Bestätigung vom Spiegelserver.

Im asynchronen oder Asynchron-Ganzseiten-Modus ist der Failover vom Primärserver zum Spiegelserver nicht automatisch, weil der Spiegelserver möglicherweise nicht alle festgeschriebenen Transaktionen

enthält, die am Primärserver angewendet wurden. Aus diesem Grund kann ein Spiegelserver beim Ausfall des Primärservers nicht standardmäßig Eigentümer einer Datenbank werden, wenn einer der beiden asynchronen Modi verwendet wird. Wenn in dieser Situation ein automatischer Failover erwünscht ist (trotz der Wahrscheinlichkeit, dass Transaktionen verloren gehen), setzen Sie mithilfe der SET MIRROR OPTION-Anweisung die Option "auto\_failover" auf "on". Anderenfalls erkennt der ausgefallene Server beim Neustart, ob Transaktionen verloren gegangen sind. Wenn Transaktionen verloren gegangen sind, schreibt er eine Meldung an das Datenbankserver-Meldungslog und fährt die Datenbank herunter. Die aktuelle Datenbank und das Transaktionslog müssen dann durch eine Sicherungskopie ersetzt werden, bevor die Spiegelung fortgesetzt werden kann.

Hinweise, wie Sie einen Server nach einem Ausfall im asynchronen oder Asynchron-Ganzseiten-Modus wiederherstellen finden Sie unter [„Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall“ auf Seite 1499](#).

**Hinweis**

Es wird empfohlen, die auto\_failover-Spiegelungsoption auf ON zu setzen, wenn Sie den asynchronen oder den Asynchron-Ganzseiten-Modus verwenden. Dadurch übernimmt der Spiegelserver automatisch als Primärserver, wenn der Primärserver ausfällt. Die Verwendung der auto\_failover-Option kann dazu führen, dass Transaktionen verloren gehen.

Die synchronize\_mirror\_on\_commit-Datenbankoption steuert, wann im asynchronen oder Asynchron-Ganzseiten-Modus gewährleistet ist, dass Datenbankänderungen an einen Spiegelserver gesendet wurden. Wenn Sie diese Option auf "On" setzen, bewirkt jedes COMMIT, dass im Transaktionslog erfasste Änderungen an den Spiegelserver gesendet werden und dass eine Bestätigung vom Spiegelserver an den Primärserver gesendet wird, sobald die Änderungen vom Spiegelserver empfangen wurden. Diese Option kann mit SET TEMPORARY OPTION für bestimmte Transaktionen gesetzt werden. Es kann auch nützlich sein, die Option bei bestimmten Anwendungen zu verwenden, indem die APPINFO-Zeichenfolge in einer Login-Prozedur untersucht wird.

SQL Anywhere unterstützt Systemereignisse, die unabhängig vom verwendeten Modus ausgelöst werden, wenn ein Failover in einem Datenbankspiegelungssystem auftritt. Sie können diese Ereignisse z.B. zur Benachrichtigung des Administrators bei einem Failover verwenden.

Im Asynchron- oder Asynchron-Ganzseiten-Modus müssen Sie bestimmen, was geschieht, wenn ein Failover auftritt und Transaktionen nicht in der Datenbank festgeschrieben werden.

Ein Spiegelungssystem, das im asynchronen oder Asynchron-Ganzseiten-Modus (asynfullpage) läuft, veranlasst den Primärserver weniger häufig zu Wartephasen als wenn der synchrone Modus verwendet wird. Jedoch auch im asynchronen oder asynfullpage-Modus muss bei gesendeten Nachrichten vom Primärserver an den Spiegelserver auf eine Bestätigung vom Spiegelserver gewartet werden, wodurch sich Verzögerungen ergeben könnten. Außerdem ist das Senden von Paketen an den Spiegelserver mit einem geringen Overhead verbunden. Der asynchrone Modus und der Asynchron-Ganzseiten-Modus werden nicht empfohlen, da Transaktionen verloren gehen können.

### Siehe auch

- „synchronize\_mirror\_on\_commit“ auf Seite 688
- „SET OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Verwendung von Datenbankspiegelungssystem-Ereignissen zum Senden von Benachrichtigungs-E-Mails bei Failover“ auf Seite 1489
- „Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall“ auf Seite 1499

## Synchronisationsstatus für Spiegelungssysteme

Wenn ein Spiegelungssystem den synchronen Modus verwendet, kann es sich in einem von zwei Status befinden:

- **Synchronisation läuft** Der Spiegelserver ist nicht verbunden oder hat noch nicht alle Logseiten des Primärservers gelesen. Dieser Wert wird auch zurückgegeben, wenn der Synchronisationsmodus "asynchronous" ist.
- **Synchronisiert** Der Spiegelserver ist verbunden und hat alle Änderungen übernommen, die auf dem Primärserver festgeschrieben wurden.

Wenn ein Partnerserver gestartet wird und ermittelt, dass er als Spiegelserver fungiert, fordert er als Erstes alle Logseiten vom Primärserver an, die er noch nicht hat. Das kann bedeuten, dass Seiten von anderen Logdateien als dem aktuellen aktiven Log auf dem Primärserver kopiert werden. Sobald er diese Seiten erhält, wendet der Spiegelserver die darin enthaltenen Änderungen an seiner Kopie der Datenbank an. Wenn alle Seiten vom Primärserver empfangen wurden, sind der Primär- und der Spiegelserver in einem synchronisierten Status. Ab diesem Zeitpunkt müssen alle auf dem Primärserver festgeschriebenen Änderungen an den Spiegelserver gesendet und von ihm bestätigt werden.

Im asynchronen oder Asynchron-Ganzseiten-Modus fordert der Spiegelserver Logseiten wie oben beschrieben an, aber die zwei Server befinden sich nie in einem synchronisierten Status. Sobald der Spiegelserver alle auf dem Primärserver verfügbaren Logseiten angefordert hat, wird der Primärserver benachrichtigt, dass er alle aktualisierten Seiten an den Spiegelserver senden muss.

In einem Scale-Out-System mit Schreibschutz ist der Synchronisationsstatus der Kopieknoten immer "synchronizing".

## Datenbankspiegelungssysteme einrichten

Richten Sie ein Datenbankspiegelungssystem ein, indem Sie Primär-, Spiegel- und Arbiterserver definieren, die Kopien der Datenbank- und Transaktionslogdateien verwalten sollen.

### Voraussetzungen

Sie müssen das MANAGE ANY MIRROR SERVER-Systemprivileg haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

## Kontext und Bemerkungen

In einem Spiegelungssystem für die Produktion müssen die Partnerserver und der Arbiterserver auf drei separaten Computern ausgeführt werden. In allen folgenden Beispielen müssen beim Einrichten eines Datenbankspiegelungssystems localhost und die Portnummer in den Computernamen und die Portnummer geändert werden, unter denen der entsprechende Datenbankserver ausgeführt werden soll.

## Aufgabe

1. Starten Sie die zu spiegelnde Datenbank auf einem Datenbankserver mit den Optionen **-su** und **-xp on**. Dieser Server wird einer der Partner für die Datenbank, der anfängliche Primärserver. Die Datenbank muss ein Transaktionslog haben. Zum Beispiel:

```
dbsrv16 -n mirror_server1 -x tcpip(PORT=6871;DOBRoad=no) -su sql "c:\server1\mirror_demo.db" -xp on
```

2. Stellen Sie eine Verbindung mit der Datenbank her. Zum Beispiel:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server1"
```

3. Definieren Sie die Partnerserver und den Arbiterserver für die Datenbank mithilfe der CREATE MIRROR SERVER-Anweisung. Definieren Sie außerdem den Primärserver und den Spiegelserver als Partner im Datenbankspiegelungssystem.

Zum Beispiel:

- a. Mit den beiden folgenden SQL-Anweisungen werden mirror\_server1 und mirror\_server2 als Partnerserver im Datenbankspiegelungssystem definiert:

```
CREATE MIRROR SERVER mirror_server1
AS PARTNER
connection_string='SERVER=mirror_server1;host=localhost:6871'
state_file='c:\\server1\\server1.state';

CREATE MIRROR SERVER mirror_server2
AS PARTNER
connection_string='SERVER=mirror_server2;host=localhost:6872'
state_file='c:\\server2\\server2.state';
```

- b. Mit den nachstehenden SQL-Anweisungen wird Folgendes definiert:
  - mirror\_demo\_primary als alternativer Servername für mirror\_server1. mirror\_demo\_primary ist der Name, unter dem sich Clients mit dem als Primärserver fungierenden Datenbankserver verbinden.
  - mirror\_demo\_mirror als alternativer Servername für mirror\_server2. mirror\_demo\_mirror ist der Name, unter dem sich Clients mit dem als Spiegelserver fungierenden Datenbankserver verbinden.

```
CREATE MIRROR SERVER mirror_demo_primary
AS PRIMARY
connection_string='SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872';

CREATE MIRROR SERVER mirror_demo_mirror
AS MIRROR
connection_string='SERVER=mirror_demo_mirror;HOST=localhost:6871,localhost:6872';
```

- c. Mit der folgenden SQL-Anweisung wird der Arbiterserver für das Datenbankspiegelungssystem definiert:

```
CREATE MIRROR SERVER demo_arbiter  
AS ARBITER  
connection_string ='SERVER=demo_arbiter;HOST=localhost:6870';
```

4. Setzen Sie die Spiegelungsoptionen für das Spiegelungssystem. Sie müssen eine Authentifizierungszeichenfolge angeben. Zum Beispiel:

```
SET MIRROR OPTION authentication_string='abc';
```

5. Erstellen Sie eine Kopie der Primärdatenbank und des aktuellen Transaktionslogs sowie aller anderen Transaktionslogs auf dem Computer, auf dem sich der zweite Partner befindet. Sie können dazu beispielsweise die BACKUP DATABASE-Anweisung verwenden.

Die Transaktionslogdateien auf Primärserver-Computer und Spiegelserver-Computer müssen identisch sein, einschließlich des Start-Offsets der aktuellen Transaktionslogdateien.

6. Starten Sie den zweiten Datenbankserver im Datenbankspiegelungssystem:

```
dbsrv16 -n mirror_server2 -x tcpip(PORT=6872;DOBROAD=no) -su sql "c:  
\server2\mirror_demo.db" -xp on
```

7. Starten Sie den Arbiterserver:

```
dbsrv16 -n demo_arbiter -su sql -x "TCPIP(PORT=6870;DOBROAD=no)" -xf "c:  
\arbiter\arbiter.state" -xa "AUTH=abc;DBN=mirror_demo"
```

### Ergebnisse

Clients können sich nun mit der gespiegelten Datenbank verbinden.

Die Rollen des Primär- und des Spiegelserver sind zum Konfigurieren der Datenbankserver im System erforderlich: Die Namen, die Sie diesen Servern geben, werden als alternative Servernamen benutzt, wenn Clients eine Verbindung zu den Datenbankservern herstellen. Jeder der beiden Partnerserver kann als Primär- oder Spiegelserver agieren.

### Nächste Schritte

Überwachen Sie Ihr Datenbankspiegelungssystem, indem Sie Ihr System zur Ressourcenliste des Monitors hinzufügen.

Überprüfen Sie den Status der Datenbankserver in einem Datenbankspiegelungssystem, indem Sie über Sybase Central eine Verbindung mit der Primärdatenbank herstellen. Informationen zur Datenbankspiegelung werden im Fensterausschnitt **Gesundheit und Statistik** angezeigt.

**Siehe auch**

- „Datenbankserveroption -su “ auf Seite 289
- „Datenbankoption -xp“ auf Seite 335
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „BACKUP-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Lektion 8: Datenbankspiegelungssysteme überwachen“ auf Seite 1212
- „Zustand und Statistik von Datenbanken“ auf Seite 812
- „Einen Datenbankserver in einem Spiegelungssystem stoppen“ auf Seite 1490
- „Fehlerbehandlung: Primärserver kann nicht neu gestartet werden“ auf Seite 1500
- „Upgrade und Neuaufbau in einem Datenbankspiegelungssystem“ [*SQL Anywhere 16 - Änderungen und Upgrades*]

**Auswahl des Primärservers durch Datenbankspiegelungssysteme**

Wenn eine Datenbank ohne Spiegelungsdefinitionen auf einem Datenbankserver (z.B. S1) gestartet wird, der mit **-xp on** gestartet wurde, und anschließend die Spiegelungsdefinitionen festgelegt werden, ist S1 der anfängliche Primärserver für die Datenbank.

Wenn Sie ein Datenbankspiegelungssystem erstmals einrichten, keine Statusinformationsdateien vorhanden sind und die Kopien von Datenbank und Transaktionslog identisch sind, können beide Datenbankserver als Primärserver fungieren. In diesem Fall werden die Servernamen verglichen und der Server mit dem niedrigeren Namen fungiert als Primärserver. Beispiel: Der Name server1 ist niedriger als server2. Deshalb wird server1 zum Primärserver.

Für den erstmaligen Start müssen beide Server laufen und verbunden sein, damit sie die Rollenverteilung vereinbaren können. Das Vorhandensein eines Arbiters reicht nicht aus, da die in den Statusinformationsdateien erfassten früheren Statusinformationen nicht existieren.

Während eines normalen Starts wirken sich die folgenden Eingaben darauf aus, welcher Datenbankserver zum Primärserver wird:

- Der Inhalt der Statusinformationsdateien
- Die Transaktionslogpositionen auf dem jeweiligen Datenbankserver
- Die Angabe eines bevorzugten Primärservers

**Siehe auch**

- „Fehlerbehandlung: Statusinformationsdateien von Partner und Arbitr“ auf Seite 1498
- „Bevorzugte Datenbankserver in Datenbankspiegelungssystemen“ auf Seite 1484
- Ablauf beim Starten eines Datenbankspiegelungssystems auf Seite 1469

## Bevorzugte Datenbankserver in Datenbankspiegelungssystemen

In einem Datenbankspiegelungssystem können Sie einen Partnerserver als bevorzugten Server festlegen. Der **preferred server** ist der Partner, der standardmäßig als Primärserver ausgeführt wird und Eigentümer der Datenbank ist.

Wenn der bevorzugte Server ausfällt, wird der als Spiegelserver fungierende Server zum Primärserver. Wenn der bevorzugte Server neu gestartet wird, führt er die folgenden Schritte aus:

1. Er ruft vom aktuellen Primärserver alle Transaktionslogeinträge ab, die er noch nicht hat.
2. Er fordert den aktuellen Primärserver auf, das Eigentum der Datenbank abzugeben. Anschließend tauschen die Server die Rollen. Der bevorzugte Server wird zum Primärserver und der andere Server zum Spiegelserver. Alle Verbindungen mit der Datenbank auf dem nicht bevorzugten Server gehen verloren, wenn sich der Eigentümer der Datenbank ändert.

Sie legen einen bevorzugten Server fest, indem Sie der CREATE MIRROR SERVER-Anweisung, die den Partnerserver definiert, den Parameter PREFERRED="YES" hinzufügen.

### Beispiel

Mit der folgenden Anweisung wird der Server mirror\_server1 als bevorzugter Server erstellt.

```
CREATE MIRROR SERVER mirror_server1
AS PARTNER
connection_string='SERVER=mirror_server1;host=localhost:6871'
state_file='c:\\server1\\server1.state'
preferred='YES';
```

### Siehe auch

- „CREATE MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „ALTER MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Benutzerinitiiert Rollentausch (Failover)“ auf Seite 1488
- Ablauf beim Starten eines Datenbankspiegelungssystems auf Seite 1469

## Verwaltung von Transaktionslogdateien in einem Datenbankspiegelungssystem

Wenn ein Partnerserver gestartet wird, überprüft er alle Transaktionslogdateien im Verzeichnis der aktuellen Transaktionslogdatei und ermittelt, welche übernommen werden müssen. Danach wendet der Datenbankserver die Vorgänge in diesen Transaktionslogs in der Datenbank an, bevor er bestimmt, ob er als Primär- oder als Spiegelserver agieren wird. Sie können die Transaktionslogdateien und die Datenbankdatei in demselben Verzeichnis speichern. Dieses Verzeichnis sollte aber keine anderen Dateien enthalten, da dies beim Starten der Datenbank zu Verzögerungen führen kann.

Der Server, der die Primärserverrolle übernimmt, muss ein Transaktionslog mit demselben Start-Offset haben wie das aktuelle Transaktionslog auf dem Spiegelserver sowie etwaige nachfolgende Transaktionslogdateien bis zur aktuellen Transaktionslogdatei des Primärservers.

Sobald ein Server die Rolle des Spiegels übernimmt, erhält er Transaktionslogseiten vom Primärserver. Wenn ein Transaktionslog auf dem Primärserver umbenannt wird, wird es auch auf dem Spiegelserver

umbenannt. Der Spiegelserver schreibt dann neue Transaktionslogseiten in eine neue Datei mit dem für das Transaktionslog angegebenen Namen.

Transaktionslogdateien auf dem Primärserver können regelmäßig gelöscht werden. Jedesmal, wenn das Transaktionslog umbenannt wird, wird dem Spiegelserver mitgeteilt, welche Transaktionslogdatei die älteste noch bestehende Datei auf dem Primärserver ist. Alle Transaktionslogdateien, die älter als diese sind, werden auf dem Spiegelserver gelöscht.

Bei Verwendung der Datenbankspiegelung können Sie das aktuelle Transaktionslog auf dem Primärserver nicht kürzen, weil dies zum Verlust von Transaktionen führen kann. Sie können das Transaktionslog beliebig oft umbenennen. Wenn Sie alte Transaktionslogs entfernen möchten, können Sie sie mithilfe eines geplanten Ereignisses löschen, sofern Sie sicher sind, dass sie nicht mehr benötigt werden. Sie können beispielsweise ein Ereignis erstellen, das täglich ausgeführt wird und das Transaktionslog umbenannt. Dieses Ereignis kann außerdem Kopien des Transaktionslogs löschen, die älter sind als eine Woche.

**Siehe auch**

- [„Fehlerbehandlung: Datenbankspiegelungssysteme“ auf Seite 1497](#)

## Verwenden eines Kopieknotens als Arbitr

Wenn Sie keinen neuen Datenbankserver erstellen möchten, um den Arbitr eines Spiegelungssystems auszuführen, das ein Scale-Out-System mit Schreibschutz umfasst, können Sie einen Server so konfigurieren, dass er für das System sowohl als Kopieknoten als auch als Arbiterserver fungiert.

**Voraussetzungen**

Sie müssen das `MANAGE ANY MIRROR SERVER`-Systemprivileg haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

**Aufgabe**

1. Stoppen Sie den Kopieknoten, der auch als Arbiterserver fungieren soll.
2. Wählen Sie eine der folgenden Optionen:

Option	Aktion
Arbiter zu einem vorhandenen Kopie-knoten hinzufügen	<p>a. Starten Sie den Kopieknotten mit den Datenbankserveroptionen -xf und -xa. Zum Beispiel:</p> <pre>dbsrv16 -n scaleout_child_demo -su sql -x "tcpip(PORT=6873)" -xf "c:\scaleoutdemo\copynode \arbiter.state" -xa "AUTH=abc;DBN=scaleoutdemo" "c: \scaleoutdemo\copynode\scaleoutdemo.db" -xp on</pre> <p>b. Erstellen Sie die Arbiterserverdefinition so, dass der Servername nicht mit den Servernamen für die Datenbankserver im Spiegelungssystem übereinstimmt. Führen Sie eine CREATE MIRROR SERVER-Anweisung aus. Zum Beispiel:</p> <pre>CREATE MIRROR SERVER myarbiter AS ARBITER connection_string = 'SERVER=scaleout_child_demo;HOST=localhost:6873';</pre>
Kopie-knoten zum vorhandenen Arbiter hinzufügen	<p>a. Stoppen Sie den vorhandenen Arbiterserver.</p> <p>b. Stellen Sie eine Verbindung mit dem Primärserver her und löschen Sie die vorhandene Arbiter-Spiegelserverdefinition.</p> <p>c. Erstellen Sie auf dem Primärserver eine neue Arbiter-Spiegelserverdefinition mit einem anderen Namen (jedoch mit den tatsächlichen Servernamen aus der Verbindungszeichenfolge). Zum Beispiel:</p> <pre>CREATE MIRROR SERVER newarbiter AS ARBITER connection_string = 'SERVER=actual_server_name;HOST=arbiter_host:6870';</pre> <p>d. Erstellen Sie eine Sicherung der gespiegelten Datenbank und kopieren Sie sie auf den Computer, auf dem der Kopieknotten ausgeführt werden soll.</p> <p>e. Starten Sie den Arbiterserver neu, allerdings mit der Option mirrored.db -xp ON im Serverbefehl, wobei mirrored.db der Name der gespiegelten Datenbank ist.</p>

## Ergebnisse

Der Arbiterserver führt auch einen Scale-Out-Kopieknotten mit Schreibschutz aus.

## Beispiel

Im Spiegelungssystem und Scale-Out-System mit Schreibschutz gibt es beispielsweise keinen Datenbankserver namens TheArbiter, der die folgende Serverdefinition verwendet.

```
CREATE MIRROR SERVER "scaleout_child"
AS COPY
connection_string = 'SERVER=scaleout_child;HOST=winxp-2:6878';
CREATE MIRROR SERVER "TheArbiter"
AS ARBITER
connection_string = 'SERVER=scaleout_child;HOST=winxp-2:6878';
```

**Siehe auch**

- „CREATE MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Datenbankspiegelungssysteme verwalten

### Sicherungen in Datenbankspiegelungssystemen

Obwohl die Datenbankspiegelung dazu beitragen kann, das Risiko von Datenverlusten zu minimieren, wird dringend empfohlen, die an einem Datenbankspiegelungssystem teilnehmenden Datenbanken zu sichern und zu validieren.

- Sie können die BACKUP DATABASE-Anweisung verwenden, um eine Sicherung relativ zum Datenbankserver durchzuführen. Die BACKUP DATABASE-Anweisung wird auf dem Primärserver ausgeführt, daher sollte der gelieferte Dateiname einen Netzlaufwerk- oder UNC-Namen angeben, der bei den Primär- und Spiegel-Datenbankservern konsistent ist.
- Sie können clientseitige Sicherungen der Datenbank mithilfe des Dienstprogramms dbbackup durchführen.

**Siehe auch**

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886
- „Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall“ auf Seite 1499

## Rollentausch (Failover) in der Datenbankspiegelung

Wenn der Primärserver aufgrund eines Hardware- oder Softwarefehlers ausfällt, verhandelt der Spiegelserver mit dem Arbiterserver, um Eigentümer der Datenbank zu werden und die Rolle des Primärservers zu übernehmen. Damit der Wechsel des Eigentümers oder **Rollentausch** stattfinden kann, müssen der weiterhin betriebsbereite Partnerserver und der Arbitr darin übereinstimmen, dass der Spiegelserver zu dem Zeitpunkt, zu dem der Rollentausch versucht wird, auf dem aktuellen Stand und im Status "synchronized" war.

- Verbindungen von Clients mit dem ursprünglichen Primärserver werden getrennt, wobei alle nicht festgeschriebenen Transaktionen verloren gehen. Clients müssen sich daher erneut mit der Datenbank auf dem neuen Primärserver verbinden, um weiterhin auf die Datenbank zugreifen zu können. Wenn der ursprüngliche Primärserver wieder verfügbar wird, nimmt er die Rolle des Spiegelserver an.
- Verbindungen von Clients mit der ursprünglichen Spiegeldatenbank bleiben bestehen, wenn ein Failover auftritt und der Spiegelserver zum Primärserver wird. Nach dem Failover können diese Clientverbindungen Änderungen an der Datenbank vornehmen.

Die Datenbankserver zeigen beim Start Statusmeldungen im Meldungsfenster des Datenbankservers an, die angeben, welche Rolle der Server annimmt und wie weit er im Startprozess vorangekommen ist. Eine Meldung wird angezeigt, wenn die Datenbank neu gestartet werden muss, weil ein oder mehrere Server im Spiegelungssystem ausfallen oder weil ein Server die Rolle von Spiegel- auf Primärserver wechselt.

Wenn ein Assertierungsfehler bei einem Server auftritt, der Teil eines Spiegelungssystems ist, gibt der Server einen Fehler in die Meldungslogdatei des Datenbankservers aus und beendet anschließend. Dies benachrichtigt die anderen Server von seinem Ausfall, damit sie die entsprechende Aktion durchführen können.

Wenn eine Datenbank in einer Hochverfügbarkeitsumgebung auf ein Problem stößt, z.B. auf ein inkompatibles oder nicht übereinstimmendes Transaktionslog, wird sie gestoppt. Der Datenbankserver, auf dem die von dem Problem betroffene Datenbank läuft, wird ebenfalls heruntergefahren, es sei denn, auf ihm werden weitere Datenbanken ausgeführt.

Details über den Status der einzelnen Datenbanken im Datenbankspiegelungssystem werden in einer Statusinformationsdatei gespeichert.

- Wenn ein Arbiterserver verwendet wird, erfolgt der Failover (Ausfallsicherung) vom Primär- zum Spiegelserver automatisch. Wenn Sie im synchronen Modus ausführen, gehen während des Failovers keine festgeschriebenen Transaktionen verloren.
- Der Failover geht sehr schnell, da der Spiegelserver das Transaktionslog bereits angewendet hat. Wenn der Spiegelserver feststellt, dass der Primärserver ausgefallen ist, setzt er nicht-festgeschriebene Transaktionen zurück und macht anschließend die Datenbank verfügbar.

Wenn der Primärserver ausfällt, während er sich im Status "Synchronisation läuft" befindet, kann der Spiegelserver nicht als Primärserver übernehmen. Das Spiegelungssystem wartet darauf, dass der Primärserver wieder verfügbar wird.

SQL Anywhere unterstützt Systemereignisse, die unabhängig vom verwendeten Modus ausgelöst werden, wenn ein Failover in einem Datenbankspiegelungssystem auftritt. Sie können diese Ereignisse z.B. zur Benachrichtigung des Administrators bei einem Failover verwenden.

### Siehe auch

- [„Benutzerinitiiert Rollentausch \(Failover\)“ auf Seite 1488](#)
- [Failover und geplante Ereignisse auf Seite 1476](#)
- [„Fehlerbehandlung: Statusinformationsdateien von Partner und Arbitr“ auf Seite 1498](#)
- [„Verwendung von Datenbankspiegelungssystem-Ereignissen zum Senden von Benachrichtigungs-E-Mails bei Failover“ auf Seite 1489](#)

## Benutzerinitiiert Rollentausch (Failover)

Initiieren Sie einen Datenbankspiegelungs-Failover (Rollentausch) vom Primärserver auf den Spiegelserver ohne Stoppen des Servers, indem Sie eine Verbindung mit dem Primärserver herstellen und die folgende Anweisung ausführen:

```
ALTER DATABASE SET PARTNER FAILOVER;
```

Wenn diese Anweisung ausgeführt wird, werden vorhandene Verbindungen zur Datenbank geschlossen, einschließlich der Verbindung, die die Anweisung ausgeführt hat. Wenn daher die Anweisung in einer Prozedur oder einem Ereignis enthalten ist, werden nachfolgende Anweisungen möglicherweise nicht ausgeführt. Welche Privilegien zum Ausführen dieser Anweisung erforderlich sind, wird durch die Serveroption -gk gesteuert.

Diese Anweisung ist eine Alternative zum Angeben eines bevorzugten Servers und kann zusammen mit Logik verwendet werden, die steuert, wann das Eigentum an einer Datenbank einem bestimmten Datenbankserver übertragen wird. Sie können beispielsweise einen Failover initiieren, der auf der Verfügbarkeit des Partnerservers (ermittelt anhand des Werts der PartnerState-Datenbankeigenschaft) basiert oder auf der Anzahl der Verbindungen mit der Datenbank (ermittelt anhand des Werts der ConnCount-Datenbankeigenschaft).

#### Siehe auch

- „Bevorzugte Datenbankserver in Datenbankspiegelungssystemen“ auf Seite 1484
- „ALTER DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- ConnCount-Datenbankeigenschaft auf Seite 771
- PartnerState-Datenbankeigenschaft auf Seite 782

## Verwendung von Datenbankspiegelungssystem-Ereignissen zum Senden von Benachrichtigungs-E-Mails bei Failover

Verwenden Sie die Ereignisse MirrorServerDisconnect und MirrorFailover als Mechanismus, um Benachrichtigungen per E-Mail zu senden, dass möglicherweise Aktionen in der Spiegeldatenbank erforderlich sind. Diese Ereignisse werden möglicherweise nicht in allen Situationen ausgelöst, die dazu führen, dass die auf dem Primärserver laufende Datenbank nicht verfügbar ist. Ein Stromausfall, der den Primär- und den Spiegelserver betrifft, würde z.B. verhindern, dass eines dieser Ereignisse ausgelöst wird. Wenn diese Art von Überwachung erforderlich ist, kann sie auf einem separaten Computer mittels einer Skriptsprache implementiert werden, wobei "dbping" periodisch aufgerufen wird, um sich mit der Spiegeldatenbank zu verbinden.

#### Beispiel

Das folgende Beispiel erstellt ein Ereignis, das einen Administrator benachrichtigt, wenn ein Failover auftritt:

```
CREATE EVENT mirror_server_unavailable
TYPE MirrorServerDisconnect
HANDLER
BEGIN
  CALL xp_startmail ( mail_user = 'George Smith',
                     mail_password = 'mypwd' );
  CALL xp_sendmail( recipient='DBAdmin',
                   subject='Mirror server disconnect occurred',
                   "message"='The following server is unavailable in the mirroring system: '
                   || event_parameter( 'MirrorServerName' ) );
  CALL xp_stopmail ( );
END;
```

#### Siehe auch

- Systemereignistypen für Datenbankspiegelungen auf Seite 1093
- „Ping-Dienstprogramm (dbping)“ auf Seite 955
- „EVENT\_PARAMETER-Funktion [System]“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Einen Datenbankserver in einem Spiegelungssystem stoppen

Möglicherweise müssen Sie einen Datenbankserver in einem Spiegelungssystem stoppen, um ein Supportpaket oder eine Minor Release zu übernehmen oder um einen Server aus dem Spiegelungssystem zu entfernen.

### Voraussetzungen

Der Datenbankserver muss mit der Datenbankserveroption -su gestartet worden sein, um das Kennwort für die Dienstprogramm Datenbank festzulegen. Sie müssen das Kennwort für die Dienstprogramm Datenbank haben.

### Aufgabe

- Führen Sie einen dbstop-Befehl aus, um den Datenbankserver zu stoppen. Sie müssen die Verbindungsparameter für die Dienstprogramm Datenbank in der Verbindungszeichenfolge angeben. Mit dem folgenden Befehl wird beispielsweise ein Datenbankserver namens mirror\_server\_1 gestoppt:

```
dbstop -c "UID=DBA;PWD=sql;DBN=utility_db;LINKS=tcip" mirror_server1
```

### Ergebnisse

Der Datenbankserver wird gestoppt. Sofern mindestens zwei Server im Hochverfügbarkeitssystem verbleiben, sollten Benutzer sich mit einer Kopie der Datenbank verbinden können. Je nachdem, welcher Server gestoppt wird, sind Benutzer jedoch möglicherweise nicht mehr in der Lage, die Datenbank zu aktualisieren.

### Nächste Schritte

Wenn Sie einen Primär-, Spiegel- oder Arbiterserver stoppen, funktioniert Ihr System weiterhin. Um jedoch die Hochverfügbarkeit aufrechtzuerhalten, müssen Sie den gestoppten Datenbankserver neu starten oder ersetzen.

### Siehe auch

- „Datenbankserveroption -su“ auf Seite 289
- „Datenbankserver starten“ auf Seite 153
- „Verbindung mit der Dienstprogramm Datenbank herstellen“ auf Seite 147
- „Upgrade von Datenbankspiegelungssystemen“ auf Seite 1497

## Spiegelserver aus Spiegelungssystemen löschen

Löschen Sie einen Spiegelserver aus einem Spiegelungssystem, indem Sie die beiden Spiegelserverdefinitionen löschen (CREATE MIRROR SERVER... AS PARTNER und CREATE MIRROR SERVER... AS MIRROR).

### Voraussetzungen

Es wird empfohlen, keinen Spiegelserver zu löschen, der als Teil eines Datenbankspiegelungssystems ausgeführt wird.

Sie können nur den Spiegelserver löschen. Wenn der Server, den Sie löschen möchten, als Primärserver fungiert, müssen Sie einen Failover initiieren, damit Spiegelserver und Primärserver die Rollen tauschen.

Sie müssen das `MANAGE ANY MIRROR SERVER`-Systemprivileg haben.

## Kontext und Bemerkungen

Wenn Sie den Servernamen beibehalten, aber die Einstellungen ändern möchten, können Sie die `CREATE OR REPLACE MIRROR SERVER`-Anweisung oder die `ALTER MIRROR SERVER`-Anweisung verwenden.

## Aufgabe

1. Stellen Sie eine Verbindung mit der Datenbank auf dem Primärserver her.
2. Wenn der Spiegelserver untergeordnete Kopieknoten hat, führen Sie eine `ALTER MIRROR SERVER`-Anweisung aus, um die untergeordneten Kopieknoten einem anderen übergeordneten Knoten zuzuordnen.
3. Löschen Sie die Spiegelserverdefinition, indem Sie eine `DROP MIRROR SERVER`-Anweisung ausführen und den Namen des Spiegelservers angeben:

```
DROP MIRROR SERVER mirror_server_name;
```

4. Löschen Sie die Partnerserverdefinition, indem Sie eine `DROP MIRROR SERVER`-Anweisung ausführen und den Namen des Partners angeben:

```
DROP MIRROR SERVER partner_server_name;
```

5. (Optional) Stoppen Sie den Datenbankserver.

## Ergebnisse

Der Spiegelserver wird gelöscht. Wenn Kopieknoten verbleiben, wird das Datenbankspiegelungssystem zu einem Scale-Out-System mit Schreibschutz.

## Beispiel

Die Partnerserver eines Spiegelungssystem wurden mit den folgenden Anweisungen erstellt:

```
CREATE MIRROR SERVER mirror_server1
AS PARTNER
connection_string='SERVER=mirror_server1;host=localhost:6871'
state_file='c:\\server1\\server1.state';
```

```
CREATE MIRROR SERVER mirror_server2
AS PARTNER
connection_string='SERVER=mirror_server2;host=localhost:6872'
state_file='c:\\server2\\server2.state';
```

```
CREATE MIRROR SERVER myprimary
AS PRIMARY
connection_string='SERVER=myprimary;HOST=localhost:6871,localhost:6872';
```

```
CREATE MIRROR SERVER mymirror  
AS MIRROR  
connection_string='SERVER=mymirror;HOST=localhost:6871,localhost:6872';
```

Führen Sie die folgende Anweisung aus, um den Spiegelserver zu löschen (mirror\_server2):

```
DROP MIRROR SERVER mirror_server2;  
DROP MIRROR SERVER mymirror
```

### Siehe auch

- „DROP MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „ALTER MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Gespiegelte Datenbanken zu laufenden Spiegelungssystemen hinzufügen

Fügen Sie eine gespiegelte Datenbank zu einem laufenden Spiegelungssystem hinzu, ohne die Verfügbarkeit der vorhandenen Server zu verringern.

### Voraussetzungen

Primär- und Spiegelserver müssen mit der Datenbankserveroption -su gestartet worden sein, um das Kennwort für die Dienstprogrammdatenbank festzulegen. Sie müssen das Kennwort für die Dienstprogrammdatenbank haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

Sie müssen auch das MANAGE MIRROR SERVER-Privileg haben.

Der Arbitrator und ein Partner des vorhandenen Spiegelungssystems müssen laufen.

Die hinzuzufügende Datenbank muss ein Transaktionslog haben.

### Kontext und Bemerkungen

Sie haben ein laufendes Spiegelungssystem und möchten die vorhandenen Partner- und Arbiterserver zum Spiegeln einer anderen Datenbank verwenden.

### Aufgabe

1. Vergewissern Sie sich, dass der Arbiterserver mit einer der folgenden Optionen gestartet wurde:
  - Datenbankserveroption -xa mit dem DBN-Parameter. Geben Sie "DBN=\*" an, damit der Arbiterserver Verbindungen für jede gespiegelte Datenbank akzeptiert. Andernfalls müssen Sie alle Datenbanken angeben, die dynamisch gestartet werden sollen und für die dieser Server als Arbitrator fungieren soll.

- Datenbankserveroption -su. Sie müssen in der Lage sein, eine Verbindung mit der Dienstprogrammdatenbank auf dem Arbiterserver herzustellen.

Zum Beispiel:

```
dbsrv16 -n mirror_arbiter -su sql -x "TCPIP(PORT=6870;DOBROAD=no)" -xf "c:\arbiter\arbiter.state" -xa "AUTH=abc;DBN=*" -o c:\arbiter\arbiter.conslog
```

2. Kopieren Sie die Datenbank, die Sie spiegeln möchten, zusammen mit ihren Transaktionslogs auf einen der vorhandenen Partnercomputer.
3. Stellen Sie eine Verbindung mit der Dienstprogrammdatenbank auf dem vorhandenen Partnerserver her. Zum Beispiel:

```
dbisql -c "UID=dba;PWD=sql;DBN=utility_db;SERVER=mirror_server1"
```

4. Starten Sie die hinzuzufügende Datenbank mit der START DATABASE-Anweisung einschließlich der Klauseln MIRROR ON und AUTOSTOP OFF. Zum Beispiel:

```
START DATABASE 'c:\\server1\\second.db'
AUTOSTOP OFF
MIRROR ON;
```

Die Datenbank wird gestartet.

5. Stellen Sie eine Verbindung mit der Datenbank her. Zum Beispiel:

```
dbisql -c UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=second
```

Erstellen Sie die Spiegelserverdefinitionen (PRIMARY, MIRROR, ARBITER und beide PARTNERS) und die Authentifizierungszeichenfolge mit SET MIRROR OPTION.

Die Authentifizierungszeichenfolge für das neue Spiegelungssystem muss mit derjenigen übereinstimmen, die durch die Option -xa des Arbiters angegeben wird. Die Hostnamen und Ports müssen mit denjenigen für die vorhandenen Partner- und Arbiterserver übereinstimmen. Die Namen der PARTNER-Spiegelserver müssen mit der Serveroption -n für die Partnerserver übereinstimmen. Die Servernamen für PRIMARY und MIRROR dürfen nicht mit Servernamen übereinstimmen, die derzeit vom System verwendet werden.

Zum Beispiel:

```
CREATE MIRROR SERVER second_primary
AS PRIMARY
connection_string='SERVER=second_primary;HOST=localhost:6871,localhost:6872';

CREATE MIRROR SERVER second_mirror
AS MIRROR
connection_string='SERVER=second_mirror;HOST=localhost:6871,localhost:6872';

CREATE MIRROR SERVER mirror_server1
AS PARTNER
connection_string='SERVER=mirror_server1;host=localhost:6871'
state_file='c:\\server1\\server1.state';
```

```
CREATE MIRROR SERVER mirror_server2
AS PARTNER
connection_string='SERVER=mirror_server2;host=localhost:6872'
state_file='c:\\server2\\server2.state';

CREATE MIRROR SERVER arbiter_server
AS ARBITER
connection_string='SERVER=mirror_arbiter;HOST=localhost:6870';

SET MIRROR OPTION authentication_string='abc';
```

6. Erstellen Sie eine Sicherung der Datenbank und kopieren Sie die Sicherung auf den zweiten Partnerserver. Verwenden Sie beispielsweise das Dienstprogramm dbbackup.

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=second" "c:\\server2"
```

7. Stellen Sie eine Verbindung mit der Dienstprogrammdatenbank auf dem zweiten Partnerserver her. Zum Beispiel:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server2;DBN=utility_db"
```

8. Starten Sie die Datenbank auf dem zweiten Partnerserver mit der START DATABASE-Anweisung einschließlich der AUTOSTOP OFF MIRROR ON-Klausel.

```
START DATABASE 'c:\\server2\\second.db'
AUTOSTOP OFF
MIRROR ON;
```

### Ergebnisse

Die neu hinzugefügte gespiegelte Datenbank muss auf beiden Partnern laufen. Überprüfen Sie, ob ein Partner die Rolle des Primärservers hat und der andere Partner die Rolle des Spiegelservers (entweder anhand des Konsolenlogs oder mit `DB_PROPERTY( 'MirrorRole' )`).

### Siehe auch

- „Datenbankserveroption -xa“ auf Seite 306

## Partnerserver verschieben

Wenn Sie einen Server in einem Datenbankspiegelungssystem auf einen anderen Server verschieben möchten, ohne das System stoppen zu müssen, löschen Sie die Spiegelserverdefinitionen des aktuellen Spiegelservers, erstellen Sie einen neuen Server und fügen Sie den neuen Server zum Spiegelungssystem hinzu.

### Voraussetzungen

Sie müssen das `MANAGE ANY MIRROR SERVER`-Privileg haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

## Kontext und Bemerkungen

Beispiele in diesem Thema referenzieren **localhost** in den Verbindungszeichenfolgen. Ersetzen Sie diese Referenzen durch die tatsächlichen Computernamen.

## Aufgabe

1. Stellen Sie eine Verbindung mit dem Partnerserver her, den Sie verschieben möchten, und vergewissern Sie sich, dass er die Rolle des Spiegelservers hat. Sie können nur den Partner mit der Rolle des Spiegelservers verschieben. Wenn der Server, den Sie verschieben möchten, der Primärserver ist, müssen Sie einen Failover initiieren, damit Primär- und Spiegelserver die Rollen tauschen.
2. Erstellen Sie ein neues Verzeichnis für den neuen Partnerserver.
3. Stellen Sie eine Verbindung mit dem Primärserver her.
4. Löschen Sie die Partnerdefinition für den zu verschiebenden Server mit der DROP MIRROR SERVER-Anweisung.

Die Spiegeldatenbank wird gestoppt. Wenn die Spiegeldatenbank die einzige laufende Datenbank auf dem Server ist, wird der Server ebenfalls gestoppt.

5. Erstellen Sie eine neue Partnerdefinition, um den Server zum neuen Partner zu machen. Führen Sie zum Beispiel folgende Anweisung aus:

```
CREATE MIRROR SERVER mirror_server3 AS PARTNER
connection_string='SERVER=demo_server3;HOST=localhost:6874'
state_file='c:\\server3\\server3.state';
```

6. Aktualisieren Sie Primär- und Spiegelserverdefinition. Führen Sie zum Beispiel folgende Anweisungen aus:

```
ALTER MIRROR SERVER mirror_demo_primary AS PRIMARY
connection_string='SERVER=mirror_demo_primary;HOST=localhost:
6871,localhost:6874';
```

```
ALTER MIRROR SERVER mirror_demo_mirror AS MIRROR
connection_string='SERVER=mirror_demo_mirror;HOST=localhost:
6871,localhost:6874';
```

7. Erstellen Sie Kopien der Primärdatenbankdatei und des dazugehörigen Transaktionslogs und fügen Sie diese zum Verzeichnis des neuen Partnerservers hinzu. Führen Sie zum Beispiel folgenden Befehl aus:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=mirror_demo"
server3
```

8. Starten Sie den neuen Partnerserver mit der Option **-xp on**, damit der neue Partner in das Spiegelungssystem eingebunden werden kann. Führen Sie zum Beispiel folgenden Befehl aus:

```
dsrv16 -n mirror_server3 -x "tcpip(PORT=6874)" -su sql "c:
\\server3\\mirror_demo.db" -xp on
```

9. Stellen Sie eine Verbindung mit dem neuen Partnerserver her und überprüfen Sie, ob er der Spiegelserver ist.

### Ergebnisse

Das Spiegelungssystem läuft mit dem neuen Spiegelserver.

### Nächste Schritte

Achten Sie darauf, die Verbindungszeichenfolgen für Clients, die Verbindungen mit dem Primärserver oder dem Spiegelserver herstellen, so zu aktualisieren, dass die Adressen beider Partner im Host-Verbindungsparameter angegeben werden.

### Siehe auch

- [„Praktische Einführung: Partnerserver verschieben“ auf Seite 1524](#)

## Arbiterserver verschieben

Verschieben Sie einen Arbiterserver, ohne das Spiegelungssystem zu stoppen, indem Sie einen neuen Server erstellen und die Arbiterspiegelserverdefinitionen so ändern, dass der neue Arbiterserver verwendet wird.

### Voraussetzungen

Sie müssen das `MANAGE ANY MIRROR SERVER`-Systemprivileg haben.

### Aufgabe

1. Starten Sie den Server, der zum Arbiterserver werden soll, mit den Optionen `-su`, `-xa` und `-xf`. Zum Beispiel:

```
dbsrv16 -n demo_arbiter2 -x "tcpip(port=6873)" -xf c:\arbiter2\arbiter2.state -xa "AUTH=abc;DBN=mirror_demo" -su sql
```

2. Stellen Sie eine Verbindung mit dem Primärserver her und ändern Sie die Arbiterspiegelserverdefinition für das Spiegelungssystem so, dass die Verbindungszeichenfolge für den neuen Arbiterserver gilt.

Führen Sie beispielsweise die folgende Anweisung aus, um die Arbiterserverdefinition in diejenige des neuen Servers zu ändern.

```
ALTER MIRROR SERVER demo_arbiter  
AS ARBITER  
connection_string='SERVER=demo_arbiter2;HOST=localhost:6873';
```

Primär- und Spiegelserver trennen die Verbindung mit dem Arbiterserver und stellen eine Verbindung mit dem neuen Arbiterserver her.

3. Warten Sie ein paar Sekunden und stoppen Sie dann den alten Arbiterserver.

## Ergebnisse

Der Arbiterserver wird auf den Primärserver verschoben.

## Nächste Schritte

Überprüfen Sie mit einem Ping die ArbiterState-Datenbankeigenschaft des Spiegelungssystems, um sicherzustellen, dass der neue Arbiterserver mit dem Spiegelungssystem verbunden ist. Führen Sie zum Beispiel folgenden Befehl aus:

```
dbping -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" -pd ArbiterState
```

Der Wert für ArbiterState ist "connected":

```
SQL Anywhere Server Ping Utility Version 16.0.4157
Type      Property      Value
-----
Database  ArbiterState    connected
```

## Siehe auch

- „Praktische Einführung: Arbiterserver verschieben“ auf Seite 1523

## Upgrade von Datenbankspiegelungssystemen

Hinweise zum Upgrade von SQL Anywhere und zum Neuaufbau einer Datenbank, die zu einem Datenbankspiegelungssystem gehört, einschließlich des Übernehmens von Supportpaketen, finden Sie unter „Upgrade und Neuaufbau in einem Datenbankspiegelungssystem“ [[SQL Anywhere 16 - Änderungen und Upgrades](#)].

## Siehe auch

- „Upgrade und Neuaufbau in einem Datenbankspiegelungssystem“ [[SQL Anywhere 16 - Änderungen und Upgrades](#)]
- „LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenimport mit der LOAD TABLE-Anweisung“ [[SQL Anywhere Server - SQL-Benutzerhandbuch](#)]

## Fehlerbehandlung: Datenbankspiegelungssysteme

Es gibt eine Reihe von erweiterten Datenbankeigenschaften, die Sie für die Fehlerbehandlung in Ihrem Spiegelungssystem verwenden können. Sie können beispielsweise die folgenden erweiterten Datenbankeigenschaften verwenden, um den Status der Datenbankserver im Spiegelungssystem zu ermitteln:

- MirrorState
- PartnerState
- ArbiterState

### Siehe auch

- [MirrorState-Datenbankeigenschaft auf Seite 780](#)
- [PartnerState-Datenbankeigenschaft auf Seite 782](#)
- [ArbiterState-Datenbankeigenschaft auf Seite 767](#)

## Fehlerbehandlung: Statusinformationsdateien von Partner und Arbiter

Ändern Sie nicht die Statusinformationsdateien. Die Partner und der Arbiter im Hochverfügbarkeitssystem mit hoher Verfügbarkeit verwalten jeweils eine Statusinformationsdatei, in der der Status des Spiegelungssystems aus Sicht des betreffenden Servers aufgezeichnet wird.

Die Statusinformationsdatei wird beim Start verwendet, um die vom Server einzunehmende Rolle zu bestimmen. Der lokale Status des Servers wird mit dem der anderen Server im Datenbankspiegelungssystem verglichen.

Sie müssen immer für jeden Server im Spiegelungssystem eine Statusinformationsdatei angeben. Verwenden Sie hierzu die `state_file`-Option der `CREATE MIRROR SERVER`-Anweisung. Siehe „[CREATE MIRROR SERVER-Anweisung](#)“ [*SQL Anywhere Server - SQL-Referenzhandbuch*].

Die Statusinformationsdatei enthält die folgenden Informationen:

Feld	Beschreibung
<b>Owner</b>	Gibt an, welcher Datenbankserver der Primärserver ist
<b>State</b>	Enthält den Synchronisationsstatus (entweder <code>synchronizing</code> oder <code>synchronized</code> ) um anzuzeigen, ob der Server Logseiten empfängt oder auf dem letzten Stand ist. Siehe „ <a href="#">Synchronisationsstatus für Spiegelungssysteme</a> “ auf Seite 1480.
<b>Mode</b>	Gibt den Synchronisationsmodus ( <code>synchronous</code> , <code>asynchronous</code> oder <code>page</code> ) an. Siehe „ <a href="#">Datenbankspiegelungsmodi</a> “ auf Seite 1477.
<b>Sequence</b>	Enthält einen Wert, der angibt, wie oft ein Failover im Datenbankspiegelungssystem aufgetreten ist. Die Sequenznummer steigt bei jedem Rollenwechsel an. Mit ihr kann bestimmt werden, ob die Einschätzung eines Servers zum Status des Spiegelungssystems aktuell ist. Siehe „ <a href="#">Datenbankspiegelung</a> “ auf Seite 1467.

Der Inhalt einer Statusinformationsdatei könnte beispielsweise folgendermaßen aussehen:

```
[demo]
Owner=server2
State=synchronizing
Mode=asynchronous
Sequence=35
```

Wenn keine Statusinformationsdatei existiert, wird sie automatisch erstellt. Statusinformationsdateien sollten nur vom Datenbankserver geändert werden. Wenn Sie jedoch ein Zurücksetzen oder ein erneutes Deployment eines Spiegelserversystems vornehmen, löschen Sie die Statusdateien.

## Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall

Die Schritte zum Wiederherstellen nach einem Primärserver-Ausfall hängen davon ab, welchen Synchronisationsmodus Sie in Ihrem Datenbankspiegelungssystem verwenden.

### Synchroner Modus

Wenn die Spiegelung im synchronen Modus ausgeführt wird, ist bei allen Transaktionen, die auf dem Primärserver vorhanden sind, garantiert, dass sie ebenfalls auf dem Spiegelserver festgeschrieben sind. Der Spiegelserver kann in fast allen Fällen als neuer Primärserver übernehmen, ohne dass ein Benutzereingriff erforderlich wäre.

#### Hinweis

In seltenen Fällen, wenn ein Primärserver die Verbindung sowohl mit dem Spiegelserver als auch mit dem Arbiterserver verliert, während ein Checkpoint gesetzt wird, kann die Synchronisation fehlschlagen, wenn die beiden Server das nächste Mal eine Verbindung herstellen. Der Spiegelserver gibt eine Fehlermeldung aus, wonach das Transaktionslog nicht mit dem Primärserver übereinstimmt, und die Spiegeldatenbank wird gestoppt. In einem solchen Fall müssen Sie die Datenbank auf dem aktuellen Primärserver manuell auf den Spiegelserver kopieren oder dort sichern, damit der Spiegelserver erfolgreich gestartet und synchronisiert werden kann.

### Asynchroner oder Asynchron-Ganzseiten-Modus

Im asynchronen oder Asynchron-Ganzseiten-Modus ist der Failover vom Primärserver zum Spiegelserver nicht automatisch, weil der Spiegelserver möglicherweise nicht alle festgeschriebenen Transaktionen enthält, die am Primärserver angewendet wurden. Außer wenn Sie "autofailover" angegeben haben, kann ein Spiegelserver beim Ausfall des Primärservers nicht standardmäßig Eigentümer einer Datenbank werden, wenn das System im asynchronen Modus läuft. Wenn der ausgefallene Server neu gestartet wird, erkennt er, ob Transaktionen verloren gegangen sind. Wenn Transaktionen verloren gegangen sind, schreibt er eine Meldung an das Datenbankserver-Meldungslog und fährt die Datenbank herunter.

Wenn Sie den ursprünglichen Spiegelserver als den neuen Primärserver starten, haben Sie zwei Optionen, um die Datenbankdateien auf beiden Servern in denselben Status zu bekommen:

- Kopieren Sie die Datenbank- und Transaktionslogdateien vom ursprünglichen Primärserver auf den Spiegelserver und starten Sie anschließend den Spiegelserver als den neuen Primärserver. Sie können einen Server zwingen, Primärserver zu werden, indem Sie die ALTER DATABASE-Anweisung mit der FORCE START-Klausel verwenden.
- Führen Sie eine Sicherung (mit dbbackup) auf dem ursprünglichen Spiegelserver durch. Kopieren Sie diese Dateien auf den ursprünglichen Primärserver und starten Sie anschließend die Datenbankserver. Siehe „Sicherungsdienstprogramm (dbbackup)“ auf Seite 886.

### Siehe auch

- „ALTER DATABASE-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbankspiegelungsmodi“ auf Seite 1477

## Fehlerbehandlung: Primärserver kann nicht neu gestartet werden

Zwingen Sie den Spiegelserver, als Primärserver zu übernehmen, wenn alle anderen Versuche, das Problem zu lösen, fehlgeschlagen sind. Bei dieser Methode wird die ALTER DATABASE-Anweisung mit der FORCE START-Klausel verwendet, sodass festgeschriebene Transaktionen verloren gehen können.

### Voraussetzungen

Sie müssen die durch die Datenbankserveroption -gd angegebenen Privilegien haben (standardmäßig das SERVER OPERATOR-Systemprivileg).

Die Partnerserver müssen mit der Datenbankoption -su gestartet worden sein, damit Sie eine Verbindung mit der Dienstprogrammdatenbank auf dem Spiegelserver herstellen können.

Sie haben bereits versucht, das Problem zu lösen, indem Sie den Primärserver manuell stoppen und neu starten sowie eine ALTER DATABASE-Anweisung mit der SET PARTNER FAILOVER-Klausel ausführen.

### Kontext und Bemerkungen

Sie können die ALTER DATABASE FORCE START-Anweisung nur verwenden, wenn die folgenden Bedingungen erfüllt sind:

- Der Primärserver ist ausgefallen (z.B. aufgrund eines Hardwareausfalls).
- Der Spiegelserver konnte nicht als Primärserver übernehmen.
- Sie können eine Verbindung mit der Dienstprogrammdatenbank auf dem Spiegeldatenbankserver herstellen.

#### Vorsicht

Die Verwendung der FORCE START-Klausel kann zum Verlust von Transaktionen führen, wenn der Primärserver Transaktionen enthält, die der Spiegelserver nicht hat.

Es wird empfohlen, dass Sie den Primärserver neu starten und ALTER DATABASE mit der SET PARTNER FAILOVER-Klausel ausführen, um einen Failover ohne Verlust von Transaktionen zu erzwingen. Verwenden Sie die FORCE START-Klausel nur als letztes Mittel, wenn der Primärserver nicht neu gestartet werden kann.

### Aufgabe

1. Stoppen Sie die Spiegeldatenbank und, wenn möglich, den Spiegelserver.
2. Wenn Datenbank- und Transaktionslogdatei vom Primärserver verfügbar sind, sichern Sie sie und validieren Sie die gesicherten Kopien. Andernfalls müssen Sie das Transaktionslog sichern und validieren.
3. Wenn die Datenbankdatei und die Transaktionslogdatei vom Primärserver gültig sind, kopieren Sie beide Dateien auf den Spiegelserver.

Wenn die Datenbankdatei vom Primärserver ungültig, aber die Transaktionslogdatei gültig ist, gehen Sie folgendermaßen vor:

- a. Übernehmen Sie die Logdatei vom Primärserver in eine Sicherung der Spiegeldatenbank und validieren Sie die Datenbank.
  - b. Kopieren Sie Datenbank- und Transaktionslogdatei auf den Spiegelserver.
4. Starten Sie die Datenbank auf dem Spiegelserver (oder starten Sie den Spiegelserver neu) mit aktivierter Spiegelung. Geben Sie bei einem Neustart des Spiegelserver die Datenbankoption -su an, um eine Verbindung mit der Dienstprogrammdatenbank herstellen zu können.
  5. Stellen Sie eine Verbindung mit der Dienstprogrammdatenbank, utility\_db, auf dem Spiegelserver her.
  6. Führen Sie eine ALTER DATABASE FORCE START-Anweisung aus, um zu erzwingen, dass der Spiegelserver zum Primärserver wird.

## Ergebnisse

Der Spiegelserver wird zum neuen Primärserver.

## Nächste Schritte

Wenn Sie den ausgefallenen Primärservercomputer durch einen anderen Primärservercomputer ersetzen möchten, müssen Sie den ausgefallenen Partner löschen und einen neuen Partner für den neuen Computer hinzufügen. Die Verbindungszeichenfolgen für Primär- und Spiegelserver müssen aktualisiert werden. Siehe „[Partnerserver verschieben](#)“ auf Seite 1494

## Beispiel

Mit der folgenden Anweisung wird der Spiegelserver für die Datenbank *mymirroredb.db* gezwungen, zum Primärserver zu werden.

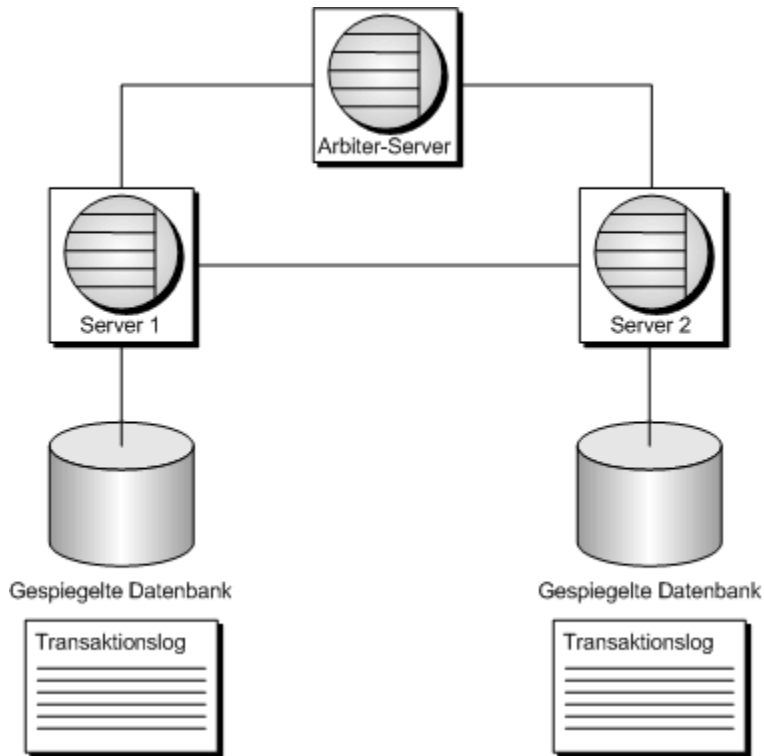
```
ALTER DATABASE mymirroredb FORCE START;
```

## Siehe auch

- „Fehlerbehandlung: Primärserver kann nicht neu gestartet werden“ auf Seite 1500
- „ALTER DATABASE-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Benutzerinitiiertes Rollentausch (Failover)“ auf Seite 1488
- „Verbindung mit der Dienstprogrammdatenbank herstellen“ auf Seite 147

## Fehlerbehandlung: Serverausfälle in Datenbankspiegelungssystemen

Die folgenden Szenarien fördern das Verständnis darüber, was passiert, wenn ein Server in einem Spiegelungssystem ausfällt. Diese Szenarien verwenden die folgende Datenbank-Spiegelungskonfiguration, die aus Server 1, Server 2 und einem Arbiterserver besteht, die im synchronen Modus ausgeführt werden:



Sie können jederzeit die Datenbankeigenschaften MirrorState, PartnerState und ArbiterState verwenden, um den Status der Datenbankserver im Spiegelungssystem zu ermitteln.

Die Kommunikation zwischen den Primär-, Spiegel- und Arbiterservern wird in einem Spiegelungssystem regelmäßig überprüft. Eine Unterbrechung der Kommunikation zwischen den drei Servern kann darauf zurückzuführen sein, dass einer oder mehrere Server nicht verfügbar sind und/oder das Netzwerk zwischen den Servern ausgefallen ist.

### Szenario 1: Primärserver fällt aus

1. Der Primärserver (Server 1) fällt aus. Alle Clientverbindungen werden getrennt.
2. Der Arbitr und Server 2 erkennen, dass Server 1 nicht mehr verfügbar ist.
3. Der Arbitr und Server 2 erreichen das Quorum, und Server 2 wird der Primärserver.
4. Server 2 beginnt, Clientverbindungen anzunehmen.

Wenn Sie im asynchronen oder Asynchron-Ganzseiten-Modus ausführen und "autofailover" nicht angegeben haben, müssen Sie in diesem Szenario möglicherweise eine Kopie der Datenbank machen und den noch betriebsbereiten Server neu starten, bevor Clients wieder eine Verbindung herstellen können.

Weitere Hinweise zur Wiederherstellung, wenn der Primärserver ausgefallen ist, finden Sie unter [„Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall“ auf Seite 1499](#).

**Szenario 2: Primärserver fällt aus und startet anschließend erneut**

1. Der Primärserver (Server 1) fällt aus. Alle Clientverbindungen werden getrennt.
2. Arbitr- und Spiegelserver (Server 2) erkennen, dass der Primärserver (Server 1) nicht mehr verfügbar ist.
3. Der Arbitr und Server 2 erreichen das Quorum, und Server 2 wird der Primärserver.
4. Server 2 beginnt, Clientverbindungen anzunehmen.
5. Server 1 kommt wieder online und verbindet erneut mit Server 2 und dem Arbiterserver.
6. Server 1 verlangt ein Quorum, aber Server 2 ist bereits der Primärserver.
7. Server 1 ist der Spiegelserver und wartet auf Änderungen von Server 2.
8. Server 2 sendet Änderungen an Server 1.

Falls Server 2 ausfällt, bevor Server 1 alle Transaktionen von Server 2 empfangen hat, kann Server 1 nicht den Status "synchronized" erreichen. Er muss warten, dass Server 2 wieder verfügbar wird, damit er die fehlenden Transaktionen erhalten und anwenden kann.

Weitere Hinweise zur Wiederherstellung, wenn der Primärserver ausgefallen ist, finden Sie unter [„Fehlerbehandlung: Wiederherstellung nach einem Primärserver-Ausfall“ auf Seite 1499](#).

**Szenario 3: Spiegelserver fällt aus**

1. Der Spiegelserver (Server 2) fällt aus.
2. Arbiterserver und Server 1 erkennen, dass der Spiegelserver (Server 2) nicht mehr verfügbar ist.

Clientverbindungen sind nicht betroffen. Sie können sich weiterhin mit dem Primärserver verbinden. Wenn jedoch entweder Server 1 oder der Arbiterserver ausfällt, können die Clients keine Verbindungen herstellen.

**Szenario 4: Spiegelserver fällt aus und startet anschließend erneut**

1. Der Spiegelserver (Server 2) fällt aus.
2. Clientverbindungen sind nicht betroffen, da es keine Änderung in der Verfügbarkeit gibt. Sie können sich weiterhin mit dem Primärserver verbinden. Wenn jedoch entweder Server 1 oder der Arbiterserver ausfällt, können Clients keine Verbindungen herstellen.
3. Server 2 kommt wieder online und verbindet erneut mit Server 1 und dem Arbiterserver.
4. Server 2 verlangt ein Quorum, aber Server 1 ist bereits der Primärserver.
5. Server 2 ist der Spiegelserver und wartet auf Änderungen von Server 1.
6. Server 1 sendet Änderungen an Server 2.

Clientverbindungen sind nicht betroffen, da es keine Änderung in der Verfügbarkeit gibt. Sie verbinden sich weiterhin mit Server 1.

### Szenario 5: Arbiterserver fällt aus

1. Server 1 (Primärserver) und Server 2 (Spiegelserver) erkennen, dass der Arbiterserver ausgefallen ist.
2. Beide Server stehen weiterhin zur Verfügung. Clientverbindungen werden nicht getrennt.

Wenn der Arbiterserver wieder online geht, erkennen Server 1 und Server 2 dies und beginnen, mit ihm zu kommunizieren. Für Clients gibt es keine Änderung in der Datenbankverfügbarkeit.

Wenn Server 1 oder Server 2 ausfällt, während kein Arbiterserver vorhanden ist, kann der andere Server alleine kein Quorum erreichen und die Datenbank ist nicht verfügbar.

### Szenario 6: Arbiterserver startet erneut

1. Der Arbiterserver geht wieder online und verbindet sich erneut mit Server 1 und Server 2.

Clientverbindungen sind nicht betroffen, da es keine Änderung in der Verfügbarkeit gibt.

### Siehe auch

- [MirrorState-Datenbankeigenschaft auf Seite 780](#)
- [ArbiterState-Datenbankeigenschaft auf Seite 767](#)
- [PartnerState-Datenbankeigenschaft auf Seite 782](#)

## Fehlerbehandlung: Unterbrochene Verbindungen bei Datenbankspiegelung

Wenn in einem Datenbankspiegelungssystem Verbindungen zwischen Datenbankservern unterbrochen werden, gelten folgende Hinweise:

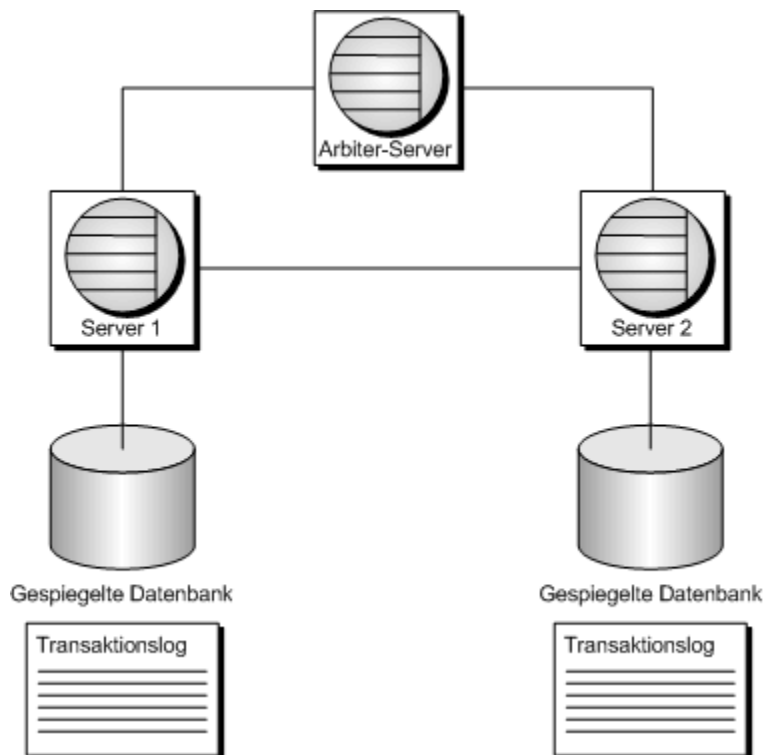
- Die Zeit, die ein Server benötigt, um die Unterbrechung einer Netzwerkverbindung zu erkennen, hängt von folgenden Faktoren ab:
  1. Art der Unterbrechung der Verbindung. Wenn ein Netzkabel am Computer abgezogen wird, erkennen einige Betriebssysteme dieses Problem sofort und unterbrechen somit die logische Verbindung. Wenn das Problem auf einen Fehler in einem Netzwerkgerät zurückzuführen ist, wird das Problem vom Server wahrscheinlich weniger rasch erkannt.
  2. Einstellung des Verfügbarkeits-Timeouts in der Spiegelserver-Verbindungszeichenfolge.
- Damit der Primärserver die Eigentümerschaft einer gespiegelten Datenbank behält, muss er mit mindestens einem der anderen Server (Spiegel- oder Arbiterserver) verbunden sein. Wenn Verbindungen zu den beiden anderen Servern verlorengehen, wird die Datenbank neu gestartet und der Primärserver wartet, bis er mindestens eine dieser Verbindungen wiederherstellen kann, um ihren Status zu überprüfen.
- Die Verbindungen zwischen Servern werden automatisch wieder aufgenommen, wenn das Problem, das eine Unterbrechung der Verbindung verursacht, behoben ist.
- Bis ein Server eine Unterbrechung der Verbindung erkennt, behält er die Rolle, die ihm zuvor zugeordnet wurde. Dieses Verhalten kann dazu führen, dass zwei Server versuchen, kurze Zeit als

Primärserver zu agieren, wenn der Server, der zuvor der Spiegelserver war, eine unterbrochene Verbindung mit dem Primärserver erkennt, bevor der Primärserver feststellt, dass seine Verbindung mit dem Spiegelserver unterbrochen wurde. Die erste Aktualisierung auf dem ursprünglichen Primärserver blockiert, wenn der Server versucht, die Änderungen an den anderen Server zu senden, sodass das Potenzial für einen Verlust von Transaktionen begrenzt wird, wenn diese Situation eintreten sollte.

Wenn der ursprüngliche Primärserver eine Unterbrechung der Verbindung mit dem ursprünglichen Spiegelserver erkennt und den Zustand des Arbiters überprüft, stellt er fest, dass ein Failover aufgetreten ist, und startet die Datenbank neu.

- Wenn ein als Spiegelserver agierender Server seine Datenbank neu starten muss, wird der Zugriff auf die Datenbank auf diesem Server blockiert, bis eine Verbindung mit dem Primärserver wiederaufgenommen wurde.
- Netzwerkausfälle können sich, abhängig von der Topologie des Netzwerks, auf Client- und Spiegelserververbindungen auswirken.

Die folgenden Szenarien fördern das Verständnis darüber, was vorgeht, wenn in einem Spiegelungssystem Verbindungen ausfallen. Diese Szenarien verwenden die folgende Datenbank-Spiegelungskonfiguration, die aus Server 1, Server 2 und einem Arbiterserver besteht, die im synchronen Modus ausgeführt werden:



Sie können jederzeit die Datenbankeigenschaften MirrorState, PartnerState und ArbiterState verwenden, um den Status der Datenbankserver im Spiegelungssystem zu bestimmen.

### **Szenario 7: Verbindung zwischen dem Primärserver und dem Arbiterserver ist getrennt**

1. Die Verbindung zwischen dem Primärserver (Server 1) und dem Arbiterserver wird unterbrochen.
2. Server 1 und der Arbiterserver stellen fest, dass die Verbindung zwischen den beiden Servern unterbrochen ist.
3. Sowohl der Primär- als auch der Spiegelserver bleiben verfügbar. Clientverbindungen werden nicht getrennt. Server 1 sendet weiterhin Änderungen an Server 2.
  - Wenn Server 1 ausfällt oder die Verbindung zum Spiegelserver (Server 2) verliert, wird Server 2 zum Primärserver, wenn er immer noch eine Verbindung mit dem Arbiterserver hat.
  - Wenn Server 1 seine Verbindung zum Server 2 und zum Arbiterserver verliert, ist die Datenbank auf Server 1 nicht mehr verfügbar. Server 1 führt einen Neustart der Datenbank durch und wartet auf die erneute Verbindung mit dem Arbiterserver und dem Server 2.
  - Wenn Server 1 und Server 2 die Verbindung mit dem Arbiterserver verlieren, während noch eine Verbindung untereinander besteht, ist das Verhalten dasselbe wie unter [Szenario 5: Arbiterserver fällt aus](#) beschrieben.

### **Szenario 8: Verbindung zwischen dem Spiegelserver und dem Arbiterserver ist getrennt**

1. Die Verbindung zwischen dem Spiegelserver (Server 2) und dem Arbiterserver wird unterbrochen.
2. Server 2 und der Arbiterserver stellen fest, dass die Verbindung zwischen den beiden Servern unterbrochen ist.
3. Sowohl der Primär- als auch der Spiegelserver bleiben verfügbar. Clientverbindungen werden nicht getrennt.
4. Server 1 sendet weiterhin Änderungen an Server 2.
5. Server 1 und Server 2 warten darauf, dass die Verbindung zum Arbiterserver wieder aufgebaut wird.
  - Wenn Server 2 ausfällt oder seine Verbindung zum Server 1 verliert, sind Clientverbindungen zu Server 1 nicht betroffen, da es keine Änderung in der Verfügbarkeit gibt. Clientverbindungen zum Server 2 gehen verloren.
  - Wenn Server 1 und Server 2 die Verbindung mit dem Arbiterserver verlieren, während noch eine Verbindung untereinander besteht, ist das Verhalten dasselbe wie unter [Szenario 5: Arbiterserver fällt aus](#) beschrieben.
6. Der Arbiterserver geht wieder online und Server 1 und Server 2 stellen eine Verbindung zu ihm her.

### **Szenario 9: Verbindung zwischen dem Primärserver und dem Spiegelserver ist getrennt**

1. Die Verbindung zwischen dem Primärserver (Server 1) und dem Spiegelserver (Server 2) wird unterbrochen.
2. Server 1 und Server 2 erkennen die Unterbrechung der Verbindung, aber möglicherweise zu unterschiedlichen Zeiten. Beide Server prüfen den Arbiterserver-Status und unternehmen dann ihre Aktion basierend auf den vom Arbiterserver erhaltenen Antworten:

- Wenn Server 1 die unterbrochene Verbindung zuerst entdeckt, aktualisiert er den Arbiterserverstatus, um anzuzeigen, dass er weiterhin der Primärserver ist und die Datenbank von Server 2 möglicherweise nicht mehr aktuell ist. Wenn Server 2 den Arbiterserverstatus prüft, ermittelt er, dass Server 1 immer noch der Primärserver ist. Server 2 führt einen Neustart seiner Datenbank durch. Server 2 wartet auf die Wiederherstellung der Verbindung zum Server 1, bevor er den Zugriff auf die Datenbank zulässt.
- Wenn Server 2 die unterbrochene Verbindung zuerst entdeckt, aktualisiert er den Arbiterserverstatus, um anzuzeigen, dass ein Failover aufgetreten ist und Server 2 zum Primärserver wird. Wenn Server 1 den Arbiterserverstatus prüft, erfährt er, dass ein Failover aufgetreten ist und Server 2 jetzt als Primärserver agiert. Server 1 führt einen Neustart seiner Datenbank durch und wartet auf die Wiederherstellung der Verbindung zum Server 2, bevor er den Zugriff auf die Datenbank zulässt.

### **Szenario 10: Verbindung vom Primärserver zum Spiegelserver und Arbiterserver ist getrennt**

1. Die Verbindung zwischen dem Primärserver (Server 1) und dem Spiegelserver (Server 2) wird unterbrochen und die Verbindung zwischen dem Primärserver (Server 1) und dem Arbiterserver ebenfalls.
2. Server 1 erkennt, dass der Arbiterserver und Server 2 nicht mehr verfügbar sind. Server 1 führt einen Neustart seiner Datenbank durch und wartet auf die Wiederherstellung der Verbindung zu den anderen Servern. Alle Clientverbindungen werden getrennt.
3. Der Arbiterserver und Server 2 erkennen, dass Server 1 nicht mehr verfügbar ist.
4. Der Arbiterserver und Server 2 erreichen das Quorum, und Server 2 wird der Primärserver.

Für den Arbiterserver und Server 2 ist das Verhalten gleich wie unter [Szenario 1: Primärserver fällt aus](#) beschrieben.

5. Server 2 beginnt, Clientverbindungen anzunehmen.
6. Server 1 kommt wieder online und verbindet sich erneut mit Server 2 und dem Arbiterserver.
7. Server 1 ist der Spiegelserver und wartet auf Änderungen vom Server 2.
8. Server 2 sendet Änderungen an Server 1.

### **Szenario 11: Verbindung vom Spiegelserver zum Primärserver und zum Arbiterserver ist getrennt**

1. Die Verbindung zwischen dem Spiegelserver (Server 2) und dem Primärserver (Server 1) und die Verbindung zwischen dem Spiegelserver (Server 2) und dem Arbiterserver werden unterbrochen.
2. Server 2 erkennt, dass der Arbiterserver und Server 1 nicht mehr verfügbar sind. Server 2 führt einen Neustart der Datenbank durch und wartet auf die erneute Verbindung mit dem Primärserver und dem Arbiterserver. Alle Clientverbindungen zum Server 2 sind getrennt.

Clientverbindungen zum Primärserver sind nicht betroffen. Clients können sich weiterhin mit dem Primärserver verbinden.

3. Der Arbiter und Server 1 erkennen, dass Server 2 nicht mehr verfügbar ist.

Für den Arbiterserver und Server 1 ist das Verhalten gleich wie unter [Szenario 3: Spiegelserver fällt aus](#) beschrieben.

4. Server 1 aktualisiert den Arbiterserverstatus, um anzuzeigen, dass Server 2 nicht mehr aktuell ist.
5. Server 2 kommt wieder online und verbindet erneut mit Server 1 und dem Arbiterserver.
6. Server 2 übernimmt die Rolle des Spiegelserver und wartet auf Änderungen vom Server 1.
7. Server 1 sendet Änderungen an Server 2.

### **Szenario 12: Verbindungen vom Arbiterserver zum Primär- und Spiegelserver sind getrennt**

1. Die Verbindung zwischen dem Arbiterserver und dem Primärserver sowie die Verbindung zwischen dem Arbiterserver und dem Spiegelserver (Server 2) sind unterbrochen.
2. Wenn die Verbindung mit dem Arbiterserver verloren geht, ist das Verhalten gleich wie unter [Szenario 5: Arbiterserver fällt aus](#) beschrieben.
3. Wenn die Verbindungen wiederhergestellt sind, ist das Verhalten gleich wie unter [Szenario 6: Arbiterserver startet erneut](#) beschrieben.

### **Szenario 13: Verbindungen zwischen allen Servern sind getrennt**

1. Die Verbindungen zwischen allen Servern sind unterbrochen.
2. Der Primärserver (Server 1), Spiegelserver (Server 2) und Arbiterserver stellen fest, dass die Verbindung zu den anderen Servern unterbrochen ist.
3. Server 1 trennt alle Clients und führt einen Neustart der Datenbank durch.
4. Server 2 trennt alle Clients und führt einen Neustart der Datenbank durch.
5. Server 1 und Server 2 warten auf die Wiederherstellung der Verbindung mit den anderen Servern, um ihre Rollen zu ermitteln.
6. Wenn die Verbindungen wieder aufgenommen werden, ermitteln Server 1 und Server 2 ihre Rollen basierend auf ihrem Status und dem Status der anderen Server.

### **Siehe auch**

- [LivenessTimeout-Verbindungseigenschaft auf Seite 724.](#)
- [MirrorState-Datenbankeigenschaft auf Seite 780](#)
- [ArbiterState-Datenbankeigenschaft auf Seite 767](#)
- [PartnerState-Datenbankeigenschaft auf Seite 782](#)

## Praktische Einführung: Datenbankspiegelungssysteme erstellen

Diese praktische Einführung enthält Anweisungen dazu, wie Sie eine Datenbankspiegelung einrichten und auf einen Failover reagieren. Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

### Privilegien

Sie müssen die folgenden Systemprivilegien haben:

- `MANAGE ANY MIRROR SERVER`
- `BACKUP DATABASE`
- `CREATE TABLE`
- `SERVER OPERATOR`

### Siehe auch

- Im Verzeichnis `%SQLANYSAMPI6%\SQLAnywhere\DBMirror` finden Sie ein Beispiel, in dem ein Datenbankspiegelungssystem verwendet wird.

## Lektion 1: Datenbankspiegelungssysteme erstellen

Erstellen Sie ein Spiegelungssystem.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

### Aufgabe

1. Erstellen Sie folgende Verzeichnisse: `c:\server1`, `c:\server2` und `c:\arbiter`.
2. Erstellen Sie eine Datenbank namens `mirror_demo.db`, die Daten aus der Beispieldatenbank enthält und ein Transaktionslog hat. Datenbanken ohne Transaktionslog können nicht im Spiegelungsmodus gestartet werden. Führen Sie den folgenden Befehl aus:

```
newdemo c:\server1\mirror_demo.db
```

3. Starten Sie den ersten Datenbankserver. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n mirror_server1 -x "tcpip(PORT=6871)" -su sql "c:\server1\mirror_demo.db" -xp on
```

- **-n** Benennt den Datenbankserver.
  - **-su** Gibt das Kennwort für die Dienstprogrammdatenbank an. Es wird empfohlen, dass Sie die Option -su einbeziehen, um das Kennwort für die Dienstprogrammdatenbank anzugeben. Auf diese Weise können Sie ggf. eine Verbindung mit der Dienstprogrammdatenbank herstellen, um den Datenbankserver herunterzufahren. Siehe „[Einen Datenbankserver in einem Spiegelungssystem stoppen](#)“ auf Seite 1490 und „[Fehlerbehandlung: Primärserver kann nicht neu gestartet werden](#)“ auf Seite 1500.
  - **-x** Gibt den Port an, auf dem der Datenbankserver läuft
  - **-xp on** Gibt an, dass der Datenbankserver für die Beteiligung an einem Datenbankspiegelungssystem zur Verfügung steht.
4. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server1"
```

5. Definieren Sie die Partnerserver und den Arbiterserver für die Datenbank mithilfe der CREATE MIRROR SERVER-Anweisung.

Führen Sie die folgenden Anweisungen aus, um mirror\_server1 und mirror\_server2 als Partnerserver im Datenbankspiegelungssystem zu definieren:

```
CREATE MIRROR SERVER mirror_server1
AS PARTNER
connection_string='SERVER=mirror_server1;host=localhost:6871'
state_file='c:\\server1\\server1.state';

CREATE MIRROR SERVER mirror_server2
AS PARTNER
connection_string='SERVER=mirror_server2;host=localhost:6872'
state_file='c:\\server2\\server2.state';
```

Mit den nachstehenden Anweisungen wird Folgendes definiert:

- mirror\_demo\_primary als alternativer Servername für mirror\_server1. mirror\_demo\_primary ist der Name, unter dem sich Clients mit dem als Primärserver fungierenden Datenbankserver verbinden.
- mirror\_demo\_mirror als alternativer Servername für mirror\_server2. mirror\_demo\_mirror ist der Name, unter dem sich Clients mit dem als Spiegelserver fungierenden Datenbankserver verbinden.

Die Rollen des Primär- und des Spiegelservers sind zum Konfigurieren der Datenbankserver im System erforderlich: Die Namen, die Sie diesen Servern geben, werden als alternative Servernamen benutzt, wenn Clients eine Verbindung zu den Datenbankservern herstellen. Jeder der beiden Partnerserver kann als Primär- oder Spiegelserver agieren.

```
CREATE MIRROR SERVER mirror_demo_primary
AS PRIMARY
connection_string='SERVER=mirror_demo_primary;HOST=localhost:
6871,localhost:6872';
CREATE MIRROR SERVER mirror_demo_mirror
AS MIRROR
connection_string='SERVER=mirror_demo_mirror;HOST=localhost:
6871,localhost:6872';
```

Führen Sie die folgende SQL-Anweisung aus, um den Arbiterserver für das Datenbankspiegelungssystem zu definieren:

```
CREATE MIRROR SERVER demo_arbiter
AS ARBITER
connection_string = 'SERVER=demo_arbiter;HOST=localhost:6870';
```

6. Legen Sie die Authentifizierungszeichenfolge für die Datenbank fest. Führen Sie die folgende Anweisung aus:

```
SET MIRROR OPTION authentication_string='abc';
```

7. Verwenden Sie das Sicherungsdienstprogramm (dbbackup), um die Datenbankdatei und das Transaktionslog aus c:\server1 in c:\server2 zu kopieren. Führen Sie den folgenden Befehl aus:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=mirror_demo" c:
\server2
```

8. Starten Sie den zweiten Partnerserver. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n mirror_server2 -x "tcpip(PORT=6872;DOBRoad=no)" -su sql "c:
\server2\mirror_demo.db" -xp on
```

9. Starten Sie den Arbiterserver. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n demo_arbiter -su sql -x "tcpip(PORT=6870;DOBRoad=no)" -xf "c:
\arbiter\arbiter.state" -xa "AUTH=abc;DBN=mirror_demo"
```

- **-xf** Gibt den Speicherort der Statusinformationsdatei für den Arbiterserver an
- **-xa** Gibt den Namen der gespiegelten Datenbank(en) und die Authentifizierungszeichenfolge (in diesem Fall abc) für den Arbiterserver an. Diese Authentifizierungszeichenfolge muss in einem Datenbankspiegelungssystem von allen Servern (Arbiter-, Primär- und Spiegelserver) verwendet werden.

10. Starten Sie Interactive SQL und stellen Sie eine Verbindung mit dem Primärserver her, indem Sie den alternativen Servernamen für den Primärserver verwenden. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:
6871,localhost:6872"
```

11. Fügen Sie Daten zur Datenbank hinzu. Führen Sie die folgenden Anweisungen aus:

```
CREATE TABLE test (col1 INTEGER, col2 CHAR(32));
INSERT INTO test VALUES(1, 'Hello from server1');
COMMIT;
```

12. (Optional) Wenn Sie den Namen des Datenbankservers ermitteln möchten, mit dem Sie verbunden sind, verwenden Sie die ServerName-Datenbankserviceeigenschaft. Führen Sie die folgende Anweisung aus:

```
SELECT PROPERTY( 'ServerName' );
```

13. Schließen Sie alle Interactive SQL-Fenster.

## Ergebnisse

Das Datenbankspiegelungssystem läuft.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 2: Testen, ob das Datenbankspiegelungssystem korrekt läuft“ auf Seite 1512](#).

## Siehe auch

- [„Datenbankspiegelung“ auf Seite 1467](#)
- [„Datenbankspiegelungssysteme einrichten“ auf Seite 1480](#)
- [„Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen“ auf Seite 1516](#)
- Ein Spiegelungsbeispiel befindet sich in `%SQLANYSAMPI6%\SQLAnywhere\DBMirror`.

## Lektion 2: Testen, ob das Datenbankspiegelungssystem korrekt läuft

Testen Sie, ob das Datenbankspiegelungssystem korrekt läuft, indem Sie Datenbank- und Datenbankservereigenschaften überprüfen.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Datenbankspiegelungssysteme erstellen“ auf Seite 1509](#).

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen“](#).

### Aufgabe

- Führen Sie den nachstehenden Befehl aus, um Folgendes anzuzeigen:
  - Die Spiegelserverrolle des Datenbankservers
  - Der Name des Datenbankservers, mit dem Sie verbunden sind
  - Die Zustände von Partner, Spiegel- und Arbiterserver

```
dbping -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" -ps ServerName -pd MirrorRole,MirrorState,PartnerState,ArbiterState
```

## Ergebnisse

Informationen zu den Datenbankeigenschaften werden zurückgegeben.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 3: Rollentausch in einem Datenbankspiegelungssystem erzwingen](#)“ auf Seite 1513.

## Siehe auch

- [MirrorRole-Datenbankeigenschaft](#) auf Seite 779
- [„Verbindungsparameter ServerName \(Server\)“](#) auf Seite 383
- [MirrorState-Datenbankeigenschaft](#) auf Seite 780
- [PartnerState-Datenbankeigenschaft](#) auf Seite 782
- [ArbiterState-Datenbankeigenschaft](#) auf Seite 767
- [„Ping-Dienstprogramm \(dbping\)“](#) auf Seite 955

## Lektion 3: Rollentausch in einem Datenbankspiegelungssystem erzwingen

Zwingen Sie die Server, die Rollen zu tauschen, ohne dass das Spiegelungssystem gestoppt werden muss.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankspiegelungssysteme erstellen](#)“ auf Seite 1509.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

### Aufgabe

1. Stellen Sie eine Verbindung mit dem Primärserver her. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872"
```

2. Verwenden Sie die ServerName-Datenbankservereigenschaft, um den Namen des Servers zu ermitteln, der derzeit Primärserver ist.

```
SELECT PROPERTY( 'ServerName' );
```

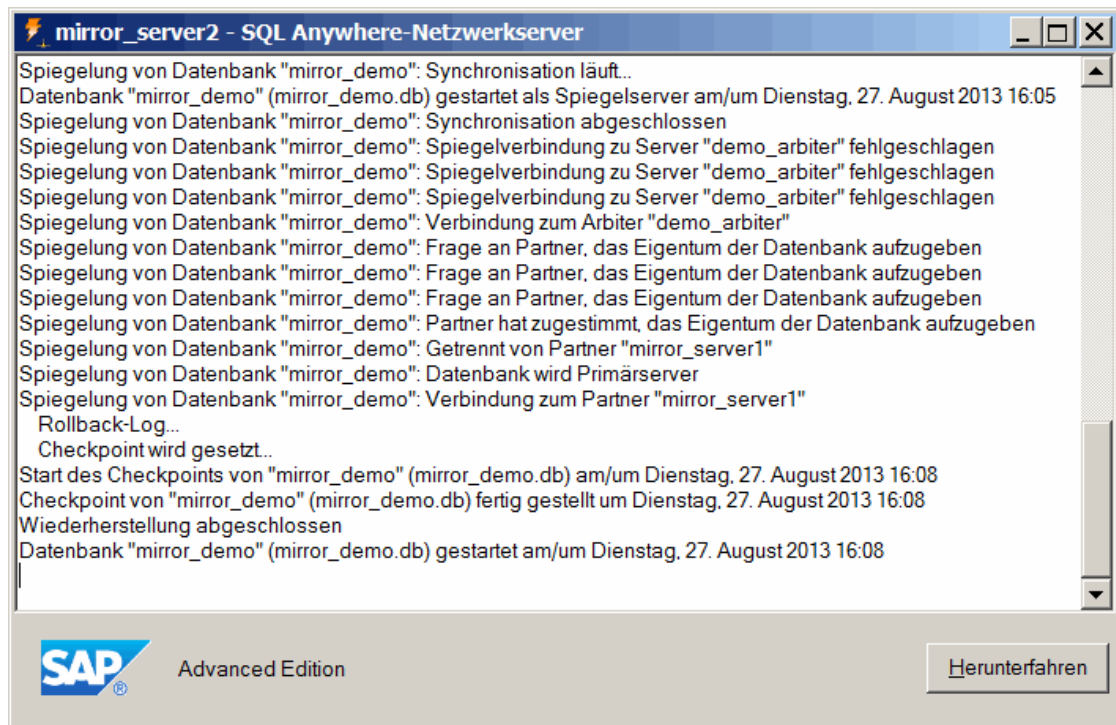
Der Name des Primärservers wird angezeigt (mirror\_server1).

Die ServerName-Datenbankservereigenschaft gibt den tatsächlichen Namen des Servers zurück, nicht den alternativen Namen.

3. Initiieren Sie den Failover, indem Sie die ALTER DATABASE SET PARTNER FAILOVER-Anweisung ausführen:

```
ALTER DATABASE SET PARTNER FAILOVER;
```

Verbindungen zum Primärserver werden geschlossen. Im Meldungsfenster des Datenbankservers für server2 wird eine Meldung angezeigt, dass er der neue Primärserver ist.



4. Stellen Sie eine Verbindung mit dem aktuellen Primärserver her:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872"
```

5. Führen Sie die folgende Anweisung aus, um zu prüfen, ob der Server, der zuvor als Spiegelserver agiert hat (mirror\_server2), nun als Primärserver agiert:

```
SELECT PROPERTY ( 'ServerName' );
```

6. Führen Sie die folgende Anweisung aus, um sicherzugehen, dass alle Transaktionen in der Spiegeldatenbank gespiegelt wurden:

```
SELECT * FROM test;
```

7. Trennen Sie die Verbindung zu Interactive SQL.

### Ergebnisse

Die Partnerserver tauschen die Rollen.

### Nächste Schritte

Gehen Sie weiter zu „[Lektion 4: Das Datenbankspiegelungssystem stoppen](#)“ auf Seite 1515.

**Siehe auch**

- „Fehlerbehandlung: Unterbrochene Verbindungen bei Datenbankspiegelung“ auf Seite 1504

## Lektion 4: Das Datenbankspiegelungssystem stoppen

Stoppen Sie das Spiegelungssystem, indem Sie die Server in der folgenden Reihenfolge stoppen: den Spiegelserver, den Primärserver und den Arbiterserver.

**Voraussetzungen**

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankspiegelungssysteme erstellen](#)“ auf Seite 1509.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

**Aufgabe**

1. Stoppen Sie das Datenbankspiegelungssystem, indem Sie den Spiegelserver, den Primärserver und schließlich den Arbiterserver stoppen. Führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

```
dbstop -y -c "UID=DBA;PWD=sql;SERVER=mirror_server2;DBN=utility_db"
```

```
dbstop -y -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=utility_db"
```

```
dbstop -y -c "UID=DBA;PWD=sql;SERVER=demo_arbiter;DBN=utility_db"
```

2. (Optional) Löschen Sie die Verzeichnisse `c:\server1`, `c:\server2` und `c:\arbiter`.

**Ergebnisse**

Das Spiegelungssystem wird gestoppt.

**Nächste Schritte**

Gehen Sie weiter zu „[Lektion 5: \(Optional\) Das Spiegelungssystem neu starten](#)“ auf Seite 1515.

## Lektion 5: (Optional) Das Spiegelungssystem neu starten

Starten Sie das Spiegelungssystem, indem Sie Partner- und Arbiterserver starten.

**Voraussetzungen**

Alle Datenbankserver im Spiegelungssystem müssen gestoppt sein.

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankspiegelungssysteme erstellen](#)“ auf Seite 1509.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

### Aufgabe

1. Führen Sie den folgenden Befehl aus, um den ersten Partner neu zu starten:

```
dbsrv16 -n mirror_server1 -x "tcPIP(PORT=6871;DOBRoad=no)" -su sql "c:\server1\mirror_demo.db" -xp on
```

2. Führen Sie den folgenden Befehl aus, um den zweiten Partner neu zu starten:

```
dbsrv16 -n mirror_server2 -x "tcPIP(PORT=6872;DOBRoad=no)" -su sql "c:\server1\mirror_demo.db" -xp on
```

3. Führen Sie den folgenden Befehl aus, um den Arbitr neu zu starten:

```
dbsrv16 -n demo_arbiter -su sql -x "tcPIP(PORT=6870;DOBRoad=no)" -xf "c:\arbiter\arbiter.state" -xa "AUTH=abc;DBN=mirror_demo"
```

### Ergebnisse

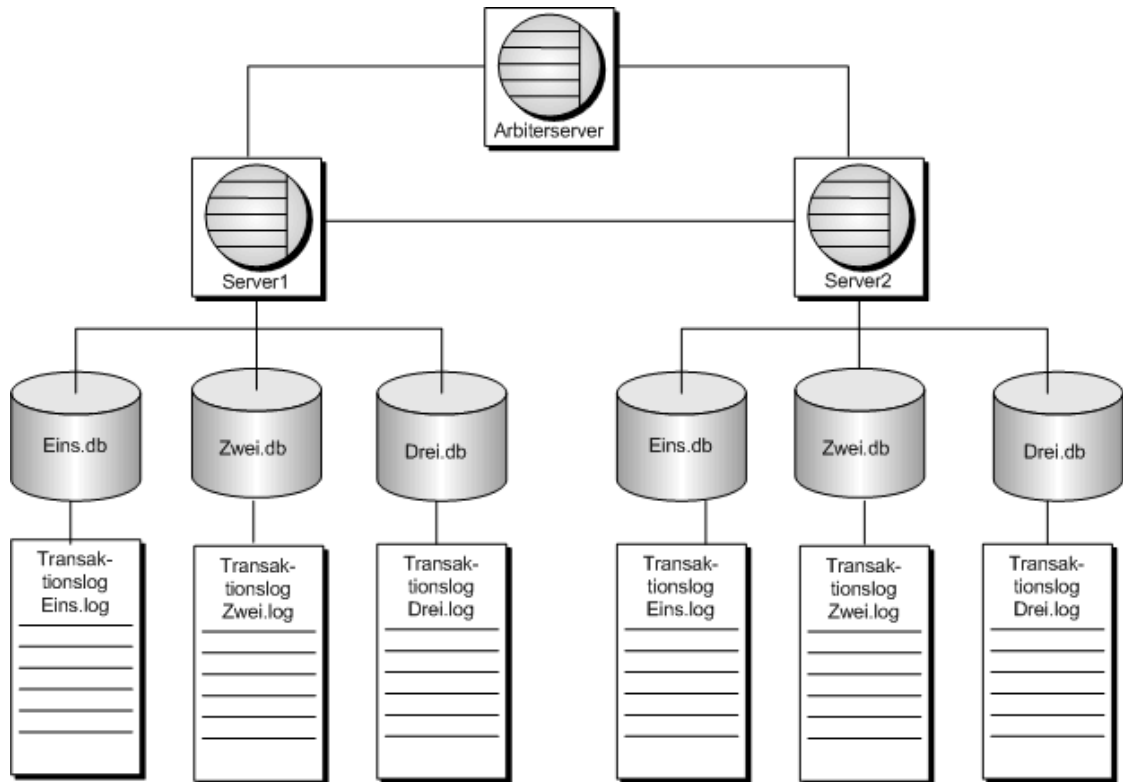
Das Spiegelungssystem wird neu gestartet.

### Siehe auch

- [Ablauf beim Starten eines Datenbankspiegelungssystems auf Seite 1469](#)

## Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen

In dieser Konfiguration hosten Primär- und Spiegelserver jeweils drei einzelne Datenbanken, die an Spiegelungssystemen teilnehmen. Alle drei Spiegelungssysteme kommunizieren mit demselben Arbiterserver. Jedes Spiegelungssystem verwendet eindeutige alternative Servernamen, die mithilfe der PRIMARY- und MIRROR-Klausel der CREATE MIRROR SERVER-Anweisung angegeben werden. Bei dieser Art von Konfiguration können die Primär-, Spiegel- und Arbiterserver jeweils auf separaten Computern laufen.



Wenn der Primärserver ausfällt, findet ein Rollentausch statt. Der Spiegelserver wird Eigentümer der Datenbanken und wird zum Primärserver. Der Client muss wieder eine Verbindung mit dem Primärserver herstellen. Es muss nur der alternative Servername angegeben werden, um die Verbindung mit dem Primärserver wiederherzustellen. Die Konfiguration bietet auch Schutz vor dem Ausfall einer einzelnen Datenbank. Wenn eine Datenbank, die auf dem Primärserver läuft, ausfällt, findet ein Rollenwechsel statt und der Spiegelserver wird Eigentümer der ausgefallenen Datenbank. Der Spiegelserver wird nur für diese Datenbank zum Primärserver. Der Client muss eine Verbindung zum Primärserver für diese Datenbank unter Verwendung des alternativen Servernamens wieder herstellen.

#### Hinweis

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

#### Privilegien

Sie müssen die Systemprivilegien **MANAGE ANY MIRROR SERVER**, **CREATE TABLE** und **SERVER OPERATOR** haben.

In dieser praktischen Einführung muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

### Siehe auch

- „Gespiegelte Datenbanken zu laufenden Spiegelungssystemen hinzufügen“ auf Seite 1492
- In `%SQLANYSAMPI6%\SQLAnywhere\DBMirror` finden Sie ein Beispiel für die Verwendung einer Datenbankspiegelung in Verbindung mit einem Scale-Out-System. Das Beispiel kann auf einem einzigen oder auf mehreren Computern ausgeführt werden.

## Lektion 1: Datenbankspiegelungssysteme mit drei Datenbanken und einem Arbiterserver erstellen

Erstellen Sie ein Spiegelungssystem mit drei gespiegelten Datenbanken, die alle denselben Arbiterserver verwenden.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

### Aufgabe

1. Erstellen Sie folgende Verzeichnisse:

- `c:\server1`
- `c:\server2`
- `c:\arbiter`

2. Erstellen Sie Kopien der SQL Anywhere 16-Beispieldatenbank (*demo.db*) mithilfe der Datei *newdemo.bat*. Führen Sie den folgenden Befehl aus:

```
newdemo.bat c:\server1\one.db
```

3. Führen Sie den folgenden Befehl aus:

```
newdemo.bat c:\server1\two.db
```

4. Führen Sie vom Verzeichnis `c:\server1` aus den folgenden Befehl aus:

```
newdemo.bat c:\server1\three.db
```

5. Starten Sie den Datenbankserver namens `server_1`:

```
dbsrv16 -n server1 -x tcpip(PORT=6871) -su sql c:\server1\one.db -xp on c:\server1\two.db -xp on c:\server1\three.db -xp on
```

Es wird empfohlen, dass Sie die Option `-su` einbeziehen, um das Kennwort für die Dienstprogrammdatenbank anzugeben. Auf diese Weise können Sie ggf. eine Verbindung mit der

Dienstprogramm Datenbank herstellen, um den Datenbankserver herunterzufahren. Siehe „[Einen Datenbankserver in einem Spiegelungssystem stoppen](#)“ auf Seite 1490.

6. Stellen Sie von Interactive SQL aus eine Verbindung zur Datenbank "one" her und definieren Sie die erforderlichen Spiegelungsobjekte:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=server1;DBN=one"
```

- a. Definieren Sie server1 als Partnerserver für Datenbank "one":

```
CREATE MIRROR SERVER server1
AS PARTNER
connection_string='SERVER=server1;host=localhost:6871'
state_file='c:\server1\server1state.txt';
```

- b. Definieren Sie den Datenbankserver primary\_one als logischen Primärserver für Datenbank "one":

```
CREATE MIRROR SERVER primary_one
AS PRIMARY
connection_string='SERVER=primary_one;host=localhost:6871,localhost:
6872';
```

- c. Definieren Sie server2 als Partnerserver für Datenbank "one":

```
CREATE MIRROR SERVER server2
AS PARTNER
connection_string='SERVER=server2;host=localhost:6872'
state_file='c:\server2\server2state.txt';
```

- d. Definieren Sie den Datenbankserver mirror\_one als logischen Spiegelserver für die Datenbank "one":

```
CREATE MIRROR SERVER mirror_one
AS MIRROR
connection_string='SERVER=mirror_one;host=localhost:6871,localhost:
6872';
```

- e. Definieren Sie den Arbiterserver:

```
CREATE MIRROR SERVER arbiter
AS ARBITER
connection_string='SERVER=arbiter;HOST=localhost:6870';
```

- f. Setzen Sie die Spiegelungsoptionen für das Datenbankspiegelungssystem:

```
SET MIRROR OPTION authentication_string='abc';
```

- g. Trennen Sie die Verbindung zu Interactive SQL.

- h. Erstellen Sie eine Sicherungskopie der Datenbank im Verzeichnis c:\server2:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=server1;DBN=one" c:\server2
```

7. Stellen Sie von Interactive SQL aus eine Verbindung zur Datenbank "two" her und definieren Sie die erforderlichen Spiegelungsobjekte:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=server1;DBN=two"
```

- a. Definieren Sie server1 als Partnerserver für Datenbank "two":

```
CREATE MIRROR SERVER server1
AS PARTNER
connection_string='SERVER=server1;host=localhost:6871'
state_file='c:\\server1\\server1state.txt';
```

- b. Definieren Sie den Datenbankserver primary\_two als logischen Primärserver für Datenbank "two":

```
CREATE MIRROR SERVER primary_two
AS PRIMARY
connection_string='SERVER=primary_two;host=localhost:6871,localhost:
6872';
```

- c. Definieren Sie server2 als Partnerserver für Datenbank "two":

```
CREATE MIRROR SERVER server2
AS PARTNER
connection_string='SERVER=server2;host=localhost:6872'
state_file='c:\\server2\\server2state.txt';
```

- d. Definieren Sie den Datenbankserver mirror\_two als logischen Spiegelserver für die Datenbank "two":

```
CREATE MIRROR SERVER mirror_two
AS MIRROR
connection_string='SERVER=mirror_two;host=localhost:6871,localhost:
6872';
```

- e. Definieren Sie den Arbiterserver:

```
CREATE MIRROR SERVER arbiter
AS ARBITER
connection_string='SERVER=arbiter;HOST=localhost:6870';
```

- f. Setzen Sie die Spiegelungsoptionen für das Datenbankspiegelungssystem:

```
SET MIRROR OPTION authentication_string='def';
```

- g. Trennen Sie die Verbindung zu Interactive SQL.

- h. Erstellen Sie eine Sicherungskopie der Datenbank im Verzeichnis c:\\server2:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=server1;DBN=two" c:\\server2
```

8. Stellen Sie von Interactive SQL aus eine Verbindung zur Datenbank "three" her und definieren Sie die erforderlichen Spiegelungsobjekte:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=server1;DBN=three"
```

- a. Definieren Sie server1 als Partnerserver für Datenbank "three":

```
CREATE MIRROR SERVER server1
AS PARTNER
connection_string='SERVER=server1;host=localhost:6871'
state_file='c:\\server1\\server1state.txt';
```

- b. Definieren Sie den Datenbankserver primary\_three als logischen Primärserver für Datenbank "three":

```
CREATE MIRROR SERVER primary_three
AS PRIMARY
connection_string='SERVER=primary_three;host=localhost:6871,localhost:
6872';
```

- c. Definieren Sie server2 als Partnerserver für Datenbank "three":

```
CREATE MIRROR SERVER server2
AS PARTNER
connection_string='SERVER=server2;host=localhost:6872'
state_file='c:\\server2\\server2state.txt';
```

- d. Definieren Sie den Datenbankserver mirror\_three als logischen Spiegelserver für die Datenbank "three":

```
CREATE MIRROR SERVER mirror_three
AS MIRROR
connection_string='SERVER=mirror_three;host=localhost:6871,localhost:6872';
```

- e. Definieren Sie den Arbiterserver:

```
CREATE MIRROR SERVER arbiter
AS ARBITER
connection_string='SERVER=arbiter;HOST=localhost:6870';
```

- f. Setzen Sie die Spiegelungsoptionen für das Datenbankspiegelungssystem:

```
SET MIRROR OPTION authentication_string='ghi';
```

- g. Trennen Sie die Verbindung zu Interactive SQL.

- h. Erstellen Sie eine Sicherungskopie der Datenbank im Verzeichnis c:\server2:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=server1;DBN=three" c:\server2
```

9. Starten Sie den Datenbankserver namens server\_2:

```
dbsrv16 -n server2 -x tcpip(PORT=6872) -su sql c:\server2\one.db -xp on c:\server2\two.db -xp on c:\server2\three.db -xp on
```

10. Starten Sie den Arbiterserver.

```
dbsrv16 -n arbiter -su sql -x tcpip(port=6870) -xf c:\arbiter\arbiterstate.txt -xa "AUTH=abc,def,ghi;DBN=one,two,three"
```

## Ergebnisse

Nach dem Starten von server2 wird im Meldungsfenster des Datenbankservers server1 angezeigt, dass server1 der Primärserver im Spiegelungssystem für die Datenbanken one, two und three ist. Außerdem wird im Meldungsfenster angezeigt, dass die Spiegeldatenbanken für one, two und three (Partner) mit server1 verbunden sind.

Im Meldungsfenster des Arbiterdatenbankservers wird angezeigt, dass server1 und server2 verbunden sind.

## Nächste Schritte

Gehen Sie weiter zu „[Lektion 2: Das Datenbankspiegelungssystem verwenden und testen](#)“ auf Seite 1522.

## Lektion 2: Das Datenbankspiegelungssystem verwenden und testen

Testen Sie die Konfiguration des Datenbankspiegelungssystems, indem Sie einen Failover initiieren.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe „[Lektion 1: Datenbankspiegelungssysteme mit drei Datenbanken und einem Arbiterserver erstellen](#)“ auf Seite 1518.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: „[Praktische Einführung: Datenbankspiegelungssysteme mit mehreren Datenbanken und einem gemeinsamen Arbiterserver erstellen](#)“.

### Aufgabe

1. Führen Sie den folgenden Befehl aus, um Interactive SQL zu starten und eine Verbindung mit der Datenbank one auf dem Primärserver herzustellen:

```
dbisql -c "UID=DBA;PWD=sql;Server=primary_one;LINKS=TCPIP"
```

2. Fügen Sie Beispieldaten zur Datenbank hinzu, indem Sie die folgenden Anweisungen ausführen:

```
CREATE TABLE test (col1 INTEGER, col2 CHAR(32));  
INSERT INTO test VALUES(1, 'Hello from server1');  
COMMIT;
```

3. Bestimmen Sie, mit welchem Datenbankserver Sie verbunden sind, indem Sie die folgende Anweisung ausführen:

```
SELECT PROPERTY( 'ServerName' );
```

Der Name des Primärservers wird angezeigt.

4. Trennen Sie die Verbindung zu Interactive SQL.
5. Initiieren Sie einen Failover. Führen Sie den folgenden Befehl aus:

```
dbstop -y -c "UID=DBA;PWD=sql;Server=server1"
```

Wenn eine Warnmeldung angezeigt wird, wonach der Datenbankserver immer noch eine Verbindung hat, klicken Sie auf **Ja**, um ihn herunterzufahren. Im Meldungsfenster des Datenbankservers für server2 wird eine Meldung angezeigt, dass er der neue Primärserver ist.

6. Starten Sie Interactive SQL erneut, indem Sie den folgenden Befehl ausführen:

```
dbisql -c "UID=DBA;PWD=sql;Server=primary_one;LINKS=tcPIP"
```

7. Führen Sie die folgende Anweisung aus, um festzustellen, ob Sie nun mit server2 verbunden sind:

```
SELECT PROPERTY ( 'ServerName' );
```

- Führen Sie die folgende Anweisung aus, um sicherzugehen, dass alle Transaktionen in die Spiegeldatenbank kopiert wurden:

```
SELECT * FROM test;
```

- Trennen Sie die Verbindung mit Interactive SQL und fahren Sie die Datenbankserver `arbiter` und `server2` herunter.

## Ergebnisse

Der Failover des Datenbankspiegelungssystems war erfolgreich, sodass `server2` zum Primärserver geworden ist. Anschließend wird das Datenbankspiegelungssystem heruntergefahren.

## Nächste Schritte

(Optional) Löschen Sie die Verzeichnisse `c:\server1`, `c:\server2` und `c:\arbiter`.

# Praktische Einführung: Arbiterserver verschieben

Verschieben Sie einen Arbiterserver, ohne das Spiegelungssystem zu stoppen, indem Sie einen neuen Server erstellen und die Arbiterserverdefinitionen so ändern, dass der neue Arbiterserver verwendet wird.

## Voraussetzungen

Diese praktische Einführung basiert auf dem unter „[Praktische Einführung: Datenbankspiegelungssysteme erstellen](#)“ beschriebenen Datenbankspiegelungssystem.

Sie müssen die Systemprivilegien `MANAGE ANY MIRROR SERVER` und `SERVER OPERATOR` haben.

## Kontext und Bemerkungen

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

## Aufgabe

- Starten Sie den Server, der zum Arbiterserver werden soll, mit den Optionen **-su**, **-xa** und **-xf**. Zum Beispiel:

```
mkdir arbiter2

dbsrv16 -n demo_arbiter2 -x "tcpip(port=6873)" -xf c:
\arbiter2\arbiter2.state -xa "AUTH=abc;DBN=mirror_demo" -su sql
```

Option	Beschreibung
-su	Kennwort für die Dienstprogrammdatenbank.
-xa	Datenbankname und Authentifizierungszeichenfolge des Arbiterservers.
-xf	Speicherort der Statusinformationsdatei für das Spiegelungssystem.

2. Stellen Sie eine Verbindung mit dem Primärserver her und ändern Sie die Arbiterserverdefinition für das Spiegelungssystem.

- a. Führen Sie den folgenden Befehl aus, um eine Verbindung mit dem Primärserver herzustellen.

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872"
```

- b. Führen Sie den folgenden Befehl aus, um die Arbiterserverdefinition in diejenige des neuen Servers zu ändern.

```
ALTER MIRROR SERVER demo_arbiter
AS ARBITER
connection_string='SERVER=demo_arbiter2;HOST=localhost:6873';
```

Primär- und Spiegelserver trennen die Verbindung mit dem Arbiterserver und stellen eine Verbindung mit dem neuen Arbiterserver her.

3. Warten Sie ein paar Sekunden und stoppen Sie dann den alten Arbiterserver.

```
dbstop -y -c "UID=DBA;PWD=sql;SERVER=demo_arbiter;HOST=localhost:6870;DBN=utility_db"
```

4. Überprüfen Sie mit einem Ping die ArbiterState-Datenbankeigenschaft des Spiegelungssystems, um sicherzustellen, dass der neue Arbiterserver mit dem Spiegelungssystem verbunden ist. Führen Sie den folgenden Befehl aus:

```
dbping -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" -pd ArbiterState
```

Der Wert für die ArbiterState-Eigenschaft ist "connected":

```
SQL Anywhere Server Ping Utility Version 16.0.0.1403
Type      Property      Value
-----
Database  ArbiterState   connected
```

### Ergebnisse

Der Arbiterserver wird auf den Primärserver verschoben.

## Praktische Einführung: Partnerserver verschieben

Wenn Sie einen Server in einem Datenbankspiegelungssystem auf einen anderen Server verschieben möchten, ohne das System stoppen zu müssen, löschen Sie die Spiegelserverdefinitionen des aktuellen

Spiegelserver, erstellen Sie einen neuen Server und fügen Sie den neuen Server zum Spiegelungssystem hinzu.

## Voraussetzungen

Diese praktische Einführung basiert auf dem unter „[Praktische Einführung: Datenbankspiegelungssysteme erstellen](#)“ beschriebenen Datenbankspiegelungssystem.

Sie müssen das `MANAGE ANY MIRROR SERVER`-Privileg haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

## Kontext und Bemerkungen

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung muss jedoch jeder Datenbankserver auf einem separaten Computer installiert werden. Verweise auf **localhost** in den Verbindungszeichenfolgen müssen in die tatsächlichen Computernamen geändert werden.

## Aufgabe

1. Stellen Sie eine Verbindung mit dem zu verschiebenden Partnerserver `mirror_server2` her und vergewissern Sie sich, dass er die Rolle des Spiegelserver hat. Sie können nur einen Partner mit der Rolle des Spiegelserver verschieben. Wenn der Server, mit dem Sie eine Verbindung herstellen möchten, als Primärserver fungiert, müssen Sie einen Failover initiieren, damit Spiegelserver und Primärserver die Rollen tauschen. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server2;HOST=localhost:6872"
SELECT DB_PROPERTY( 'MirrorRole' )
```

Die Spiegelungsrolle für den aktuellen Server wird zurückgegeben.

- Wenn **Mirror** zurückgegeben wird, fungiert `mirror_server2` derzeit als Spiegelserver.
- Wenn **Primary** zurückgegeben wird, fungiert `mirror_server2` derzeit als Primärserver und Sie müssen einen Failover initiieren, um `mirror_server2` zum Spiegelserver zu machen. Führen Sie den folgenden Befehl aus, um einen Failover zu initiieren:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server2;HOST=localhost:6871,localhost:6872" ALTER DATABASE SET PARTNER FAILOVER
```

Die beiden Partnerserver tauschen die Rollen.

2. Erstellen Sie ein neues Verzeichnis für den neuen Partnerserver. Führen Sie den folgenden Befehl aus:

```
mkdir c:\server3
```

3. Stellen Sie eine Verbindung mit dem Primärserver her. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872"
```

4. Löschen Sie die Partnerdefinition des zu verschiebenden Servers mit der DROP MIRROR SERVER-Anweisung. Führen Sie die folgende Anweisung aus:

```
DROP MIRROR SERVER mirror_server2;
```

Die Spiegeldatenbank wird gestoppt. Wenn die Spiegeldatenbank die einzige laufende Datenbank auf dem Server ist, wird der Server ebenfalls gestoppt.

5. Erstellen Sie eine neue Partnerdefinition für den Server, der der neue Partnerserver werden soll. Führen Sie die folgenden Anweisungen aus:

```
CREATE MIRROR SERVER mirror_server3 AS PARTNER  
connection_string='SERVER=demo_server3;HOST=localhost:6874'  
state_file='c:\\server3\\server3.state';
```

6. Aktualisieren Sie Primär- und Spiegelserverdefinition. Führen Sie die folgenden Anweisungen aus:

```
ALTER MIRROR SERVER mirror_demo_primary AS PRIMARY  
connection_string='SERVER=mirror_demo_primary;HOST=localhost:  
6871,localhost:6874';  
ALTER MIRROR SERVER mirror_demo_mirror AS MIRROR  
connection_string='SERVER=mirror_demo_mirror;HOST=localhost:  
6871,localhost:6874';
```

7. Erstellen Sie Kopien der gespiegelten Datenbankdatei und des Transaktionslogs vom Primärserver und fügen Sie sie zum Verzeichnis `c:\\server3` hinzu. Führen Sie dazu den folgenden Befehl aus:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=mirror_demo" c:  
\\server3
```

8. Starten Sie den neuen Partnerserver mit der Option **-xp on**, damit er in das Spiegelungssystem eingebunden wird. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n mirror_server3 -x "tcpip(PORT=6874)" -su sql "c:  
\\server3\\mirror_demo.db" -xp on
```

9. Stellen Sie eine Verbindung mit dem neuen Partnerserver her und überprüfen Sie, ob er der Spiegelserver ist. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server3;HOST=localhost:6874"  
"SELECT DB_PROPERTY( 'MirrorRole' )"
```

Dieser Befehl gibt **Mirror** zurück.

### Ergebnisse

Das Spiegelungssystem läuft mit dem neuen Spiegelserver.

### Nächste Schritte

Achten Sie darauf, die Verbindungszeichenfolgen für Clients, die Verbindungen mit dem Primärserver oder dem Spiegelserver herstellen, so zu aktualisieren, dass die Adressen beider Partner im Host-Verbindungsparameter angegeben werden.

Die folgende Zeichenfolge ist für die Verbindung mit der Datenbank auf dem Primärserver erforderlich:

```
'UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6873';
```

Die folgende Zeichenfolge ist für die Verbindung mit der Datenbank auf dem Spiegelserver erforderlich:

```
'UID=DBA;PWD=sql;SERVER=mirror_demo_mirror;HOST=localhost:6871,localhost:6873';
```

## SQL Anywhere Veritas Cluster Server-Agenten

### Hinweis

Die SQL Anywhere Veritas Cluster Server-Agenten erfordern eine separate Lizenz.

Ein **Cluster** ist eine Gruppe von Computern, **Knoten** genannt, die zusammenarbeiten, um eine Reihe von Anwendungen auszuführen. Clients, die sich mit in einem Cluster laufenden Anwendungen verbinden, behandeln den Cluster wie ein einziges System. Wenn ein Knoten ausfällt, übernehmen andere Knoten im Cluster automatisch die Dienste, die der ausgefallene Knoten zur Verfügung gestellt hat. Clients bemerken den Ausfall des Knotens nicht, außer möglicherweise ein leichtes Nachlassen der Verfügbarkeit (die Zeit, die zur Wiederaufnahme der Dienste auf den verbliebenen Knoten erforderlich ist),

Wenn Sie SQL Anywhere in einem Cluster verwenden, gehen nicht-festgeschriebene Transaktionen verloren, wenn ein anderer Knoten für eine ausgefallene Datenbank bzw. eine ausgefallenen Datenbankserver übernimmt, und Clients müssen sich nach einem Failover mit der Datenbank erneut verbinden.

SQL Anywhere unterstützt eine Reihe von Cluster-Umgebungen, bei der die Cluster-Software jede beliebige Anwendung zu einem generischen Ressourcensubjekt mit automatischem Failover machen kann, was eine hohe Verfügbarkeit gewährleistet. Ein Failover kann allerdings nur beim Datenbankserver-Prozess durchgeführt werden, die Monitor- und Steuerungsprozesse werden nur teilweise erfasst.

Weitere Hinweise finden Sie unter <http://www.sybase.com/detail?id=1034743>.

Cluster-Software enthält in der Regel eine API, um benutzerdefinierte, für eine bestimmte Anwendung geltende Ressourcen zu erstellen. SQL Anywhere bietet zwei benutzerdefinierte Failover-Ressourcen für den Veritas Cluster Server: SAServer und SADBatabase. Der SAServer-Agent ist für den Datenbankserver-Failover zuständig, während der SADBatabase-Agent für den Failover einer bestimmten Datenbankdatei zuständig ist. Sie können, abhängig von Ihrer Anwendung, einen oder beide Agenten verwenden.

Um die SQL Anywhere Veritas Cluster Server-Agenten zu verwenden, müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdateiabank muss bei allen Systemen im Cluster identisch sein.

Der SADatabase-Agent verwendet die Dienstprogrammdatenbank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdatenbank haben. Legen Sie das Kennwort für die Dienstprogrammdatenbank fest, indem Sie beim Starten des Datenbankservers die Datenbankserveroption `-su` angeben.

Unter Unix ist der VCS-Agent unter `$SQLANY16/vcsagent/saserver` installiert.

Es gibt drei Möglichkeiten, um einen neuen Agenten für den Veritas Cluster Server zu konfigurieren und ihn hinzuzufügen:

1. Den Cluster-Manager verwenden
2. Befehlszeilen-Dienstprogramme verwenden
3. Mit einem Texteditor die *main.cf*-Konfigurationsdateien bearbeiten

Die Anleitungen in den folgenden Abschnitten verwenden den Cluster-Manager.

Hinweise zu den verfügbaren Dienstprogrammen finden Sie in der Dokumentation *Veritas Cluster Server Administration Guide (in englischer Sprache)*.

Wenn Sie die Datei *main.cf* mit einem Texteditor manuell konfigurieren möchten, müssen Sie vor dem Bearbeiten der Datei *main.cf* alle Veritas Cluster Server-Dienste stoppen. Andernfalls treten die Änderungen nicht in Kraft.

### Siehe auch

- „Getrennt lizenzierbare Komponenten“ [*SQL Anywhere 16 - Einführung*]
- „Datenbankserveroption `-su`“ auf Seite 289

## SAServer-Agentenkonfiguration

### Den SAServer-Agenten einrichten

Der SAServer-Agent steuert den Failover eines SQL Anywhere-Datenbankservers auf einen anderen Knoten im Cluster.

#### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdatenbank muss bei allen Systemen im Cluster identisch sein.

Der SADatabase-Agent verwendet die Dienstprogrammdatenbank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdatenbank haben. Sie können das Kennwort für die Dienstprogrammdatenbank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption `-su` angeben.

- Unter Unix ist der VCS-Agent unter `$SQLANY16/vcsagent/saserver` installiert.

## Aufgabe

1. Fahren Sie alle SQL Anywhere-Datenbankserver herunter, die auf Knoten im Cluster ausgeführt werden.
2. Wählen Sie einen Knoten im Cluster aus und erstellen Sie auf diesem Knoten ein Verzeichnis namens `SAServer` im `%VCS_HOME%\bin`-Verzeichnis. Möglicherweise finden Sie in diesem Ordner weitere Veritas Cluster Server-Agenten (z.B. NIC und IP).
3. Kopieren Sie die folgenden Dateien aus dem Verzeichnis `%SQLANY16%\VCSAgent\SAServer` in das `SAServer`-Verzeichnis, das Sie in Schritt 2 erstellt haben:
  - `Online.pl`
  - `Offline.pl`
  - `Monitor.pl`
  - `Clean.pl`
  - `SAServer.xml`
4. Kopieren Sie die Datei `%VCS_HOME%\bin\VCSdefault.dll` in das `%VCS_HOME%\bin\SAServer`-Verzeichnis und benennen Sie sie in `SAServer.dll` um.
5. Kopieren Sie die Datei `%SQLANY16%\VCSAgent\SAServer\SAServerTypes.cf` in das `%VCS_HOME%\conf\config`-Verzeichnis.
6. Wiederholen Sie die Schritte 1 - 5 bei allen anderen Knoten im Cluster.
7. Starten Sie den Veritas Cluster Server-Manager und geben Sie Ihren Benutzernamen und das Kennwort ein, um sich mit dem Cluster zu verbinden.
8. Fügen Sie den SAServer-Agenten hinzu:
  - a. Klicken Sie auf **File » Import Types**.
  - b. Navigieren Sie zu `%VCS_HOME%\conf\config\SAServerTypes.cf` und klicken Sie auf **Import**

## Ergebnisse

Der SAServer-Agent wird eingerichtet.

## Siehe auch

- „Datenbankserveroption `-su`“ auf Seite 289

## Datenbankserver für Failover mit dem SAServer-Agenten einrichten

Sie können einen Datenbankserver für Failover auf einen anderen Datenbankserver einrichten, indem Sie den Veritas Cluster Server einsetzen.

### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdateiabank muss bei allen Systemen im Cluster identisch sein.

Der SADBDatabase-Agent verwendet die Dienstprogrammdateiabank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdateiabank haben. Sie können das Kennwort für die Dienstprogrammdateiabank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption `-su` angeben.

- Unter Unix ist der VCS-Agent unter `$$SQLANY16/vcsagent/saserver` installiert.

Beim Stoppen eines Netzwerkserver müssen Sie eine Verbindungszeichenfolge mit einer Benutzer-ID angeben, die Berechtigungen zum Stoppen des Servers besitzt. Standardmäßig ist zum Stoppen des Netzwerkserver das `SERVER OPERATOR`-Systemprivileg erforderlich. Sie können die Server-Befehlszeilenoption `-gk` verwenden, um das Standardverhalten zu ändern.

### Aufgabe

1. Starten Sie den Veritas Cluster Server-Manager und geben Sie Ihren Benutzernamen und das Kennwort zur Herstellung einer Verbindung ein.

2. Fügen Sie SAServer als eine Ressource einer Dienstgruppe hinzu:

- a. Klicken Sie auf **Edit » Add » Resource**.
- b. Klicken Sie in der Liste **Resource Type** auf **SAServer**.

Wenn SAServer in der Liste **Resource Type** unter Windows nicht angezeigt wird, müssen Sie möglicherweise die Datei `SAServer.xml` dem Ordner `%VCS_ROOT%\cluster manager\attrpool\Win2K\400` hinzufügen und die Cluster-Dienste neu starten.

- c. Geben Sie in das Feld **Resource Name** einen Namen ein.
- d. Ordnen Sie die folgenden Attributwerte den entsprechenden Attributen zu:

- **cmdStart** `dbsrv16 -x tcpip Datenbankdatei_auf_gemeinsamer_Festplatte -n Servername`
- **cmdMonitor** `dbping -c "Server=Servername"`
- **cmdStop** `dbstop -c Benutzer_ID,Kennwort -y`

- e. Klicken Sie auf **Aktiviert**.  
Das gibt an, dass die Ressource zur Verfügung steht.
  - f. Klicken Sie auf **OK**.
3. Stellen Sie sicher, dass die Ressourcenabhängigkeiten korrekt konfiguriert sind. Es gibt weitere Ressourcen, die gestartet und gruppiert werden müssen, bevor SAServer gestartet werden kann, wie die gemeinsam genutzten Festplattenressourcen und die IP-Adressenressourcen.
  4. Rechtsklicken Sie auf die Dienstgruppe und klicken Sie auf **Online** » *Knotenname*, wobei *Knotenname* der Name des Computers im Cluster ist, der die Ressource ausführen soll.

### Ergebnisse

Die Dienstgruppe ist nun online.

### Siehe auch

- „Datenbankserveroption -su “ auf Seite 289

## Den SAServer-Agenten testen

Sie können den Failover im SAServer-Agenten mit VCS testen.

### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdatenbank muss bei allen Systemen im Cluster identisch sein.  
Der SADBDatabase-Agent verwendet die Dienstprogrammdatenbank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdatenbank haben. Sie können das Kennwort für die Dienstprogrammdatenbank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption -su angeben.
- Unter Unix ist der VCS-Agent unter `$SQLANY16/vcsagent/saserver` installiert.

Sie müssen das SELECT-Privileg für die Tabelle haben, aus der Sie auswählen, oder das SELECT ANY TABLE-Systemprivileg.

### Aufgabe

1. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her. Zum Beispiel:

```
dbisql -c "UID=DBA;PWD=sql;Server=VCS;HOST=HostName"
```

2. Führen Sie die folgende Abfrage aus:

```
SELECT * FROM Departments;
```

Die Abfrage sollte ohne Fehler ablaufen.

3. Fahren Sie das System herunter, auf dem der Datenbankserver läuft.
4. Verbinden Sie sich erneut von Interactive SQL aus, indem Sie dieselbe Verbindungszeichenfolge verwenden und die Abfrage erneut ausführen. Sie sollten in der Lage sein, sich zu verbinden und die Abfrage erfolgreich auszuführen.

### Ergebnisse

Ein Failover sollte aufgetreten sein und alle Ressourcen sollten auf dem alternativen Server gestartet worden sein.

### Siehe auch

- „[Datenbankserveroption -su](#)“ auf Seite 289

## SADatabase-Agentenkonfiguration

### Den SADatabase-Agenten einrichten

Der SADatabase-Agent steuert den Failover eines SQL Anywhere-Datenbankservers auf einen anderen Knoten im Cluster.

### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdatenbank muss bei allen Systemen im Cluster identisch sein.

Der SADatabase-Agent verwendet die Dienstprogrammdatenbank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdatenbank haben. Sie können das Kennwort für die Dienstprogrammdatenbank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption `-su` angeben.

- Unter Unix ist der VCS-Agent unter `$$SQLANY16/vcsagent/saserver` installiert.

Die Datei *offline.pl* verlangt zum Stoppen der Datenbank standardmäßig das SERVER OPERATOR-Systemprivileg. Sie können die Server-Befehlszeilenoption *-gk* verwenden, um das Standardverhalten zu ändern.

Die Datei *online.pl* verlangt zum Starten der Datenbank auf einem Netzwerkserver standardmäßig das SERVER OPERATOR-Systemprivileg. Sie können die Server-Befehlszeilenoption *-gk* verwenden, um das Standardverhalten zu ändern.

## Aufgabe

1. Fahren Sie alle SQL Anywhere-Datenbankserver herunter, die auf Knoten im Cluster ausgeführt werden.
2. Erstellen Sie ein Verzeichnis namens *%VCS\_HOME%\bin\SADatabase* auf einem der Knoten im Cluster.
3. Kopieren Sie die folgenden Dateien aus dem Verzeichnis *&%SQLANY16%\VCSAgent\SADatabase* in das Verzeichnis *%VCS\_HOME%\bin\SADatabase*, das Sie in Schritt 2 erstellt haben:
  - *Online.pl*
  - *Offline.pl*
  - *Monitor.pl*
  - *Clean.pl*
  - *SADatabase.xml*
4. Kopieren Sie die Datei *%VCS\_HOME%\bin\VCSdefault.dll* in das *%VCS\_HOME%\bin\SADatabase*-Verzeichnis und benennen Sie sie in *SADatabase.dll* um.
5. Kopieren Sie die Datei *%SQLANY16%\VCSAgent\SADatabase\SADatabaseTypes.cf* in das Verzeichnis *%VCS\_HOME%\conf\config*.
6. Wiederholen Sie die Schritte 1 bis 5 für alle Systeme, die am Cluster teilnehmen.
7. Starten Sie den Veritas Cluster Server-Manager und geben Sie Ihren Benutzernamen und das Kennwort ein, um sich mit dem Cluster zu verbinden.
8. Fügen Sie den SADatabase-Agenten hinzu:
  - a. Klicken Sie auf **File » Import Types**
  - b. Navigieren Sie zu *%VCS\_HOME%\conf\config\* und klicken Sie auf **Import**.

## Ergebnisse

Der SADatabase-Agent wird eingerichtet.

## Siehe auch

- „Datenbankserveroption *-su*“ auf Seite 289

## Datenbanken für Failover mit dem SADBDatabase-Agenten einrichten

Sie müssen eine Datenbank zur Dienstgruppe hinzufügen, bevor sie für den Failover konfiguriert wird.

### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdateiabank muss bei allen Systemen im Cluster identisch sein.

Der SADBDatabase-Agent verwendet die Dienstprogrammdateiabank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdateiabank haben. Sie können das Kennwort für die Dienstprogrammdateiabank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption `-su` angeben.

- Unter Unix ist der VCS-Agent unter `$SQLANY16/vcsagent/saserver` installiert.

### Aufgabe

1. Fügen Sie SADBDatabase als Ressource der Dienstgruppe hinzu:
  - a. Klicken Sie auf **Edit » Add » Resource**.
  - b. Klicken Sie in der Liste **Resource Type** auf **SADBDatabase**.

Wenn SADBDatabase in der Liste **Resource Type** unter Windows nicht angezeigt wird, müssen Sie möglicherweise die Datei *SADBDatabase.xml* dem Ordner `%VCS_ROOT%\cluster manager\attrpool\Win2K\400` hinzufügen und die Cluster-Dienste neu starten.
  - c. Geben Sie in das Feld **Resource Name** einen Namen ein.
  - d. Fügen Sie die angegebenen Werte den folgenden Attributen hinzu, indem Sie bei jedem Attribut auf die Schaltfläche in der Spalte **Edit** klicken:
    - **DatabaseFile** Der Standort der Datenbankdatei, z.B. `E:\demo.db`
    - **DatabaseName** Ein Name für die Datenbank
    - **ServerName** Ein Name für den Datenbankserver. Für jedes System im Cluster kann ein unterschiedlicher Servername angegeben werden. Der Bereich des Attributs sollte "Per System" und nicht "Global" sein.
    - **UtilDBpwd** Das Kennwort für die Dienstprogrammdateiabank für alle Systeme im Cluster
  - e. Klicken Sie auf **Enabled**.

Das gibt an, dass die Ressource zur Verfügung steht.
  - f. Klicken Sie auf **OK**.

2. Stellen Sie sicher, dass die Ressourcenabhängigkeiten korrekt konfiguriert sind. Es gibt weitere Ressourcen, die gestartet/gruppiert werden müssen, bevor SADBatabase gestartet werden kann, wie die gemeinsam genutzten Festplattenressourcen und die IP-Adressenressourcen.
3. Rechtsklicken Sie auf die Dienstgruppe und klicken Sie auf **Online** *Knotenname*, wobei *Knotenname* der Name des Computers im Cluster ist, der die Ressource ausführen soll.

## Ergebnisse

Die Dienstgruppe ist nun online.

## Siehe auch

- „Datenbankserveroption -su“ auf Seite 289

## Den SADBatabase-Agenten testen

Sie können den Failover mit dem SADBatabase-Agenten über Interactive SQL testen.

### Voraussetzungen

Für die Verwendung von SQL Anywhere Veritas Cluster Server-Agenten müssen Ihre Systeme folgendermaßen eingerichtet sein:

- Sie müssen Veritas Cluster Server 4.1 oder später verwenden.
- SQL Anywhere muss auf jedem Systemknoten im Cluster identisch installiert sein.
- Datenbankdateien müssen auf einem Device mit gemeinsam genutzten Speicher gespeichert sein, auf das alle Systeme im Cluster zugreifen können.
- Das Kennwort für die Dienstprogrammdatenbank muss bei allen Systemen im Cluster identisch sein.

Der SADBatabase-Agent verwendet die Dienstprogrammdatenbank, um bestimmte Datenbankdateien zu starten und zu stoppen. Alle an einem Cluster teilnehmenden Systeme müssen dasselbe Kennwort für die Dienstprogrammdatenbank haben. Sie können das Kennwort für die Dienstprogrammdatenbank festlegen, indem Sie beim Starten des Datenbankservers die Serveroption -su angeben.

- Unter Unix ist der VCS-Agent unter `$SQLANY16/vcsagent/saserver` installiert.

Sie müssen das SELECT-Privileg für die Tabelle haben, aus der Sie auswählen, oder das SELECT ANY TABLE-Systemprivileg.

Welche Privilegien zum Stoppen einer Datenbank auf dem Netzwerkserver erforderlich sind, wird durch die Datenbankserveroption -gd bestimmt. Standardmäßig ist zum Stoppen einer Datenbank auf dem Netzwerkserver das SERVER OPERATOR-Systemprivileg erforderlich.

## Aufgabe

1. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her. Zum Beispiel:

```
dbisql -c "UID=DBA;PWD=sql;Server=VCS;HOST=HostName"
```

2. Führen Sie die folgende Abfrage aus:

```
SELECT * FROM Departments;
```

Die Abfrage sollte ohne Fehler ablaufen.

3. Nehmen wir an, dass die Datenbank ausfällt und der auf dem ersten Systemknoten laufende Datenbankserver nicht auf die Datenbankdatei zugreifen kann. Dies würde zu einem Failover der Datenbankdatei zum Datenbankserver führen, der auf dem zweiten Systemknoten gestartet wurde. Sie können einen Ausfall der Datenbankdatei auf dem ersten Knoten verursachen, indem Sie einen ähnlichen Befehl wie den folgenden ausgeben:

```
dbisql -q -c "UID=DBA;PWD=sql;Server=VCS1;DBN=utility_db" STOP DATABASE  
DEMO ON VCS1 UNCONDITIONALLY;
```

### Ergebnisse

Die Datenbankdatei auf dem ersten Computer fällt aus. Es gibt eine Verzögerung, bevor Veritas Cluster Server erkennt, dass die Datei ausgefallen ist, weil Veritas Cluster Server den Zustand seiner Ressource standardmäßig alle 60 Sekunden überprüft (Sie können dieses Intervall in Ihrer Ressourcenkonfiguration verkürzen). Daraufhin erfolgt ein Failover der Datenbankdatei auf den zweiten Computer und diese Datenbankdatei wird mithilfe des Datenbankservers auf dem zweiten Computer gestartet, der möglicherweise einen anderen Namen hat als der ursprüngliche Datenbankserver.

Wenn der neue Datenbankserver z.B. VCS2 heißt, müssen Clients den neuen Datenbankservernamen in ihren Verbindungszeichenfolgen angeben:

```
"UID=DBA;PWD=sql;Server=VCS2;DBN=DEMO;HOST=HostName"
```

### Nächste Schritte

Verbinden Sie sich erneut von Interactive SQL aus. Sie sollten in der Lage sein, sich zu verbinden und die Abfrage erfolgreich auszuführen.

### Siehe auch

- „Datenbankserveroption -su“ auf Seite 289

## SQL Anywhere-Scale-Out mit Schreibschutz

### Hinweis

Scale-Out mit Schreibschutz erfordert eine separate Lizenz. Siehe „[Getrennt lizenzierbare Komponenten](#)“ [[SQL Anywhere 16 - Einführung](#)].

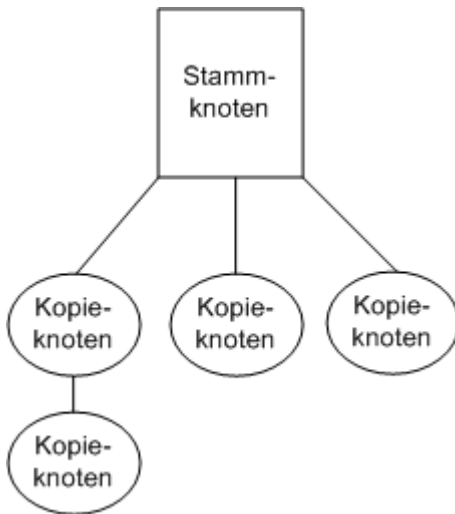
Scale-Out mit Schreibschutz ist eine Konfiguration, mit der Sie Berichterstellungs- oder andere Vorgänge auslagern können, die einen schreibgeschützten Zugriff auf die Datenbank erfordern.

Eine Scale-Out-Struktur besteht aus dem Stammknoten und den Kopieknoten.

- Der **Stammknoten** eines Scale-Out-Systems enthält die einzige Kopie der Datenbank, die nicht schreibgeschützt ist. Der Stammknoten kann entweder eine einzelne Datenbank oder ein

Datenbankspiegelungssystem sein. Unter dem Stammknoten können sich ein oder mehrere Zweige mit Kopieknoten befinden.

- Ein **Kopieknoten** ist ein Datenbankserver, auf dem eine Kopie einer Datenbank mit schreibgeschütztem Zugriff ausgeführt wird. Einem Kopieknoten können weitere Kopieknoten untergeordnet sein.



#### Siehe auch

- „Scale-Out mit Schreibschutz in einem Datenbankspiegelungssystem“ auf Seite 1538
- „Lektion 9: (Optional) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen“ auf Seite 1214
- „Zustand und Statistik von Datenbanken“ auf Seite 812
- Weitere Hinweise zur Verwendung von Hochverfügbarkeit bzw. schreibgeschütztem Scale-Out für das Hosting von Webanwendungen finden Sie unter „SQL Anywhere-Webdienste mit Hochverfügbarkeit und Scale-Out-Lösungen“ auf Seite 1540.

## Funktionsweise des Scale-Out

Der Stammknoten ist der einzige Datenbankserver, der sowohl Lese- als auch Schreibanforderungen akzeptiert. Wenn Sie zusätzliche Kopieknoten gestartet haben, sendet der Stammdatenbankserver Transaktionslogseiten an die Kopieknoten in der Struktur, die als seine untergeordneten Knoten definiert sind, vorausgesetzt dass diese bereits verbunden und für den Empfang von Transaktionslogseiten bereit sind. Die Seiten werden normalerweise gesendet, ohne dass auf eine Antwort gewartet wird. Der Stammdatenbankserver fordert jedoch gelegentlich eine Bestätigung an, um sicherzustellen, dass der Kopieknoten nicht mehr asynchrone Anforderungen erhält, als er verarbeiten kann.

Wenn der Kopieknoten Seiten erhält, schreibt er sie auf die Festplatte und sendet sie an seine untergeordneten Knoten (falls zutreffend).

Der übergeordnete Knoten erkennt, wenn ein untergeordneter Knoten nicht mehr verfügbar ist, und stellt in diesem Fall das Senden von Transaktionslogseiten an den untergeordneten Knoten ein. Wenn der untergeordnete Knoten neu gestartet wird, fordert er die Transaktionslogseiten an, die er nicht erhalten hat, und der übergeordnete Knoten nimmt das Senden von Transaktionslogseiten an den untergeordneten Knoten wieder auf. Der untergeordnete Knoten benachrichtigt den übergeordneten Knoten über Statusänderungen des Kopieknotens, und die Statusinformationen werden in der Struktur ganz nach oben bis zum Stammdatenbankserver weitergereicht.

Wenn der Stammdatenbankserver nicht mehr verfügbar ist, werden alle untergeordneten Knoten im Scale-Out-System weiterhin ausgeführt, erhalten aber keine Aktualisierungen mehr vom Primärdatenbankserver. Alle Verbindungen zu den Kopieknoten können veraltete Daten abrufen. Wenn der Stammdatenbankserver wieder zur Verfügung steht, können seine untergeordneten Knoten die Verbindungen wieder herstellen und den Empfang von Transaktionslogseiten wieder aufnehmen.

Wenn ein Kopieknoten auf ein Problem stößt, z.B. auf ein inkompatibles oder nicht übereinstimmendes Transaktionslog, wird die Datenbank gestoppt. Der Datenbankserver, auf dem die von dem Problem betroffene Datenbank läuft, wird ebenfalls heruntergefahren, es sei denn, auf ihm werden weitere Datenbanken ausgeführt.

Sie können Scale-Out in Verbindung mit einer Datenbankspiegelung verwenden, wenn Sie die Verfügbarkeit Ihrer Datenbank sicherstellen möchten.

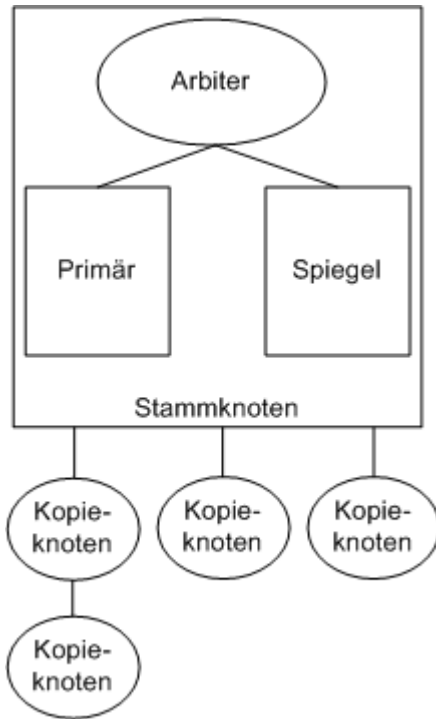
### Siehe auch

- „Scale-Out mit Schreibschutz in einem Datenbankspiegelungssystem“ auf Seite 1538
- „Lektion 9: (Optional) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen“ auf Seite 1214
- „Zustand und Statistik von Datenbanken“ auf Seite 812

## Scale-Out mit Schreibschutz in einem Datenbankspiegelungssystem

In einem Datenbankspiegelungssystem können Sie auf die Datenbank, die auf dem Spiegelserver läuft, mit einer schreibgeschützten Verbindung zugreifen. Diese Funktion ist nützlich, wenn Sie Berichterstellungs- oder andere Vorgänge auslagern möchten, die einen schreibgeschützten Zugriff auf diese Datenbank erfordern. Der einzige Unterschied zwischen einem Spiegelserver und einem Kopieknoten besteht darin, dass ein Kopieknoten nicht als Primär- oder Spiegelserver in einem Datenbankspiegelungssystem beteiligt sein kann. Ein Kopieknoten kann auch als Arbiter für eine Datenbank fungieren, die er kopiert.

Sie können die Datenbankspiegelung in Verbindung mit Scale-Out mit Schreibschutz verwenden, um die Verfügbarkeit des Stammknotens sicherzustellen. Wenn Scale-Out in Verbindung mit der Datenbankspiegelung verwendet wird, besteht der Stammknoten des Scale-Out-Systems logisch aus dem Primär-, dem Spiegel- und dem Arbiterserver, anstatt aus nur einem Datenbankserver.



Sobald Sie die Datenbankserver im Spiegelungssystem starten, können zusätzliche Datenbankserver auf die beteiligten Spiegelserver zugreifen, um die schreibgeschützten Kopien der Datenbank zu verwalten. Fügen Sie den Spiegelservern so viele Zweige von Kopieknoten hinzu wie nötig.

### Unterschiede zwischen Kopieknoten und Primär- und Spiegelservern

Wenn in einem Datenbankspiegelungssystem Kopieknoten verwendet werden, können sie dem aktuellen Primärserver, dem aktuellen Spiegelknoten oder einem anderen Kopieknoten untergeordnet sein. Der Kopieknoten erhält seine Transaktionslogseiten von dem ihm übergeordneten Knoten. Anders als bei Spiegelknoten haben Kopieknoten keine Statusinformationsdatei, da ihr Status keinen Einfluss darauf hat, welcher Datenbankserver Eigentümer der Datenbank ist. Ein Kopieknoten kann auch als Arbiter für eine Datenbank fungieren, die er kopiert. Wenn ein Kopieknoten als Arbiter fungiert, muss er einen beliebigen Spiegelservernamen haben, der nicht mit dem Servernamen eines der Datenbankserver im Hochverfügbarkeitssystem übereinstimmt.

### Siehe auch

- „Datenbankspiegelung“ auf Seite 1467
- „Verwenden eines Kopieknotens als Arbiter“ auf Seite 1485
- „ISYSMIRRORSERVER-Systemtabelle“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- Weitere Hinweise zur Verwendung von Hochverfügbarkeit bzw. schreibgeschütztem Scale-Out für das Hosting von Webanwendungen finden Sie unter „[SQL Anywhere-Webdienste mit Hochverfügbarkeit und Scale-Out-Lösungen](#)“ auf Seite 1540.

## SQL Anywhere-Webdienste mit Hochverfügbarkeit und Scale-Out-Lösungen

Die folgenden SQL Anywhere-Komponenten sind für die Konfiguration von Lösungen mit hoher Verfügbarkeit und/oder Scale-Out für das Hosting von Webanwendungen erforderlich:

- **Relay Server (RS)** Der Relay Server ist der Eintrittspunkt für HTTP-Anforderungen (in der Regel aus dem Internet), der Funktionen für virtuelles Hosting und Lastverteilung bereitstellt. Der Relay Server akzeptiert HTTP-Anforderungen, die virtuelle Entitäten, eine so genannte **Serverfarm**, betreffen, und leitet sie weiter. Jede Serverfarm kann aus einer oder mehreren SQL Anywhere-Datenbanken oder Webservern bestehen. Der Relay Server ist der HTTP/Web-Zugriffspunkt, der alle HTTP-Anforderungen an einen geeigneten Backend-Server zur Verarbeitung weiterleitet.
- **Outbound Enabler (OE)** Der Outbound Enabler stellt eine Brücke zwischen dem Relay Server und einem Backend-Datenbankserver dar. Es gibt einen Outbound Enabler-Prozess pro Backend-Server, der sich in einer Serverfarm befindet. Seine Aufgabe ist es sicherzustellen, dass sein designierter Backend-Server betriebsbereit ist. Außerdem ist er dafür verantwortlich, einen Kommunikationskanal mit dem Relay Server einzurichten und Anforderungen an seinen Backend-Server weiterzuleiten. Da der Outbound Enabler die Verbindung mit dem Relay Server initiiert, kann er auf einfache Art eine abgehende Verbindung von einem LAN aus über eine Firewall an einen Relay Server in der DMZ herstellen. Siehe „Outbound Enabler“ [\[Relay Server\]](#).
- **SQL Anywhere-(Backend-)Server** Beim SQL Anywhere-(Backend-)Server handelt es sich um eine erweiterte Datenbank und einen Webserver, der Webanwendungen, die vollständig in SQL geschrieben sind, hosten kann. SQL Anywhere-Server können für anspruchsvolle Umgebungen bereitgestellt werden, die Hochverfügbarkeit und Scale-Out-Lösungen erfordern. Hochverfügbarkeit bietet Fehlertoleranzfunktionen, um vor Unterbrechungen des Dienstes zu schützen und das Scale-Out stellt die Lastverteilung bereit, um den Durchsatz während Spitzenbelastungen zu erhöhen.

### Hochverfügbarkeit

Es sind drei SQL Anywhere-Server erforderlich, um Hochverfügbarkeit zur Verfügung zu stellen: ein **Arbiterserver** und zwei **Partnerserver**. Einem Partner ist die Rolle des **Primärserver**s zugeordnet und der andere ist der **Spiegelserver**. Schreibvorgänge, wie etwa eine Einfügung in eine globale Tabelle, sind nur auf dem Primärserver zulässig, während Lesevorgänge, wie z.B. eine SELECT-Anweisung, auf beiden Servertypen zulässig sind. Der Primärserver hält seinen Spiegelserver automatisch synchronisiert, wenn er Aktualisierungen erhält. Im Fall eines Fehlers auf dem Primärserver übernimmt der Arbiterserver die Rollen der Partnerserver, sodass der Spiegelserver zum Primärserver wird.

Hochverfügbarkeit kann innerhalb einer Webdienstumgebung genutzt werden, indem alle HTTP-Anforderungen über einen Relay Server weitergeleitet werden. Der Relay Server verarbeitet die URL der HTTP-Anforderung, um die Ziel-Serverfarm zu ermitteln. Stellen Sie sich der Einfachheit halber eine Relay Server-Konfiguration vor, die HTTP-Anforderungen entweder an eine readFarm oder an eine writeFarm weiterleitet. Wenngleich der primäre Backend-Server sowohl Lese- als auch Schreibenanforderungen verarbeiten kann, können Sie ihn so konfigurieren, dass er nur Schreibenanforderungen verarbeitet, sofern noch andere schreibgeschützte Kopieknotten vorhanden sind, die die Lesefunktion im Fall eines Serverausfalls übernehmen können. Andernfalls können Sie ihn so konfigurieren, dass er sowohl Lese- als auch Schreibenanforderungen verarbeitet. Sie können jedoch den Spiegelserver so konfigurieren, dass er Leseanforderungen verarbeitet und dadurch die Leselast verteilt

wird, oder so, dass er keine Anforderungen verarbeitet und dadurch die Hardwarenutzung auf dem Spiegelserver reduziert wird. Die Clientanwendung benötigt keine Kenntnis des physischen Servers, auf den sie für Lese- und Schreibanforderungen zugreifen soll. Sie erstellt einfach ihre URL, um Anforderungen an die readFarm oder die writeFarm zu richten.

Zusätzlich zum Relay Server benötigt jeder Partner-Backend-Server zwei Outbound Enabler, einen für jede Farm, die der Backend-Server nutzt. Zwei Outbound Enabler steuern die Kommunikationskanäle mit dem Primärserver-Partner und zwei Outbound Enabler richten die Kommunikation mit dem Spiegelserver-Partner ein. In dieser Konfiguration gibt es zu jedem Zeitpunkt jeweils nur einen Primärserver. Er aktiviert den der writeFarm zugewiesenen Outbound Enabler und deaktiviert fakultativ den der readFarm zugewiesenen Outbound Enabler, sofern noch andere Mitglieder in der readFarm vorhanden sind, bei denen es sich nicht um Kopieknoten handelt. Der Spiegelserver deaktiviert den Outbound Enabler, der der writeFarm zugewiesen ist, und aktiviert fakultativ auch den Outbound Enabler, der der readFarm zugewiesen ist.

Wenn der Primärserver aufgrund eines Hardware- oder Softwarefehlers ausfällt, verhandelt der Spiegelserver mit dem Arbiterserver, um die Rolle des Primärservers zu übernehmen, und wird somit Mitglied der writeFarm. Er sollte auch Mitglied der readFarm werden, falls das System keine anderen schreibgeschützten Kopieknoten hat. Zum Zeitpunkt des Ausfalls wird der ursprüngliche Primärserver sofort sowohl von der writeFarm als auch von der readFarm zurückgenommen, sofern er ein Mitglied ist. Der ursprüngliche Primärserver kann erst wiederhergestellt werden, wenn die Ursache des Ausfalls behoben wurde. Wenn er wiederhergestellt wurde, übernimmt er die Rolle des Spiegelserver und wird fakultativ mit der readFarm verbunden. Der plötzliche Fehler führt möglicherweise dazu, dass aktuell vom ausfallenden Server bearbeitete Anforderungen falsch verarbeitet werden. Die Verarbeitungszeit für die writeFarm-Wiederherstellung anhand des Spiegelserver hängt von der Verarbeitungszeit für den Rollenwechsel des SQL Anywhere-Spiegelserver sowie vom Statusabrufrintervall ab, das auf dem Outbound Enabler der writeFarm des Spiegelserver festgelegt wurde. Dieses Statusabrufrintervall kann festgelegt werden. Wenn es nicht explizit festgelegt wird, beträgt sein Standardwert 5 Sekunden.

## **Scale-Out**

Es sind mindestens zwei SQL Anywhere-Server erforderlich, um die Scale-Out-Funktionalität zur Verfügung zu stellen: ein Stammknoten und ein Kopieknoten. Ein Kopieknoten ist wie ein Spiegelserver schreibgeschützt, er kann jedoch nie die Rolle des Primärserver übernehmen. Er dient ausschließlich zur Verarbeitung von Leseanforderungen. Wie bereits im Szenario mit Hochverfügbarkeit erläutert, wird der Primärserver der writeFarm zugewiesen und der Kopieknoten ersetzt den Spiegelserver als readFarm-Mitglied. Mit einem Stammknoten und einem einzigen Kopieknoten sind insgesamt nur zwei Outbound Enabler erforderlich, einer für jeden Server. Optional können Sie den Primärserver der readFarm hinzufügen, damit die Umgebung voll funktionsfähig bleibt, wenn alle Kopieknoten ausfallen. Der Outbound Enabler, der dem Stammknoten zugewiesen ist, ist für den Empfang von Anforderungen an die writeFarm konfiguriert, während der Outbound Enabler des Kopieknotens für die Entgegennahme von Anforderungen an die readFarm konfiguriert ist. Der Stammknoten aktualisiert seine Kopieknoten laufend, wenn er Schreibaktualisierungen erhält. Die Konfiguration kann durch das Hinzufügen von Kopieknoten zur readFarm erweitert werden. Die Ausführung von 10 Kopieknoten für die readFarm bietet Lastverteilung und fängt Serverausfälle innerhalb der readFarm auf.

## **Hochverfügbarkeit plus Scale-Out**

Die oben beschriebenen Konfigurationsszenarien können kombiniert werden, um sowohl Hochverfügbarkeit als auch Scale-Out zur Verfügung zu stellen. Eine solche Konfiguration würde

Fehlertoleranz für beschreibbare (Primär-/Spiegelserver) und lesbare (Spiegelserver und Kopieknoten) Backend-Server bereitstellen. Außerdem erhöht das Hinzufügen von Kopieknoten das Durchsatzpotenzial für schreibgeschützte HTTP-Anforderungen. In dieser Konfiguration bilden der Primär- und der Spiegelserver den Stammknoten. Der Primär- und der Spiegelserver und die Kopieknoten haben jeweils einen Outbound Enabler zur Teilnahme an der readFarm. Der Primär- und der Spiegelserver haben einen zusätzlichen Outbound Enabler zur Teilnahme an der writeFarm. Optional können Sie den Primär- und den Spiegelserver aus der readFarm entfernen.

### Outbound Enabler-Konfiguration

Im Rahmen dieser Erläuterung muss ein Outbound Enabler so konfiguriert sein, dass er folgende Objekte identifizieren kann:

- Zugehörige Serverfarm
- Verbindungsparameter des Relay Servers
- SQL Anywhere-Verbindungsparameter (Backend-Farm)

Mit dem folgenden Befehl richtet der Outbound Enabler eine Verbindung mit dem Relay Server ein, die auf durch die Option `-cr` angegebenen Parametern basiert. Wenn sie aktiv ist, leitet der Relay Server Anforderungen an die readFarm an den Backend-Server weiter, der entsprechend der Option `-cs` Option konfiguriert ist.

```
rsoe.exe -f readFarm -id saHost1 -cr url_suffix="/rs/server/  
rs_server.dll";host=rs_server;port=80 -cs host=sahost1;port=8080;status_url=  
satest/oe_read_status?ro=1
```

Basierend auf dem obigen Beispiel leitet eine Anforderungs-URL der Form `http://rs_server/rs/client/rs_client.dll/readFarm/service_path[?service_query]`

die Anforderung an den Relay Server weiter, der auf `rs_server` gehostet wird. Der Relay Server entfernt die Domänen- und Farm-Komponente aus der URL und leitet die Anforderung über den Outbound Enabler-Kanal des Relay Servers an einen aktiven Outbound Enabler weiter. Der Outbound Enabler leitet die Anforderung dann an seinen Backend-Server weiter.

Ein Outbound Enabler behält einen Kanal zum Relay Server nur bei, wenn er erkennt, dass der Backend-Server für die Verarbeitung von Anforderungen bereit ist. Hierzu fragt er den Server in einem konfigurierbaren Intervall ab, indem er eine HTTP-Anforderung mit der Option `-cs` verwendet. Die `status_url`-Option liefert den betreffenden URL-Pfad für den Ping-Dienst. In der obigen Beispielkonfiguration sendet der Outbound Enabler HTTP-Anforderungen an `http://sahost1:8080/satest/oe_read_status?ro=1`. Wenn der Server mit **AVAILABLE=TRUE | ON | 1** antwortet, behält der Outbound Enabler die Kommunikationsverbindung mit dem Relay Server bei, der auf `rs_server` gehostet wird, oder initiiert diese.

### SQL Anywhere-Konfiguration

Weitere Hinweise zum Konfigurieren und Starten von SQL Anywhere als Webserver finden Sie unter [„SQL Anywhere als HTTP-Webserver“ \[SQL Anywhere Server - Programmierung\]](#).

Unter Verwendung des RSOE-Startbeispiels (Relay Server Outbound Enabler), das im Abschnitt zur Outbound Enabler-Konfiguration beschrieben ist, kann ein `oe_read_status`-Dienst wie folgt geschrieben werden:

```
// READ-ONLY SA-OE ping service
// optionally includes primary as a READ node.
call sa_make_object( 'service', 'oe_read_status' );
alter service oe_read_status
    type 'raw'
    authorization off
    secure off
    user DBA
    as call sp_oe_read_status(:ro);

// if ro is 1 then only read-only servers are activated: mirror or copy
// if ro is 0 then include all servers: primary, mirror, copy...
create or replace procedure sp_oe_read_status( ro int )
begin
    declare readonly long varchar;
    declare res long varchar;

    set res = 'AVAILABLE=';

    set ro = isnull(ro, 0);
    if ro = 1 then
        select db_property('ReadOnly') into readonly;
        if readonly = 'On' then
            set res = res || 'TRUE';
        else
            set res = res || 'FALSE';
        end if;
    end if;;

    call sa_set_http_header('Content-Length', length(res) );
    select res;
end;
```

Der oben beschriebene Webdienst und die gespeicherte Prozedur können für alle SQL Anywhere-Server verwendet werden, die die Rolle eines Primär- oder Spiegelservers oder eines Kopieknotsens haben. Wenn die `ReadOnly`-Datenbankeigenschaft auf "On" gesetzt ist, wird **AVAILABLE=TRUE** zurückgegeben. Bei kleinen Änderungen würde ein Dienst für die Verwendung in einer beschreibbaren Serverfarm, zum Beispiel `writeFarm`, nur dann **AVAILABLE=TRUE** zurückgeben, wenn die `ReadOnly`-Datenbankeigenschaft auf "Off" gesetzt ist. Optional kann ein Ping-Dienst für einen Outbound Enabler seine Einstellung für `AVAILABILITY` auf andere Faktoren basieren, wie etwa einen Eintrag in einer globalen Tabelle. Zum Beispiel kann ein stufenweises Deployment eine Tabelle oder Prozedur auf dem Primärserver aktualisieren, der die Serverfarm-Mitgliedschaft jedes Servers aktiviert oder deaktiviert, wenn die Aktualisierung an den Spiegelserver oder den Kopieknotten übergeben wird.

## Relay Server-Konfiguration

So konfigurieren Sie den Relay Server:

1. Erstellen Sie die `readFarm`- und `writeFarm`-Backend-Farmen.
2. Konfigurieren Sie den Primär- und den Spiegelserver sowie Kopieknotten, die Mitglieder der Relay Server-Backend-Farm `readFarm` sein sollen.

3. Konfigurieren Sie den Primär- und den Spiegelserver, die Mitglieder der Relay Server-Backend-Farm writeFarm sein sollen.
4. Setzen Sie für beide Farmen die active\_cookie-Konfigurationsoption auf **yes** und die active\_header-Konfigurationsoption auf **no**. (Dieser letzte Schritt kann in Sybase Central durchgeführt werden, indem **SQL Anywhere** als Backend-Farm-Affinitätstyp gewählt wird.) Wenn Sie keine Affinität benötigen und die Performance steigern möchten, können Sie die active\_cookie-Konfigurationsoption deaktivieren.

### Client-/Anwendungskonfiguration

- **Einschränkungen** Derzeit können SQL Anywhere-Backend-Server nur die Hochverfügbarkeit einer Datenbank unterstützen. Die maximale Verarbeitungszeit für Failover für Hochverfügbarkeit entspricht dem Maximalwert von:
  - Abrufhäufigkeit des Outbound Enablers. Weitere Hinweise finden Sie unter der Befehlszeilenoption -d unter [Outbound Enabler-Syntax \[Relay Server\]](#).
  - Zeitraum, der erforderlich ist, damit der Spiegelserver zum Primärserver wird.

### Siehe auch

- „Einführung in den Relay Server“ [\[Relay Server\]](#)
- „Relay Server-Konfigurationsdatei“ [\[Relay Server\]](#)
- „Konfigurationsaktualisierungen für die Relay Server-Farm“ [\[Relay Server\]](#)
- [Eigenschaften im Backend-Farm-Abschnitt \[Relay Server\]](#)

## Verbindungen mit Datenbanken in Scale-Out-Systemen herstellen

Zum Einrichten eines Scale-Out-Systems wird empfohlen, mit der CREATE MIRROR SERVER-Anweisung für den Datenbankserver, der als Stammknoten fungiert, zwei Definitionen zu erstellen:

- Eine Definition für die Partnerrolle  
In einem Scale-Out-System müssen Sie einen Partnerserver definieren. Der in der Definition des Partnerservers angegebene Name wird in Verbindungszeichenfolgen und beim Starten des Datenbankservers verwendet.
- Eine Definition für die Primärserverrolle  
Die als Primärserver definierte Datenbank ist standardmäßig der übergeordnete Knoten für Kopieknoten im Scale-Out-System. Wenn kein Primärserver definiert ist, müssen Sie für jeden dem System hinzugefügten Kopieknoten einen übergeordneten Knoten angeben.

Wenn Sie Scale-Out mit Schreibschutz verwenden, ist zu empfehlen, dass die Anwendung sich mit dem Stammdatenbankserver verbindet und der Stammdatenbankserver Informationen aus der Verbindungszeichenfolge der Anwendung sowie Status- und Lastinformationen von den Kopieknoten verwendet, um zu ermitteln, mit welchem Knoten die Anwendung eine Verbindung herstellen soll. Sie können mithilfe des NodeType=COPY-Verbindungsparameters festlegen, dass die Anwendung sich mit

dem Kopieknoden verbindet, der die geringste Last aufweist. Wenn Sie dies angeben, leitet der Stammdatenbankserver den Client zum betreffenden Knoten um. Siehe „[Verbinden mit Kopieknoden](#)“ auf Seite 1545.

Wenn eine Anwendung innerhalb eines kurzen Zeitraums mehrere Verbindungen dieser Art herstellt und löscht, wird die Verbindung gepoolt und der Stammdatenbankserver wird nicht gefragt, welcher Kopieknoden verwendet werden soll. Dieses Verhalten reduziert die Auslastung auf dem Stammdatenbankserver, weist aber möglicherweise nicht das erwartete Verhalten auf. In der Anwendung kann festgelegt sein, dass ihre Verbindungen nicht gepoolt werden sollen. Damit wird sichergestellt, dass der Stammserver bei jeder Verbindung bestimmt, mit welchem Kopieknoden diese erfolgen soll. Siehe [Verbindungspooling und Scale-Out mit Schreibschutz](#) auf Seite 78.

#### **Tip**

Überprüfen Sie den Status der Datenbankserver in einem Scale-Out-System, indem Sie die Primärdatenbank mithilfe des SQL Anywhere-Monitors überwachen.

Sie können ein Scale-Out-System auch aus Sybase Central überwachen, indem Sie sich mit der Primärdatenbank verbinden und den Status der Datenbankserver im Fensterausschnitt **Gesundheit und Statistik** prüfen.

#### **Siehe auch**

- „[Scale-Out mit Schreibschutz in einem Datenbankspiegelungssystem](#)“ auf Seite 1538
- „[Lektion 9: \(Optional\) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen](#)“ auf Seite 1214
- „[Zustand und Statistik von Datenbanken](#)“ auf Seite 812

## **Verbinden mit Kopieknoden**

Stellen Sie eine Verbindung mit einem Kopieknoden her, indem Sie sich mit dem Primärserver verbinden und den NodeType-Verbindungsparameter als Teil der Verbindungszeichenfolge angeben. Der NodeType-Verbindungsparameter akzeptiert die folgenden Werte:

- **DIRECT** Dies ist die Standardeinstellung beim Verbinden mit einem Datenbankserver.  
  
Wenn der NodeType Verbindungsparameter auf DIRECT eingestellt ist, akzeptiert der Datenbankserver die Verbindung, ohne eine Lastverteilung oder Weiterleitung auszuführen.
- **PRIMARY** Wenn der NodeType-Verbindungsparameter auf PRIMARY eingestellt ist und Sie eine Verbindung zum Primärserver hergestellt haben, wird die Verbindung akzeptiert. Wenn Sie sich mit einem Nicht-Primärserver (z.B. dem Spiegelserver oder einem Kopieknoden) verbunden haben, leitet der Datenbankserver die Verbindung zum Primärserver um.
- **COPY** Wenn der NodeType-Verbindungsparameter auf COPY eingestellt ist, führt der Datenbankserver die Lastverteilung aus und wählt einen Kopieknoden. In einem Scale-Out-System mit Schreibschutz überprüft der Datenbankserver die Kopieknoden in seinem eigenen Zweig (einschließlich seiner selbst, wenn er nicht der Stammknoten ist) und wählt den Kopieknoden mit der geringsten Last. Wenn der Datenbankserver sich nicht selbst auswählt, leitet er den Client zum ausgewählten Datenbankserver um.

- **MIRROR** Wenn der NodeType-Verbindungsparameter auf MIRROR eingestellt ist und Sie sich mit dem Spiegelserver verbunden haben, wird die Verbindung akzeptiert. Wenn Sie sich mit einem Nicht-Spiegelserver verbunden haben, leitet der Datenbankserver die Verbindung zum Spiegelserver um.
- **READONLY** Wenn der NodeType-Verbindungsparameter auf READONLY eingestellt, werden Sie mit einem beliebigen schreibgeschützten Server verbunden, entweder mit einem Kopieknoten oder mit dem Spiegelserver. Wenn es keine Kopieknoten gibt, ist dies gleichwertig mit der Einstellung MIRROR. Wenn es Kopieknoten gibt, ist dies gleichwertig mit der Einstellung COPY.

Sobald der Stammdatenbankserver ermittelt hat, mit welchem Kopieknoten verbunden werden soll, wird die Verbindung automatisch zu diesem Knoten umgeleitet (falls erforderlich).

### Siehe auch

- „Verbindungsparameter NodeType (NODE)“ auf Seite 375
- „Verbindungen mit Datenbank in Spiegelungssystemen herstellen“ auf Seite 1472

## Einrichten eines Scale-Out-Systems mit Schreibschutz

Folgende Schritte müssen für die Konfiguration eines Scale-Out-Systems durchgeführt werden:

1. Starten Sie einen Datenbankserver mit der Datenbankoption **-xp on**. Dieser Datenbankserver ist der Stammknoten für das Scale-Out-System.
2. Fügen Sie der Stammdatenbank die Scale-Out-Objektdefinitionen hinzu. Sie müssen die Server definieren und Optionen für die Server angeben.
3. Erstellen Sie Sicherungskopien von der Stammdatenbank.
4. Starten Sie die Kopieknoten (die Sicherungskopien der Datenbank).

### Hinweise zu Kerberos-Authentifizierung und integrierten Logins

Wenn Sie den NodeType-Verbindungsparameter zum Umleiten von Verbindungen verwenden, die Kerberos-Authentifizierung oder integrierte Logins benutzen, müssen alle Datenbankserver in der Scale-Out-Struktur wie folgt konfiguriert werden:

- **Integrierte Logins** Alle Datenbankserver in der Scale-Out-Struktur müssen ein Teil derselben Windows-Benutzergruppe sein oder so konfiguriert werden, dass dieselben Windows-Benutzer auf sie zugreifen.
- **Kerberos-Authentifizierung** Bei allen Datenbankservern in der Scale-Out-Struktur muss die Kerberos-Authentifizierung aktiviert sein. Der Kerberos-Serverprinzipal für alle Server in der Scale-Out-Struktur muss denselben Realm haben.

## Einrichten des Stammknotens

Sie erstellen den Stammknoten eines Scale-Out-Systems mit Schreibschutz mit der Datenbank, von der Sie Kopien benötigen.

## Voraussetzungen

Sie müssen das **MANAGE ANY MIRROR SERVER**-Systemprivileg haben.

## Kontext und Bemerkungen

Wenn Sie den Stammknoten konfigurieren, definieren Sie den Stammdatenbankserver als Partnerserver. Sie können auch einen Primärserver definieren.

## Aufgabe

1. Starten Sie einen Datenbankserver, auf dem die Datenbank ausgeführt wird, von der Sie schreibgeschützte Kopien benötigen. Sie müssen beim Starten des Datenbankservers die Datenbankoption **-xp on** angeben.

Beispiel: Der folgende Befehl startet einen Datenbankserver namens **scaleout\_root\_demo** an Port 6871. Es wird empfohlen, dass Sie zum Angeben einer Portnummer die Option **-x** verwenden, weil diese Portnummer zu einem späteren Zeitpunkt in der **CREATE MIRROR SERVER**-Anweisung verwendet wird.

```
dbsrv16 -n scaleout_root_demo -x TCPIP(port=6871) "c:\scaleoutdemo
\scaleoutdemo.db" -xp on
```

2. Definieren Sie die Scale-Out-Objekte in der Stammdatenbank unter Verwendung der **CREATE MIRROR SERVER**-Anweisung.

Es wird empfohlen, zwei Definitionen für den Stammdatenbankserver zu erstellen: **CREATE MIRROR SERVER ... AS PARTNER** und **CREATE MIRROR SERVER ... AS PRIMARY**. Sie müssen den **connection\_string**-Parameter in beiden Definitionen angeben.

- a. Der Name, den Sie dem Datenbankserver in der Anweisung mit der **AS PARTNER**-Klausel geben, ist der Name, der im Befehl zum Starten des Datenbankservers und in Client-Verbindungszeichenfolgen verwendet wird. Zum Beispiel:

```
CREATE MIRROR SERVER "scaleout_root_demo"
AS PARTNER
connection_string = 'SERVER=scaleout_root_demo;HOST=localhost:6871';
```

- b. Der Name, den Sie dem Datenbankserver in der Anweisung mit der **AS PRIMARY**-Klausel geben, ist der Name des Datenbankservers, der standardmäßig der übergeordnete Knoten für die dem Scale-Out-System hinzugefügten Kopieknoten ist. Wenn Sie keinen Primärserver definieren, müssen Sie beim Erstellen von Kopieknoten den Namen des übergeordneten Servers angeben. Das Definieren eines Primärservers wird daher empfohlen.

```
CREATE MIRROR SERVER "scaleout_primary_demo"
AS PRIMARY
connection_string = 'SERVER=scaleout_primary_demo;HOST=localhost:
6871';
```

3. Legen Sie die Scale-Out-Optionen für die Datenbank mit der **SET MIRROR OPTION**-Anweisung fest. Sie müssen einen Wert für den **authentication\_string**-Parameter angeben und den **child\_creation**-Parameter auf "automatic" setzen (Standardeinstellung). Zum Beispiel:

```
SET MIRROR OPTION child_creation='automatic';  
SET MIRROR OPTION authentication_string='abc';
```

### Ergebnisse

Der Stammknoten steht nun zur Verfügung.

### Nächste Schritte

Erstellen Sie Sicherungskopien der Stammdatenbank, die verwendet werden, um untergeordnete Knoten zum Scale-Out-System mit Schreibschutz hinzuzufügen.

### Siehe auch

- „Datenbankoption -xp“ auf Seite 335
- „Datenbankserveroption -x “ auf Seite 305
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „Hinzufügen von untergeordneten Kopieknoten“ auf Seite 1549

## Hinzufügen von Kopieknoten

Fügen Sie Kopieknoten zu einem Scale-Out-System mit Schreibschutz hinzu.

### Voraussetzungen

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

In der Stammdatenbank ist SET MIRROR OPTION für child\_creation auf "automatic" eingestellt.

### Kontext und Bemerkungen

Kopieknotendefinitionen werden in der Datenbank gespeichert. Sie können Kopieknoten für das Scale-Out-System im Voraus festlegen oder die Kopieknoten bei der Verbindungsaufnahme vom Stammdatenbankserver festlegen lassen. Es wird empfohlen, die Definitionen der Kopieknoten vom Stammdatenbankserver erstellen zu lassen, da auf diese Weise die Wahrscheinlichkeit von Fehlern in Ihren Definitionen für Kopieknoten verringert wird.

### Aufgabe

1. Erstellen Sie Sicherungskopien von der Stammdatenbank.
2. Starten Sie die Kopien der Datenbank als Kopieknoten. Beim Starten der Datenbankserver, auf denen die Kopieknoten ausgeführt werden, müssen Sie eindeutige Namen und Ports sowie die Datenbankoption **-xp on** angeben. Zum Beispiel:

```
dbsrvl6 -n scaleout_child_demo -x TCPIP(port=6873) "c:\scaleoutdemo  
\copynode\scaleoutdemo.db" -xp on
```

## Ergebnisse

Die Datenbanken werden als Kopieknotten gestartet.

### Siehe auch

- „BACKUP-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „Datenbankoption -xp“ auf Seite 335
- „Hinzufügen von untergeordneten Kopieknotten“ auf Seite 1549

## Hinzufügen von untergeordneten Kopieknotten

Die `child_creation`-Option der `SET MIRROR OPTION`-Anweisung steuert, wie untergeordnete Knoten dem Scale-Out-System mit Schreibschutz hinzugefügt werden. Die folgenden Werte werden für die `child_creation`-Option unterstützt:

- **Automatic** Der Stammdatenbankserver authentifiziert den Kopieknotten bei seinem Start oder erstellt einen neuen Kopieknotten, wenn der Kopieknotten nicht bekannt ist. Dies ist die empfohlene Einstellung, da der Stammserver die Definition für unbekannte Kopieknotten erstellt, sodass Sie diese nicht manuell erstellen müssen.
- **Off** Stellen Sie eine Verbindung mit dem Stammdatenbankserver her und führen Sie eine `CREATE MIRROR SERVER`-Anweisung zum Hinzufügen eines neuen Kopieknottens aus.
- **Manual** Fügen Sie der Struktur Kopieknotten hinzu, indem Sie eine Verbindung zu einem Kopieknotten herstellen und eine `CREATE MIRROR SERVER`-Anweisung für diesen Datenbankserver ausführen. Diese Anweisung erfordert das `MANAGE ANY MIRROR SERVER`-Systemprivileg. Der Kopieknotten sendet eine Anforderung an den Stammdatenbankserver zur Definition des neuen Kopieknottens. Wenn der Kopieknotten definiert ist, lässt der Stammdatenbankserver zu, dass der neue Kopieknotten Logseiten anfordert.

In der Datenbank wird die Verbindungszeichenfolge gespeichert, die dem primären Datenbankserver im System zugeordnet ist. Beim Start eines zuvor nicht definierten neuen Kopieknottens, stellt dieser mit dieser Verbindungszeichenfolge die Verbindung zum Stammdatenbankserver her. Der Stammdatenbankserver verwendet den Wert der `authentication_string`-Option, die in der Datenbank zur Authentifizierung des Kopieknottens gespeichert ist.

Als Teil der Spiegelserver-Verbindungsanforderung sendet der Kopieknotten den Namen des Kopiedatenbankservers und eine Zeichenfolge, die die IP-Adressen und Ports des Kopiedatenbankservers enthält, an den Stammdatenbankserver. Wenn der Kopieknotten authentifiziert ist, ermittelt der Stammdatenbankserver, ob der Kopieknotten bekannt ist. Wenn der Kopieknotten nicht bekannt ist, führt der Stammdatenbankserver eine `CREATE MIRROR SERVER`-Anweisung aus, um die neue Kopie und ihre Verbindungszeichenfolge zu definieren. Sobald die Kopie bekannt ist, kann der Stammdatenbankserver eine Verbindung mit ihr herstellen. Die Kopie fordert dann alle Transaktionslogseiten an, die sie noch nicht hat, und sobald der Kopieknotten diese Seiten hat, beginnt der Stammdatenbankserver damit, neue Transaktionslogseiten an den Kopieknotten zu senden.

Alle Kopieknottenserver müssen eindeutige Servernamen haben.

### Siehe auch

- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Zuordnung von übergeordneten Knoten zu Kopieknoten

Ein Kopieknoten muss einen übergeordneten Knoten haben. Der übergeordnete Knoten kann der Stammdatenbankserver oder ein anderer Kopieknoten sein. Sie können das Scale-Out-System mit Schreibschutz so einrichten, dass der übergeordnete Knoten automatisch zugewiesen wird. Sie können auch zu jedem beliebigen Zeitpunkt die Position eines Knotens innerhalb der Scale-Out-Hierarchie ändern.

### Automatisches Zuweisen des übergeordneten Knotens eines Kopieknotens

Die SET MIRROR OPTION-Anweisung unterstützt zwei Optionen, die zum Zuweisen neuer Kopieknoten zu einem übergeordneten Knoten in der Struktur verwendet werden können, um die mit dem Verteilen von Transaktionslogseiten verbundene Belastung gleichmäßig auf die Knoten zu verteilen:

- **auto\_add\_server** Gibt den Namen eines Datenbankservers an, der als oberster Knoten der Struktur für die automatische Zuweisung fungiert.

Wenn die auto\_add\_server-Option festgelegt ist, wird der durch diese Option angegebene Datenbankserver als oberster Knoten verwendet. Wenn die add\_auto\_server-Option nicht angegeben ist, wird der Stammdatenbankserver als übergeordneter Knoten für alle Kopieknoten mit automatischer Zuordnung verwendet und die auto\_fan\_out-Option wird ignoriert.

- **auto\_add\_fan\_out** Gibt die maximale Anzahl der Kopieknoten an, die pro Zweig in der Struktur zulässig sind. Der Mindestwert, den Sie angeben können, ist 2, der Standardwert 10. Neuen Knoten, die als Ergebnis einer der folgenden Aktionen erstellt werden, wird ihr übergeordneter Knoten automatisch zugewiesen:
  - Herstellen einer Verbindung zum Primärserver, wenn die child\_creation-Option auf "automatic" eingestellt ist
  - Ausführen der Anweisung CREATE MIRROR SERVER ... USING AUTO PARENT auf dem Kopieknoten, wenn die child\_creation-Option auf "manual" eingestellt ist
  - Ausführen der Anweisung CREATE MIRROR SERVER ... USING AUTO PARENT auf dem Stammdatenbankserver

Der Stammdatenbankserver bestimmt, welcher Knoten in der Struktur als übergeordneter Knoten den neuen Kopieknoten zugewiesen werden soll. Dies geschieht auf der Grundlage der Anzahl der untergeordneten Elemente für jeden Knoten und dessen Status, wie er durch periodische Statusaktualisierungen an den Stammdatenbankserver gemeldet wird. Der Kopieknoten sieht die Zuordnung zu seinem neuen übergeordneten Knoten, wenn er vom Stammdatenbankserver empfangene Transaktionslogvorgänge anwendet. D.h. der Kopieknoten ändert seine übergeordnete Verbindung bei Erhalt des Transaktionslogvorgangs.

**Siehe auch**

- „SET MIRROR OPTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „CREATE MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**Knotenpositionen**

Sobald ein Kopieknott ausgeführt wird, können Sie ihm auf dem Stammdatenbankserver mit der ALTER MIRROR SERVER-Anweisung einen neuen übergeordneten Knoten zuweisen:

```
ALTER MIRROR SERVER "copy-server-name"  
FROM SERVER "new-parent-name" ;
```

Die Anweisung wird im Transaktionslog auf dem Stammdatenbankserver protokolliert. Wenn die Änderung an den Kopieknott gesendet wird, erkennt der Knoten, dass seine eigene Definition gerade geändert wird, und verbindet sich dann mit dem neuen übergeordneten Knoten, der in der Anweisung angegeben ist.

**Siehe auch**

- „ALTER MIRROR SERVER-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

**Ermitteln von übergeordneten Knoten für Kopieknott**

Ein Kopieknott ermittelt den Server, zu dem er eine Verbindung herstellen muss, indem er in der Systemtabelle ISYSMIRRORSERVER nach seiner eigenen Spiegelserverdefinition sucht und feststellt, welcher Wert für den übergeordneten Knoten angegeben ist.

- NULL bedeutet, dass der übergeordnete Knoten des Kopieknotts der Stammknoten ist.
- Ist in der Spalte für den übergeordneten Knoten eine ID vorhanden, ist der Server mit dieser ID der übergeordnete Knoten des Kopieknotts.

Sobald der Kopieknott weiß, welcher Server sein übergeordneter Knoten ist, verwendet er den in der Datenbank gespeicherten Wert der connection\_string-Option, um eine Verbindung zum korrekten übergeordneten Knoten herzustellen.

**Ermitteln des übergeordneten Knotens eines Kopieknotts in einem Datenbankspiegelungssystem**

Wenn Scale-Out in Verbindung mit einem Datenbankspiegelungssystem verwendet wird, können Kopieknott so definiert werden, dass ihr jeweiliger Partner der Server ist, der derzeit als Primärserver oder als Spiegelserver fungiert. In dieser Konfiguration wird ein Server in ISYSMIRRORSERVER mit dem Typ PRIMARY und ein Server mit dem Typ MIRROR definiert. Jeder dieser Server kann als übergeordneter Knoten für einen Kopieknott ausgewählt werden.

**Siehe auch**

- „SYSMIRRORSERVER-Systemansicht“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]
- „SET MIRROR OPTION-Anweisung“ [[SQL Anywhere Server - SQL-Referenzhandbuch](#)]

## Scale-Out-Systeme mit Schreibschutz verwalten

### Tipp

Überprüfen Sie den Status der Datenbankserver in einem Scale-Out-System, indem Sie die Primärdatenbank mithilfe des SQL Anywhere-Monitors überwachen.

Sie können ein Scale-Out-System auch aus Sybase Central überwachen, indem Sie sich mit der Primärdatenbank verbinden und den Status der Datenbankserver im Fensterausschnitt **Gesundheit und Statistik** prüfen.

## Kopieknotten aus Scale-Out-Systemen mit Schreibschutz löschen

Entfernen Sie eine Kopieknottedatenbank aus einem Scale-Out-System mit Schreibschutz, indem Sie die Spiegelserverdefinitionen für den Kopieknotten löschen.

### Voraussetzungen

Sie müssen das MANAGE ANY MIRROR SERVER-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit dem Primärserver (Stammserver) her.
2. Wenn der zu löschende Kopieknotten untergeordnete Kopieknotten hat, führen Sie eine ALTER MIRROR SERVER-Anweisung aus, um alle untergeordneten Kopieknotten einem anderen übergeordneten Knoten zuzuordnen.

```
ALTER MIRROR SERVER "child-copy-server-name"  
FROM SERVER "new-parent-name";
```

3. Führen Sie eine DROP MIRROR SERVER-Anweisung aus, um die Spiegelserverdefinitionen vom zu löschenden Kopieknotten zu löschen.

```
DROP MIRROR SERVER "copy-server-name"
```

Die Spiegeldatenbank wird gestoppt. Wenn die Spiegeldatenbank die einzige laufende Datenbank auf dem Server ist, wird der Server ebenfalls gestoppt.

### Ergebnisse

Der Kopieknotten wird aus dem Scale-Out-System mit Schreibschutz entfernt.

### Nächste Schritte

Löschen Sie die Datenbankdateien.

**Siehe auch**

- „Zuordnung von übergeordneten Knoten zu Kopieknoten“ auf Seite 1550
- „ALTER MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „DROP MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## So handhaben Scale-Out-Systeme mit Schreibschutz den Verlust der Verbindung mit einem übergeordneten Knoten

Wenn der übergeordnete Server für einen Kopieknoten nicht mehr verfügbar ist, bleibt die Datenbank des Kopieknotens verfügbar. Der Kopieknoten versucht über den in der `max_retry_connect_time`-Option für den Spiegelserver definierten Zeitraum (standardmäßig 120 Sekunden) hinweg weiterhin, eine Verbindung zu seinem übergeordneten Knoten herzustellen. Wenn in der angegebenen Zeit keine Verbindung hergestellt werden kann, versucht der Kopieknoten für weitere `max_retry_connect_time` Sekunden, eine Verbindung mit seinem alternativen übergeordneten Knoten (definiert mit der `OR SERVER`-Klausel der `CREATE MIRROR SERVER`-Anweisung) herzustellen, sofern ein solcher definiert wurde.

Wenn keine Verbindung hergestellt werden kann, versucht der Kopieknoten, eine Verbindung mit dem Stammdatenbankserver herzustellen und Logseiten von diesem abzurufen. Wenn die durch `promotion_time` angegebene Zeit verstrichen ist, seit keine Verbindung mit dem ursprünglichen übergeordneten Knoten oder dem alternativen übergeordneten Knoten hergestellt werden konnte, sendet der Kopieknoten eine Anforderung, damit der Stammdatenbankserver den bisherigen übergeordneten Knoten des Kopieknotens durch den Kopieknoten selbst ersetzt und dabei dem Kopieknoten gleichgeordnete Knoten als dessen untergeordnete Knoten zuordnet. Dieses Verhalten kann dazu führen, dass der Kopieknoten mehr als die in der `auto_add_fan_out`-Einstellung festgelegten untergeordneten Knoten hat.

Wenn der Kopieknoten innerhalb von `max_disconnected_time` Sekunden weder mit dem übergeordneten Knoten noch mit dem alternativen übergeordneten Knoten oder dem Stammdatenbankserver eine Verbindung herstellen kann, wird die Datenbank heruntergefahren. Die Standardeinstellung für `max_disconnected_time` lautet, dass nie heruntergefahren wird.

Solange der Kopieknoten versucht, eine Verbindung mit einem anderen Datenbankserver herzustellen, versucht er weiterhin, eine Verbindung mit dem ursprünglichen übergeordneten Knoten herzustellen. Wenn dieser Verbindungsversuch erfolgreich ist, nimmt der Kopieknoten das Abrufen von Logseiten vom ursprünglichen übergeordneten Datenbankserver wieder auf.

Beim ersten Starten eines Kopieknotens wird dessen Datenbank für schreibgeschützte Verbindungen verfügbar, auch wenn andere Knoten in der Struktur, einschließlich des übergeordneten Knotens, nicht verfügbar sind.

### Status eines Servers in einem Scale-Out-System festlegen

Mit der folgenden Anweisung können Sie den Status einer Verbindung mit dem übergeordneten Knoten eines Kopieknotens ermitteln:

```
SELECT DB_EXTENDED_PROPERTY('MirrorServerState',server_name );
```

Mit der folgenden Anweisung erhalten Sie einen Hinweis darauf, wie viel vom Transaktionslog auf den Knoten verarbeitet wurde:

```
SELECT DB_PROPERTY('CurrentRedoPos');
```

Der Wert der CurrentRedoPos-Eigenschaft auf einem untergeordneten Knoten kann mit der LastWrittenRedoPos-Datenbankeigenschaft auf dem Primärserver verglichen werden, um einen Hinweis darauf zu erhalten, auf welchem Stand der Kopieknoten ist.

Die sa\_mirror\_server\_status-Systemprozedur gibt den Verbindungsstatus aller Server unterhalb des Servers zurück, auf dem die Prozedur aufgerufen wird.

### Siehe auch

- „sa\_mirror\_server\_status-Systemprozedur“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „SET MIRROR OPTION-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]
- „CREATE MIRROR SERVER-Anweisung“ [*SQL Anywhere Server - SQL-Referenzhandbuch*]

## Partnerserver in Kopieknoten konvertieren

Konvertieren Sie einen Partnerserver in einem Datenbankspiegelungssystem in einen Kopieknoten in einem Scale-Out-System mit Schreibschutz, ohne das System zu stoppen.

### Voraussetzungen

Sie müssen das MANAGE ANY MIRROR SERVER-Systemprivileg haben.

### Aufgabe

1. Stellen Sie eine Verbindung mit dem zu konvertierenden Partnerserver her und vergewissern Sie sich, dass er die Rolle des Spiegelservers innehat. Sie können nur den Partner mit der Rolle des Spiegelservers konvertieren. Wenn der Server, den Sie in einen Kopieknoten konvertieren möchten, der Primärserver ist, müssen Sie einen Failover initiieren, damit Primär- und Spiegelserver die Rollen tauschen.
2. Stellen Sie eine Verbindung mit dem Primärserver her.
3. Ändern Sie die Spiegelserverdefinitionen:
  - Aktualisieren Sie die Spiegelserverdefinition vom Typ PRIMARY und entfernen Sie die Verbindungsinformationen des zu konvertierenden Partners.
  - Löschen Sie die Spiegelserverdefinition vom Typ MIRROR.
  - Ändern Sie die Partnerdefinition für den Server, der in einen Kopieknoten konvertiert werden soll.

Führen Sie zum Beispiel folgende Anweisungen aus:

```
ALTER MIRROR SERVER mirror_demo_primary  
connection_string='SERVER=mirror_demo_primary;HOST=localhost:6871';  
  
DROP MIRROR SERVER mirror_demo_mirror;
```

```
ALTER MIRROR SERVER mirror_server2 AS COPY FROM SERVER PRIMARY;
```

Sowohl der Stammserver als auch der konvertierte Partnerserver führen im Rahmen dieser Konfigurationsänderungen einen Neustart der Datenbank durch, aber der Server selbst läuft weiter. Während des Neustarts der Datenbank werden Verbindungen mit der Datenbank getrennt.

4. (Optional) Wenn Sie das Spiegelungssystem demontieren möchten, können Sie einfach den Arbiterserver löschen.

## Ergebnisse

Der Partnerserver ist nun ein Scale-Out-Kopieknoten mit Schreibschutz.

## Nächste Schritte

Vergewissern Sie sich, dass der Partner in einen Kopieknoten konvertiert wurde, indem Sie den Inhalt der SYSMIRRORSERVER-Systemansicht anzeigen.

## Siehe auch

- „Praktische Einführung: Partnerserver in Kopieknoten konvertieren“ auf Seite 1563

# Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen

Konfigurieren Sie den Stammknoten des Scale-Out-Systems mit Schreibschutz als Partnerserver in einem Spiegelungssystem, indem Sie einen Arbitr erstellen und einen Kopieknoten in den zweiten Partner für das Spiegelungssystem konvertieren.

## Voraussetzungen

Sie müssen das `MANAGE ANY MIRROR SERVER`-Systemprivileg haben.

## Aufgabe

1. Stellen Sie eine Verbindung mit dem Stammknoten des Scale-Out-Systems mit Schreibschutz her. Führen Sie zum Beispiel folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_root_demo"
```

2. Passen Sie die vorhandenen Partner- und Spiegelserverdefinitionen wie folgt an:

- Erstellen Sie die Spiegelserverdefinition für den neuen Spiegelserver.
- Ändern Sie die Spiegelserverdefinition für den vorhandenen Primärserver (Stammserver) so, dass sie die Hosts und Ports sowohl für den Stammserver als auch für den Spiegelserver enthält.
- Ändern Sie die Spiegelserverdefinition für den vorhandenen Partnerserver (Stammserver) so, dass sie einen Speicherort für eine Statusdatei enthält. Die Statusdatei wird automatisch erstellt.

Führen Sie zum Beispiel folgende Anweisungen aus:

```
-- Define mirror server definition for the mirror server
CREATE MIRROR SERVER scaleout_mirror_demo AS MIRROR
  connection_string='SERVER=scaleout_mirror_demo;HOST=localhost:
6871,localhost:6873';

-- Alter existing primary to include both partners
ALTER MIRROR SERVER scaleout_primary_demo
  connection_string='SERVER=scaleout_primary_demo;HOST=localhost:
6871,localhost:6873';

-- Alter the existing Partner to include state file
ALTER MIRROR SERVER scaleout_root_demo state_file='c:\\scaleoutdemo\\
\\server1\\server1.state';
```

3. Konvertieren Sie einen vorhandenen Kopieknotten in den Spiegelserver. Führen Sie zum Beispiel folgende Anweisung aus:

```
ALTER MIRROR SERVER scaleout_child_demo AS PARTNER state_file='c:\\
\\scaleoutdemo\\\\copynode\\server3.state'
```

4. Starten Sie einen Server, der als Arbiterserver für das Spiegelungssystem fungieren soll. Führen Sie zum Beispiel folgende Befehle aus:

```
mkdir c:\\scaleoutdemo\\arbiter

dbsrv16 -n scaleout_arbiter_demo -su sql -x "TCPIP(PORT=6870)" -xf "c:\\
\\scaleoutdemo\\\\arbiter\\\\arbiter.state" -xa "AUTH=abc;DBN=scaleoutdemo"
```

5. Fügen Sie über den Primärserver (Stammserver) die Spiegelserverdefinitionen für den Arbitr hinzu. Führen Sie zum Beispiel folgende Anweisung aus:

```
CREATE MIRROR SERVER scaleout_arbiter_demo
AS ARBITER
  connection_string ='SERVER=scaleout_arbiter_demo;HOST=localhost:6870';
```

### Ergebnisse

Das Scale-Out-System mit Schreibschutz ist nun auch Teil eines Spiegelungssystems.

### Nächste Schritte

Siehe „Partnerserver verschieben“ auf Seite 1494

### Siehe auch

- „Praktische Einführung: Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen“ auf Seite 1565

## Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen

Richten Sie einen Stammdatenbankserver ein, der automatisch einen Kopieknotten hinzufügt, und überwachen Sie ihn.

## Privilegien

Sie müssen die Systemprivilegien **MANAGE ANY MIRROR SERVER** und **MANAGE ANY DBSPACE** haben.

In dieser praktischen Einführung muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

## Kontext

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

## Siehe auch

- In `%SQLANYSAMPI6%\SQLAnywhere\DBMirror` finden Sie ein Beispiel für die Verwendung eines Datenbankspiegelungssystems in Verbindung mit einem Scale-Out-System.
- [„Praktische Einführung: Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen“](#) auf Seite 1565

# Lektion 1: Scale-Out-System mit Schreibschutz erstellen

Erstellen Sie ein Scale-Out-System mit einem Stammknoten (Stammdatenbankserver) und Kopieknoten (schreibgeschützte Sicherungskopien der Datenbank).

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“](#).

## Kontext und Bemerkungen

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

## Aufgabe

1. Erstellen Sie die Verzeichnisse `c:\scaleoutdemo` und `c:\scaleoutdemo\copynode`.

2. Führen Sie an einer Eingabeaufforderung den folgenden Befehl aus, um die Datenbank *scaleoutdemo.db* zu erstellen, die Daten aus der Beispieldatenbank enthält:

```
newdemo c:\scaleoutdemo\scaleoutdemo.db
```

3. Starten Sie den Stammdatenbankserver für das Scale-Out-System:

```
dbsrv16 -n scaleout_root_demo -su sql -x TCP/IP(port=6871) "c:\scaleoutdemo\scaleoutdemo.db" -xp on
```

Es wird empfohlen, dass Sie die Option `-su` einbeziehen, um das Kennwort für die Dienstprogramm Datenbank anzugeben. Auf diese Weise können Sie ggf. eine Verbindung mit der Dienstprogramm Datenbank herstellen, um den Datenbankserver herunterzufahren.

4. Stellen Sie über Interactive SQL eine Verbindung mit der Datenbank her:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_root_demo;DBN=scaleoutdemo"
```

5. Definieren Sie in Interactive SQL den Stammdatenbankserver für das Scale-Out-System:

```
CREATE MIRROR SERVER "scaleout_primary_demo"  
AS PRIMARY  
connection_string = 'SERVER=scaleout_primary_demo;HOST=localhost:6871';
```

6. Definieren Sie den Stammdatenbankserver als Partner im Scale-Out-System. Der Name des Partnerservers muss dem Namen des Datenbankservers, der in der Befehlszeile zum Starten des Datenbankservers verwendet wird, entsprechen.

```
CREATE MIRROR SERVER "scaleout_root_demo"  
AS PARTNER  
connection_string = 'SERVER=scaleout_root_demo;HOST=localhost:6871';
```

7. Legen Sie die Optionen für den Stammdatenbankserver des Scale-Out-Systems fest:

```
SET MIRROR OPTION auto_add_server='scaleout_primary_demo';  
SET MIRROR OPTION child_creation='automatic';  
SET MIRROR OPTION authentication_string='abc';  
SET MIRROR OPTION auto_add_fan_out='10';
```

8. Erstellen Sie eine Sicherungskopie der Datenbank und platzieren Sie sie im Verzeichnis *c:\scaleoutdemo\copynode*.

```
BACKUP DATABASE DIRECTORY 'c:\\scaleoutdemo\\copynode';
```

9. Starten Sie an einer Eingabeaufforderung die Sicherungskopie der Datenbank als Kopieknoten des *scaleout\_root\_demo*-Stammdatenbankservers:

```
dbsrv16 -n scaleout_child_demo -su sql -x TCP/IP(port=6873) "c:\scaleoutdemo\copynode\scaleoutdemo.db" -xp on
```

10. Stellen Sie in Interactive SQL eine Verbindung mit dem Kopieknoten her:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_child_demo"
```

Sobald sich der Kopieknoten mit dem Stammdatenbankserver verbindet, erhalten Sie eine Warnmeldung, in der Sie darauf hingewiesen werden, dass der Kopieknoten eine schreibgeschützte

Kopie der Datenbank ist. Sie können nun eine Verbindung mit dem Kopieknoten herstellen und dort Abfragen ausführen.

11. In Interactive SQL können Sie die Spiegelserver im Scale-Out-System anzeigen, indem Sie folgende Abfrage ausführen:

```
SELECT * FROM SYSMIRRORSERVER;
```

12. Schließen Sie alle Interactive SQL-Fenster.

## Ergebnisse

Sie haben ein Scale-Out-System mit Schreibschutz erstellt.

## Nächste Schritte

Gehen Sie weiter zu [„Lektion 2: Scale-Out-System mit Schreibschutz aus Sybase Central überwachen“](#) auf Seite 1559.

## Siehe auch

- [„Datenbankserveroption -su“](#) auf Seite 289
- [„Funktionsweise des Scale-Out“](#) auf Seite 1537
- [„Einrichten eines Scale-Out-Systems mit Schreibschutz“](#) auf Seite 1546
- [„Scale-Out-Systeme mit Schreibschutz verwalten“](#) auf Seite 1552

# Lektion 2: Scale-Out-System mit Schreibschutz aus Sybase Central überwachen

Starten Sie Sybase Central und stellen Sie eine Verbindung mit *scaleoutdemo.db* her, um Ihr Scale-Out-System mit Schreibschutz zu überwachen.

## Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Scale-Out-System mit Schreibschutz erstellen“](#) auf Seite 1557.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“](#).

## Aufgabe

1. Starten Sie Sybase Central. Klicken Sie auf **Start » Programme » SQL Anywhere 16 » Administrationstools » Sybase Central**.
2. Stellen Sie in Sybase Central folgendermaßen eine Verbindung mit *scaleoutdemo.db* her:
  - a. Klicken Sie auf **Verbindungen » Verbinden mit SQL Anywhere 16**.
  - b. Füllen Sie im Fenster **Verbinden** die folgenden Felder aus, um eine Verbindung mit der Testdatenbank *scaleoutdemo.db* herzustellen:

- i. Im Feld **Benutzer-ID** geben Sie **DBA** ein.
  - ii. Im Feld **Kennwort** geben Sie **sql** ein.
  - iii. Klicken Sie in der Dropdown-Liste **Aktion** auf **Mit einer laufenden Datenbank auf diesem Computer verbinden**.
  - iv. Im Feld **Servename** geben Sie **scaleout\_root\_demo** ein.
- c. Klicken Sie auf **Verbinden**.
3. Klicken Sie auf die Registerkarte **Übersicht** im Hauptfenster, um die Datenbank *scaleoutdemo.db* zu überwachen.
4. Klicken Sie auf die Dropdown-Liste **Datenbankspiegelung und Skalierung**, um den Primärservernamen des Scale-Out-Systems sowie Informationen zu den Kopieknoten des Scale-Out-Systems anzuzeigen.
5. Schließen Sie Sybase Central.

### Ergebnisse

Sie haben in Sybase Central eine Verbindung mit Ihrem Scale-Out-System mit Schreibschutz hergestellt und es überwacht.

### Nächste Schritte

Gehen Sie weiter zu [„Lektion 9: \(Optional\) Scale-Out-Systeme mit Schreibschutz aus dem SQL Anywhere-Monitor überwachen“](#) auf Seite 1214.

### Siehe auch

- [„SQL Anywhere-Monitor“](#) auf Seite 1115
- [„Schnellstart zur Verwendung des Monitors“](#) auf Seite 1119

## Lektion 3: Scale-Out-System mit Schreibschutz herunterfahren

Um Ihr Scale-Out-System mit Schreibschutz herunterzufahren, müssen Sie die Datenbankserver *scaleout\_child\_demo* und *scaleout\_root\_demo* herunterfahren.

### Voraussetzungen

In dieser Lektion wird davon ausgegangen, dass Sie bereits alle vorherigen Lektionen abgeschlossen haben. Siehe [„Lektion 1: Scale-Out-System mit Schreibschutz erstellen“](#) auf Seite 1557.

In dieser Lektion wird davon ausgegangen, dass Sie die Rollen und Privilegien haben, die im Abschnitt "Privilegien" am Anfang dieser praktischen Einführung aufgeführt sind: [„Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“](#).

### Aufgabe

- Fahren Sie Ihr Scale-Out-System mit Schreibschutz herunter.

- a. Doppelklicken Sie auf das Netzwerkserver-Symbol für den `scaleout_child_demo`-Datenbankserver im Infobereich der Taskleiste.
- b. Klicken Sie im Meldungsfenster des Datenbankservers auf **Herunterfahren**.
- c. Klicken Sie auf **Ja**, um den Datenbankserver herunterzufahren.
- d. Wiederholen Sie diesen Schritt, um den `scaleout_root_demo`-Datenbankserver herunterzufahren.

## Ergebnisse

Ihr Scale-Out-System mit Schreibschutz wird heruntergefahren.

## Praktische Einführung: Server sowohl als Kopieknoten als auch als Arbiter verwenden

Richten Sie einen Server so ein, dass er sowohl als Arbiterserver als auch als Kopieknoten ausgeführt wird. In dieser praktischen Einführung wird beschrieben, wie Sie ein Spiegelungssystem einrichten, das auch in ein Scale-Out-System mit Schreibschutz eingebunden ist.

### Voraussetzungen

Sie müssen das `MANAGE ANY MIRROR SERVER`-Systemprivileg haben.

Bei dieser Aufgabe muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

### Kontext und Bemerkungen

Zwar wird empfohlen, den Arbiterserver in einem Spiegelungssystem auf einem physisch von den anderen Servern getrennten Computer auszuführen, aber dies ist nicht immer möglich.

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

### Aufgabe

1. Erstellen Sie folgende Verzeichnisse: `c:\server1`, `c:\server2` und `c:\arbiter`.
2. Erstellen Sie eine Datenbank namens `mirror_demo.db`, die Daten aus der Beispieldatenbank enthält und ein Transaktionslog hat. Datenbanken ohne Transaktionslog können nicht im Spiegelungsmodus gestartet werden. Führen Sie den folgenden Befehl aus:

```
newdemo c:\server1\mirror_demo.db
```

3. Starten Sie den ersten Datenbankserver. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n mirror_server1 -x "tcpip(PORT=6871)" -su sql "c:\server1\mirror_demo.db" -xp on
```

4. Verbinden Sie sich mit der mirror\_demo-Datenbank. Führen Sie zum Beispiel folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server1"
```

5. Erstellen Sie die Spiegelserverdefinitionen. Führen Sie zum Beispiel folgende SQL-Anweisungen aus:

```
CREATE MIRROR SERVER mirror_demo_primary AS PRIMARY
connection_string='SERVER=mirror_demo_primary;HOST=localhost:
6871,localhost:6872';

CREATE MIRROR SERVER mirror_demo_mirror AS MIRROR
connection_string='SERVER=mirror_demo_primary;HOST=localhost:
6871,localhost:6872';

CREATE MIRROR SERVER mirror_server1 AS PARTNER
connection_string='SERVER=mirror_server1;HOST=localhost:6871'
state_file='c:\server1\server1.state';

CREATE MIRROR SERVER mirror_server2 AS PARTNER
connection_string='SERVER=mirror_server2;HOST=localhost:6872'
state_file='c:\server2\server2.state';
```

6. Erstellen Sie die Arbiterserverdefinition mit der CREATE MIRROR SERVER-Anweisung. Der *Spiegelservername* für den Arbiterserver muss sich von dem in der Verbindungszeichenfolge angegebenen Servernamen unterscheiden.

```
CREATE MIRROR SERVER demo_arbiter AS ARBITER
connection_string='SERVER=demo_server3;HOST=localhost:6870';
```

7. Setzen Sie die Spiegelungsoptionen für das Spiegelungssystem. Sie müssen eine Authentifizierungszeichenfolge angeben und die auto\_add\_server-Option auf den Namen des Primärservers setzen. Führen Sie die folgenden Anweisungen aus:

```
SET MIRROR OPTION auto_add_server='mirror_demo_primary';
SET MIRROR OPTION authentication_string='abc';
```

In der Arbiterserverdefinition muss sich der *Arbiterservername* vom tatsächlichen Servernamen für den Arbiterserver unterscheiden. Die Client-Verbindungszeichenfolge für den Arbiterserver muss den ServerName-Verbindungsparameter [SERVER] mit dem tatsächlichen Servernamen enthalten.

8. Erstellen Sie den Spiegelserver.

- a. Erstellen Sie Kopien der Datenbankdatei und des Transaktionslogs in c:\server1 und fügen Sie sie in c:\server2 und c:\arbiter hinzu. Führen Sie den folgenden Befehl aus:

```
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=mirror_demo"
server2
dbbackup -c "UID=DBA;PWD=sql;SERVER=mirror_server1;DBN=mirror_demo"
arbiter
```

- b. Starten Sie den Spiegelserver:

```
dbsrv16 -n mirror_server2 -x "tcpip(port=6872)"
server2\mirror_demo.db -su sql -xp on
```

9. Starten Sie den Arbiterserver als Kopieknoten und als Arbitrer, indem Sie die Serveroptionen -xa, -xp und -xf angeben.

```
dbsrvl6 -n demo_server3 -x "tcpip(port=6870)" arbiter\mirror_demo.db -xp
on -xf arbiter\arbiter.state -xa "AUTH=abc;DBN=mirror_demo" -su sql
```

10. Verwenden Sie das Dienstprogramm dbping, um zu ermitteln, wann die Hochverfügbarkeitskonfiguration bereit ist:

```
dbping -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" -pd
Mirrorstate,PartnerState,ArbiterState

SQL Anywhere Server Ping Utility Version 16.0.4157
Type          Property          Value
-----
Database      MirrorState          synchronized
Database      PartnerState         connected
Database      ArbiterState         connected
Ping database successful.
```

11. Verwenden Sie die folgende Abfrage, um die in diesem System mit Hochverfügbarkeit gespiegelten Knoten anzuzeigen:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server1" "SELECT
server_name,state FROM sa_mirror_server_status()"
```

12. Vergewissern Sie sich, dass demo\_server3 ein COPY-Knoten ist und dass der Arbitrer verbunden ist, indem Sie den Inhalt der SYSMIRRORSERVER-Tabelle überprüfen:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" "SELECT
server_name, server_type FROM SYSMIRRORSERVER"
```

## Ergebnisse

Der Server, der den Arbitrer ausführt, führt auch einen Kopieknoten aus.

## Praktische Einführung: Partnerserver in Kopieknoten konvertieren

In dieser praktischen Einführung wird beschrieben, wie Sie einen Partnerserver in einem Datenbankspiegelungssystem in einen Kopieknoten in einem Scale-Out-System mit Schreibschutz konvertieren, ohne das System zu stoppen.

### Voraussetzungen

Diese praktische Einführung basiert auf dem unter [„Praktische Einführung: Datenbankspiegelungssysteme erstellen“](#) beschriebenen Datenbankspiegelungssystem.

Sie müssen das MANAGE ANY MIRROR SERVER-Systemprivileg haben.

Standardmäßig erfordert die Verwendung der Anweisung ALTER DATABASE...SET PARTNER FAILOVER das SERVER OPERATOR-Systemprivileg. Die erforderlichen Privilegien können mithilfe der Datenbankserveroption -gd geändert werden.

### Kontext und Bemerkungen

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

### Aufgabe

1. Stellen Sie eine Verbindung mit dem zu konvertierenden Partnerserver her und vergewissern Sie sich, dass er die Rolle des Spiegelservers innehat. Sie können nur den Partner mit der Rolle des Spiegelservers konvertieren. Wenn der Server, den Sie in einen Kopieknotten konvertieren möchten, der Primärserver ist, müssen Sie einen Failover initiieren, damit Primär- und Spiegelserver die Rollen tauschen. Stellen Sie zum Beispiel eine Verbindung mit `mirror_server2` her:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_server2;HOST=localhost:6872"
```

Die `MirrorRole`-Datenbankseigenschaft gibt die aktuelle Rolle des Servers zurück. Führen Sie die folgende Anweisung aus:

```
SELECT DB_PROPERTY( 'MirrorRole' );
```

Wenn **Primary** zurückgegeben wird, initiieren Sie einen Failover, indem Sie die folgende Anweisung ausführen:

```
ALTER DATABASE SET PARTNER FAILOVER;
```

Die aktuelle Primärdatenbank wird gestoppt und neu gestartet.

2. Stellen Sie eine Verbindung mit dem Primärserver her.

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary;HOST=localhost:6871,localhost:6872"
```

3. Ändern Sie die Definitionen:

- Aktualisieren Sie die Spiegelserverdefinition vom Typ **PRIMARY** und entfernen Sie die Verbindungsinformationen des zu konvertierenden Partners.
- Löschen Sie die Spiegelserverdefinition vom Typ **MIRROR**.
- Ändern Sie die Partnerdefinition für den Server, der in einen Kopieknotten konvertiert werden soll.

Führen Sie die folgenden Anweisungen aus:

```
ALTER MIRROR SERVER mirror_demo_primary  
connection_string='SERVER=mirror_demo_primary;HOST=localhost:6871';  
  
DROP MIRROR SERVER mirror_demo_mirror;  
  
ALTER MIRROR SERVER mirror_server2 AS COPY FROM SERVER PRIMARY;
```

Beide Partnerserver führen im Rahmen dieser Konfigurationsänderungen einen Neustart der Datenbank durch, aber der Server selbst läuft weiter. Während des Neustarts der Datenbank werden Verbindungen mit der Datenbank getrennt.

4. (Optional) Wenn Sie das Spiegelungssystem demontieren möchten, können Sie einfach den Arbiterserver löschen. Führen Sie die folgende Anweisung aus:

```
DROP MIRROR SERVER demo_arbiter;
```

5. Vergewissern Sie sich, dass mirror\_server2 in einen Kopieknottens konvertiert wurde, indem Sie den Inhalt der SYSMIRRORSERVER-Systemansicht anzeigen. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=mirror_demo_primary" "SELECT  
server_name, server_type FROM SYSMIRRORSERVER"
```

## Ergebnisse

Der Spiegelserver ist nun ein Scale-Out-Kopieknottens mit Schreibschutz.

# Praktische Einführung: Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen

In dieser praktischen Einführung wird beschrieben, wie Sie ein Spiegelungssystem zu einem vorhandenen Scale-Out-System mit Schreibschutz hinzufügen. Der Stammserver des Scale-Out-Systems mit Schreibschutz wird gleichzeitig zum Spiegelserver.

## Voraussetzungen

In dieser praktischen Einführung wird davon ausgegangen, dass ein laufendes Scale-Out-System mit Schreibschutz vorhanden ist, wie unter [„Praktische Einführung: Scale-Out-System mit Schreibschutz erstellen“](#) beschrieben.

Konfigurieren Sie den Stammknoten des Scale-Out-Systems mit Schreibschutz als Primärserver in einem Spiegelungssystem, indem Sie Spiegelserver definieren, einen Arbiterserver erstellen und Kopieknottens in Spiegelpartner des Spiegelungssystems konvertieren.

Sie müssen das MANAGE ANY MIRROR SERVER-Systemprivileg haben.

In dieser praktischen Einführung muss eine Kopie der Datenbank gesichert werden. Weitere Hinweise finden Sie je nach Sicherungsmethode in den Beschreibungen der entsprechenden Privilegien.

## Kontext und Bemerkungen

Bei dieser praktischen Einführung werden alle Datenbankserver auf demselben Computer ausgeführt. In einer Produktionsumgebung müssen die einzelnen Datenbankserver jedoch auf separaten Computern installiert werden.

Wenn Sie diese praktische Einführung auf Datenbankserver anwenden, die auf verschiedenen Computern ausgeführt werden, müssen Sie in den Verbindungszeichenfolgen die Verweise auf **localhost** in die tatsächlichen Computernamen ändern.

### Aufgabe

1. Stellen Sie eine Verbindung mit dem Stammknoten des Scale-Out-Systems mit Schreibschutz her. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_root_demo"
```

2. Definieren Sie Primär- und Spiegelserver. Führen Sie die folgenden Anweisungen aus:

```
-- Alter existing primary to include both partners
ALTER MIRROR SERVER scaleout_primary_demo
connection_string='SERVER=scaleout_primary_demo;HOST=localhost:
6871,localhost:6873';

-- Alter existing Partner to include state file
ALTER MIRROR SERVER scaleout_root_demo state_file='c:\\scaleoutdemo\\
\\server1\\server1.state';

-- Define mirror
CREATE MIRROR SERVER scaleout_mirror_demo AS MIRROR
connection_string='SERVER=scaleout_mirror_demo;HOST=localhost:
6871,localhost:6873';

--Convert an existing copy node to the mirror server

ALTER MIRROR SERVER scaleout_child_demo
connection_string='SERVER=scaleout_child_demo;HOST=localhost:6873'
state_file='c:\\scaleoutdemo\\copynode\\server3.state';
```

3. Konvertieren Sie einen vorhandenen Kopieknoten in den Spiegelserver. Führen Sie die folgende Anweisung aus:

```
--Convert an existing copy node to the mirror server

ALTER MIRROR SERVER scaleout_child_demo
connection_string='SERVER=scaleout_child_demo;HOST=localhost:6873'
state_file='c:\\scaleoutdemo\\copynode\\server3.state';
```

4. Starten Sie einen Server, der als Arbiterserver für das Spiegelungssystem fungieren soll. Führen Sie die folgenden Befehle aus:

```
mkdir c:\\scaleoutdemo\\arbiter

dbsrv16 -n scaleout_arbiter_demo -su sql -x "TCPIP(PORT=6870)" -xf "c:\\
\\scaleoutdemo\\arbiter\\arbiter.state" -xa "AUTH=abc;DBN=scaleoutdemo"
```

5. Stellen Sie eine Verbindung mit dem Stammknoten her und fügen Sie den Arbiters hinzu. Führen Sie die folgenden Anweisungen aus.

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_primary_demo"

CREATE MIRROR SERVER scaleout_arbiter_demo
AS ARBITER
connection_string = 'SERVER=scaleout_arbiter_demo;HOST=localhost:6870';
```

6. Konvertieren Sie einen vorhandenen Kopieknoten in den Spiegelserver. Führen Sie die folgende Anweisung aus:

```
ALTER MIRROR SERVER scaleout_child_demo AS PARTNER state_file='c:\\
\\scaleoutdemo\\copynode\\server3.state'
```

7. Vergewissern Sie sich, dass `scaleout_child_demo` der Spiegelserver ist, indem Sie den Inhalt der `SYSMIRRORSERVER`-Tabelle überprüfen. Führen Sie den folgenden Befehl aus:

```
dbisql -c "UID=DBA;PWD=sql;SERVER=scaleout_primary_demo" "SELECT
server_name, server_type FROM SYSMIRRORSERVER"
```

Der Server `scaleout_child_demo` ist nun der zweite PARTNER-Server.

8. Aktualisieren Sie die Verbindungszeichenfolgen in Ihren Clientanwendungen, um die Adressen beider Partner im Host-Verbindungsparameter anzugeben. Zum Beispiel:

```
dbping -c "UID=DBA;PWD=sql;SERVER=scaleout_primary_demo;HOST=localhost:
6871,localhost:6873"
```

9. (Optional) Fügen Sie einen weiteren Kopieknoten hinzu.
- Erstellen Sie eine Sicherungskopie der Primärdatenbank und platzieren Sie sie im Verzeichnis `c:\scaleoutdemo\copynode2`.
  - Führen Sie die folgende Anweisung aus:

```
BACKUP DATABASE DIRECTORY 'c:\\scaleoutdemo\\copynode2';
```

- Starten Sie die Sicherungskopie der Datenbank als untergeordneten Knoten (Kopieknoten) des Datenbankservers `scaleout_root_demo`. Führen Sie den folgenden Befehl aus:

```
dbsrv16 -n scaleout_child2_demo -su sql -x TCPIP(port=6874) "c:
\\scaleoutdemo\\copynode2\\scaleoutdemo.db" -xp on
```

## Ergebnisse

Das Scale-Out-System mit Schreibschutz ist nun auch Teil eines Spiegelungssystems.

## Siehe auch

- „Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen“ auf Seite 1555



---

# Replikation

Dieser Abschnitt beschreibt, wie Sie SQL Anywhere als Open Server verwenden.

## Siehe auch

- [SQL Remote](#)
- „Synchronisationstechnologie im Vergleich“ [[SQL Anywhere 16 - Einführung](#)]

## SQL Anywhere als Open Server

SQL Anywhere kann gegenüber Clientanwendungen als Open Server auftreten. Durch diese Funktion können Sybase Open Client-Anwendungen native Verbindungen mit SQL Anywhere-Datenbanken herstellen.

Wenn Sie eine Sybase-Anwendung einfach nur mit SQL Anywhere benutzen wollen, brauchen Sie sich über Sybase Open Client, Sybase Open Server oder TDS nicht weiter zu informieren. Kenntnisse darüber, wie diese Komponenten zusammenwirken, können jedoch beim Konfigurieren der Datenbank und beim Einrichten von Anwendungen hilfreich sein.

### Sybase Open Client und Sybase Open Server

SQL Anywhere und andere Mitglieder der Adaptive Server-Familie verhalten sich als **Open Server**. Das heißt, Sie können Clientanwendungen entwickeln, die die **Sybase Open Client**-Bibliotheken von Sybase verwenden. Sybase Open Client enthält sowohl die Clientbibliothek (CT-Library) als auch ältere DB Library-Schnittstellen.

### Tabular Data Stream (TDS)

Sybase Open Clients und Sybase Open Server tauschen ihre Daten über ein Anwendungsprotokoll aus, das als **Tabular Data Stream** (TDS) bezeichnet wird. Alle Anwendungen, die mit den Sybase Open Clientbibliotheken erstellt werden, sind auch TDS-Anwendungen, da die Sybase Open Client-Bibliotheken die TDS-Schnittstelle verwalten. Einige Anwendungen allerdings, wie zum Beispiel jConnect, sind TDS-Anwendungen, obwohl sie die Sybase Open Clientbibliotheken nicht benutzen. Sie kommunizieren direkt über das TDS-Protokoll.

Viele Anwendungen haben eine eigene Schnittstelle zu TDS, während die Open Server die Sybase Open Server-Bibliotheken als TDS-Schnittstelle verwenden. Sybase Adaptive Server Enterprise und SQL Anywhere haben solche internen TDS-Schnittstellen. Sie treten gegenüber Clientanwendungen als Open Server auf, verwenden aber die Sybase Open Server-Bibliotheken nicht.

### Programmierschnittstellen und Anwendungsprotokolle

SQL Anywhere unterstützt zwei Anwendungsprotokolle. TDS wird für Sybase Open Client-Anwendungen und für andere Sybase-Anwendungen verwendet, wie z.B. OmniConnect. Für ODBC- und Embedded SQL-Anwendungen wird ein separates Anwendungsprotokoll verwendet, das speziell für SQL Anywhere entwickelt wurde.

### TDS benutzt TCP/IP

Anwendungsprotokolle wie TDS sind über den Kommunikationsprotokollen der niedrigeren Ebene angeordnet, die den Netzwerkverkehr abwickeln. SQL Anywhere unterstützt TDS nur über das TCP/IP-Netzwerkprotokoll. Im Gegensatz dazu unterstützt das für SQL Anywhere speziell entwickelte Anwendungsprotokoll einige Netzwerkprotokolle sowie ein Protokoll für gemeinsam genutzten Speicher, das für Anwendungen auf einem einzelnen Computer konzipiert ist.

## Sybase-Anwendungen und SQL Anywhere

Die Fähigkeit von SQL Anywhere, als Open Server zu fungieren, ermöglicht es Sybase-Anwendungen wie OmniConnect, mit SQL Anywhere zusammenzuarbeiten.

### OmniConnect-Unterstützung

Sybase OmniConnect bietet eine vereinheitlichte Sicht verstreuter Daten in einer Organisation und ermöglicht es damit den Benutzern, mehrere Datenquellen abzufragen, ohne zu wissen, wie die Daten im Einzelnen strukturiert sind oder wo sie sich befinden. Außerdem führt OmniConnect heterogene Verknüpfungen von Daten im Unternehmen durch, sodass Tabellenverknüpfungen quer über Plattformen in Datenbanken wie IBM DB2, Sybase Adaptive Server Enterprise, Oracle und VSAM möglich sind.

Mit der Open Server-Schnittstelle kann SQL Anywhere als Datenquelle für OmniConnect fungieren.

## Einrichten von SQL Anywhere als Open Server

### Systemanforderungen für den Einsatz von SQL Anywhere als Open Server

Es gibt im Client und im Server getrennte Anforderungen für den Einsatz von SQL Anywhere als Open Server.

#### Serverseitige Anforderungen

Serverseitig muss folgende Ausstattung gegeben sein, damit SQL Anywhere als Open Server betrieben werden kann:

- **SQL Anywhere-Serverkomponenten** Sie müssen den Netzwerkservice (*dsrv16.exe*) verwenden, wenn Sie über ein Netzwerk auf einen Open Server zugreifen möchten. Den Personal Server (*dbeng16.exe*) können Sie nur bei Verbindungen von demselben Computer als Open Server verwenden.
- **TCP/IP** Sie brauchen einen TCP/IP-Protokoll-Stack, um SQL Anywhere als Open Server verwenden zu können, auch wenn Sie sich nicht über ein Netzwerk verbinden.

#### Clientseitige Anforderungen

Um Sybase Clientanwendungen zur Verbindung mit einem Open Server (darunter auch SQL Anywhere) zu verwenden, benötigen Sie die folgende Ausstattung:

- **Sybase Open Client-Komponenten** Die Sybase Open Client-Bibliotheken stellen die Netzwerk-Bibliotheken bereit, die Ihre Anwendung benötigt, um über TDS zu kommunizieren, wenn Ihre Anwendung Sybase Open Client verwendet.
- **jConnect** Wenn Ihre Anwendung JDBC verwendet, benötigen Sie jConnect und eine Java-Laufzeitumgebung. Um jConnect herunterzuladen, navigieren Sie zu <http://www.sybase.com/products/allproductsa-z/softwaredeveloperkit/jconnect>.
- **DSEdit** Sie benötigen DSEdit, den Verzeichnisdienst-Editor, um die Servernamen für Ihre Sybase Open Client-Anwendung verfügbar zu machen. Auf Unix-Plattformen wird dieses Dienstprogramm sybinit genannt.

DSEdit ist nicht in SQL Anywhere enthalten. Es ist Teil der Sybase Open Server-Software.

## Starten eines Datenbankservers als Open Server

Das TCP/IP-Kommunikationsprotokoll ist erforderlich, wenn ein SQL Anywhere-Datenbankserver als Open Server verwendet wird. Dieses Protokoll wird für den Netzwerkserver standardmäßig gestartet.

Sie können den Personal Datenbankserver als Open Server für die Kommunikation auf demselben Computer verwenden, weil er das TCP/IP-Protokoll unterstützt. Sie müssen das Protokoll beim Starten des Personal Servers anfordern. Der folgende Befehl startet beispielsweise das TCP/IP-Kommunikationsprotokoll:

```
dbeng16 -x tcpip -n myserver c:\mydata.db
```

Der SQL Anywhere-Datenbankserver kann andere Anwendungen über das TCP/IP-Protokoll bedienen, während er gleichzeitig auch Sybase Open Client-Anwendungen über TDS bedient.

### Sybase Open Client-Einstellungen

Um eine Verbindung mit dem Datenbankserver herzustellen, muss die Schnittstellendatei auf dem Clientcomputer einen Eintrag enthalten, der den Namen des Computers angibt, auf dem der Datenbankserver läuft, sowie den verwendeten TCP/IP-Port.

### Siehe auch

- [ServerPort-Verbindungseigenschaft auf Seite 736](#)

## Eigenschaften von Sybase Open Client- und jConnect-Verbindungen

Wenn SQL Anywhere Anwendungen über TDS versorgt, setzt er automatisch relevante Datenbankoptionen auf Werte, die mit dem Standardverhalten von Adaptive Server Enterprise kompatibel sind. Diese Optionen werden vorübergehend gesetzt, nur für die Dauer der Verbindung. Die Clientanwendung kann sie jederzeit aufheben.

### Standardeinstellungen

Zu den Datenbankoptionen, die bei der Verbindung gesetzt werden, gehören folgende:

Option	Gesetzt auf
allow_nulls_by_default	Off
ansi_blanks	On
ansinull	Off
chained	Off
close_on_endtrans	Off
date_format	YYYY-MM-DD
date_order	MDY
escape_character	Off
isolation_level	1
on_tsq_l_error	Continue
quoted_identifier	Off
time_format	HH:NN:SS.SSS
timestamp_format	YYYY-MM-DD HH:NN:SS.SSS
tsq_l_variables	On

### So werden die Startoptionen gesetzt

Die Standard-Datenbankoptionen werden für die TDS-Verbindung über eine Systemprozedur gesetzt, die sp\_tsq\_l\_environment heißt. Diese Prozedur setzt folgende Optionen:

```
SET TEMPORARY OPTION allow_nulls_by_default='Off';
SET TEMPORARY OPTION ansi_blanks='On';
SET TEMPORARY OPTION ansinull='Off';
SET TEMPORARY OPTION chained='Off';
SET TEMPORARY OPTION close_on_endtrans='Off';
SET TEMPORARY OPTION date_format='YYYY-MM-DD';
SET TEMPORARY OPTION date_order='MDY';
SET TEMPORARY OPTION escape_character='Off';
SET TEMPORARY OPTION isolation_level='1';
SET TEMPORARY OPTION on_tsq_l_error='Continue';
SET TEMPORARY OPTION quoted_identifier='Off';
SET TEMPORARY OPTION time_format='HH:NN:SS.SSS';
SET TEMPORARY OPTION timestamp_format='YYYY-MM-DD HH:NN:SS.SSS';
SET TEMPORARY OPTION tsq_l_variables='On';
```

#### Hinweis

Ändern Sie nicht die sp\_tsq\_l\_environment-Prozedur. Sie wird vom System in dieser Form benötigt.

Die Prozedur setzt nur Optionen für Verbindungen, die das TDS-Kommunikationsprotokoll verwenden. Dazu gehören Sybase Open Client- und JDBC-Verbindungen mit jConnect. Andere Verbindungen (ODBC und Embedded SQL) haben Standardeinstellungen für die Datenbank.

## Optionseinstellungen für TDS-Verbindungen ändern

Wenn SQL Anywhere Anwendungen über TDS bedient, setzt es relevante Datenbankoptionen automatisch auf Werte, die mit dem Standardverhalten von Adaptive Server Enterprise kompatibel sind. Sie können die Optionen für TDS-Verbindungen jederzeit ändern.

### Voraussetzungen

Es gibt keine Voraussetzungen für diese Aufgabe.

### Aufgabe

1. Erstellen Sie eine Prozedur, die die gewünschten Datenbankoptionen setzt.
2. Setzen Sie die login\_procedure-Option auf den Namen der neuen Prozedur.

### Ergebnisse

Zukünftige Verbindungen verwenden diese Prozedur. Sie können die Prozedur für verschiedene Benutzer-IDs unterschiedlich konfigurieren.

### Beispiel

In diesem Prozedurbeispiel wird nur die quoted\_identifier-Option gegenüber der Standardeinstellung geändert.

```
CREATE PROCEDURE my_startup_procedure()  
BEGIN  
    IF CONNECTION_PROPERTY('CommProtocol')='TDS' THEN  
        SET TEMPORARY OPTION quoted_identifier='Off';  
    END IF  
END;
```

Führen Sie den folgenden Befehl aus, um die login\_procedure-Option auf den Namen einer neuen Prozedur zu setzen:

```
SET OPTION login_procedure= 'DBA.my_startup_procedure';
```

### Siehe auch

- [„Datenbankoptionen“ auf Seite 544](#)



---

# Index

## Symbole

#

in Konfigurationsdateien verwenden,882

&

in Konfigurationsdateien verwenden,882

Unix-Befehlszeile,192

-? , Serveroption

unter Windows Mobile nicht unterstützt,426

-? server, Option

Datenbankserveroption,216

-a, Option

Datenbankoption,321

Dienstprogramm zur Logkonvertierung  
(dbtran),948

Initialisierungsdienstprogramm (dbinit),927

Linux, Dienstprogramm für Dienste (dbsvc),969

Windows, Dienstprogramm für Dienste  
(dbsvc),976

-ac, Option

Dienstprogramm für Supportanfragen  
(dbsupport),993

-ad, Option

Datenbankoption,322

-af, Option

Dienstprogramm für Supportanfragen  
(dbsupport),993

Initialisierungsdienstprogramm (dbinit),927

-al, Option

Datenbankoption,323

Datenbankserveroption,216

-an, Option

Dienstprogramm zum Entladen (dbunload),1001

-ap, Option

Broadcast Repeater-Dienstprogramm (dbns16),892

Dienstprogramm zum Entladen (dbunload),1001

-ar, Option

Datenbankoption,323

Dienstprogramm zum Entladen (dbunload),1001

-as, Option

Datenbankoption,324

Linux, Dienstprogramm für Dienste (dbsvc),969

Windows, Dienstprogramm für Dienste  
(dbsvc),976

-aw, Option

Sicherungsdienstprogramm (dbbackup),886

-b, Option

Datenbankserveroption,216

Datenquelle, Dienstprogramm (dbdsn),906

Dienstprogramm zum Erstellen von Zertifikaten  
(createcert),894

Initialisierungsdienstprogramm (dbinit),927

Sicherungsdienstprogramm (dbbackup),886

-bc, Option

Sicherungsdienstprogramm (dbbackup),886

-c, Option

Datenbankserveroption,217

Datenquelle, Dienstprogramm (dbdsn),908

Dienstprogramm dbisqlc,915

Dienstprogramm zum Entladen (dbunload),1001

Dienstprogramm zum Erstellen von Zertifikaten  
(createcert),894

Dienstprogramm zum Upgrade (dbupgrad),1018

Dienstprogramm zur Logkonvertierung  
(dbtran),948

Histogramm-Dienstprogramm, (dbhist),924

Informationsdienstprogramm (dbinfo),926

Initialisierungsdienstprogramm (dbinit),927

Interactive SQL (dbisql), Dienstprogramm,939

Ping-Dienstprogramm (dbping),955

Sicherung, Dienstprogramm (dbbackup),886

SQL Anywhere-Konsolendienstprogramm  
(dbconsole),982

SQL Anywhere-Skriptausführung,  
Dienstprogramm (dbrunsql),959

Stopp-Dienstprogramm (dbstop),984

Validierungs-Dienstprogramm (dbvalid),1021

Verbindungszeichenfolgen,31

-ca, Option

Datenbankserveroption,219

Dienstprogramm zum Erstellen von Zertifikaten  
(createcert),894

-cc, Option

Datenbankserveroption,220

Dienstprogramm für Supportanfragen  
(dbsupport),991

-cd, Option

Dienstprogramm für Supportanfragen  
(dbsupport),991

-ce, Option

Dienstprogramm für Supportanfragen  
(dbsupport),991

-cet, Option

- Dienstprogramm für Supportanfragen (dbsupport),991
- ch, Option
  - Datenbankserveroption,221
- chx, Option
  - Datenbankserveroption,222
- cid, Option
  - Dienstprogramm für Supportanfragen (dbsupport),991
- ck, Option
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- cl, Option
  - Datenbankserveroption,224
  - Datenquelle, Dienstprogramm (dbdsn),905
- cm, Option
  - Datenquelle, Dienstprogramm (dbdsn),906
  - Dienstprogramm zum Entladen (dbunload),1001
  - Linux, Dienstprogramm für Dienste (dbsvc),972
  - unter Windows Mobile nicht unterstützt,426
  - Windows, Dienstprogramm für Dienste (dbsvc),979
- co, Option
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- cp, Option
  - Datenbankserveroption,225
  - Dienstprogramm für Supportanfragen (dbsupport),991
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- cr, Option
  - Datenbankserveroption,226
  - Dienstprogramm für Supportanfragen (dbsupport),991
- cs, Option
  - Datenbankserveroption,227
- cv, Option
  - Datenbankserveroption,227
- cw, Option
  - Datenquelle, Dienstprogramm (dbdsn),908
- d, Option
  - Datenquelle, Dienstprogramm (dbdsn),905
  - Dienstprogramm dbisqlc,915
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - Dienstprogramm zum Entladen (dbunload),1001
- Dienstprogramm zur Logkonvertierung (dbtran),948
- Interactive SQL (dbisql), Dienstprogramm,939
- Linux, Dienstprogramm für Dienste (dbsvc),968
- Ping-Dienstprogramm (dbping),955
- Serverauflistung, Dienstprogramm (dblocate),961
- Sicherungsdienstprogramm (dbbackup),886
- SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
- Stopp-Dienstprogramm (dbstop),984
- Validierungs-Dienstprogramm (dbvalid),1021
- Windows, Dienstprogramm für Dienste (dbsvc),974
- d1, Option
  - Interactive SQL (dbisql), Dienstprogramm,939
- datasource, Option
  - Interactive SQL (dbisql), Dienstprogramm,939
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
- dba, Option
  - Initialisierungsdienstprogramm (dbinit),927
- dbs, Option
  - Initialisierungsdienstprogramm (dbinit),927
- dc, Option
  - Dienstprogramm zum Entladen (dbunload),1001
- dh, Option
  - Datenbankoption,326
- dn, Option
  - Serverauflistung, Dienstprogramm (dblocate),961
- dr, Option
  - Datenquelle, Dienstprogramm (dbdsn),906
- ds, Option
  - Datenbankoption,325
- dt, Option
  - Datenbankserveroption,228
- dv, Option
  - Serverauflistung, Dienstprogramm (dblocate),961
- e, Option
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Entladen (dbunload),1001
  - SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
- ea, Option
  - Dienstprogramm zum Entladen (dbunload),1001
  - Initialisierungsdienstprogramm (dbinit),927
- ec, Option
  - Datenbankserveroption,230

- 
- Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - ec-Option
    - Client/Server-Kommunikationen sichern,1454
  - ek, Option
    - Datenbankoption,326
    - Dienstprogramm zum Entladen (dbunload),1001
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Initialisierungsdienstprogramm (dbinit),927
    - Löschen-Dienstprogramm (dberase),916
    - Transaktionslog-Dienstprogramm (dblog),998
  - en, Option
    - Ping-Dienstprogramm (dbping),955
  - ep, Option
    - Datenbankserveroption,233
    - Dienstprogramm zum Entladen (dbunload),1001
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Initialisierungsdienstprogramm (dbinit),927
    - Löschen-Dienstprogramm (dberase),916
    - Transaktionslog-Dienstprogramm (dblog),998
  - er, Option
    - Dienstprogramm zum Entladen (dbunload),1001
  - es, Option
    - Datenbankserveroption,234
  - et, Option
    - Dienstprogramm zum Entladen (dbunload),1001
    - Initialisierungsdienstprogramm (dbinit),927
  - f, Option
    - Datenbankserveroption,234
    - Datenquelle, Dienstprogramm (dbdsn),906
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Interactive SQL (dbisql), Dienstprogramm,939
    - Spawn-Dienstprogramm (dbspawn),983
    - SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
  - fc, Option
    - Datenbankserveroption,235
  - fips, Option
    - AES256\_FIPS-Verschlüsselungsalgorithmus,237
    - AES\_FIPS-Verschlüsselungsalgorithmus,237
    - Datenbankserveroption,237
  - fx, Option
    - Validierungs-Dienstprogramm (dbvalid),1021
  - g, Option
    - Datenquelle, Dienstprogramm (dbdsn),905
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Linux, Dienstprogramm für Dienste (dbsvc),968
  - SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
  - Windows, Dienstprogramm für Dienste (dbsvc),974
  - ga, Option
    - Datenbankserveroption,238
  - gb, Option
    - Datenbankserveroption,238
    - unter Windows Mobile nicht unterstützt,426
  - gc, Option
    - Datenbankserveroption,239
  - gd, Option
    - Datenbankserveroption,240
  - ge, Option
    - Datenbankserveroption,241
    - unter Windows Mobile nicht unterstützt,426
  - gf, Option
    - Datenbankserveroption,241
  - gk, Option
    - Datenbankserveroption,242
  - gl, Option
    - Datenbankserveroption,242
  - gm, Option
    - Datenbankserveroption (dbsrv16),244
  - gn, Option
    - Datenbankserver, Multiprogrammierung-Stufe,175
    - Datenbankservernutzung,174
    - Datenbankserveroption (dbsrv16),244
  - gna, Option
    - Auswirkung auf abfrageinterne Parallelität,245
    - Datenbankserveroption (dbsrv16),245
    - unter Windows Mobile nicht unterstützt,426
  - gnh, Option
    - Auswirkung auf abfrageinterne Parallelität,246
    - Datenbankserveroption (dbsrv16),246
    - unter Windows Mobile nicht unterstützt,426
  - gnl, Option
    - Auswirkung auf abfrageinterne Parallelität,247
    - Datenbankserveroption (dbsrv16),247
    - unter Windows Mobile nicht unterstützt,426
  - gns, Option
    - Datenbankserveroption (dbsrv16),248
    - unter Windows Mobile nicht unterstützt,426
  - gp, Option

- Datenbankserveroption,249
- gr, Option
  - Datenbankserveroption,249
- gss, Option
  - Datenbankservernutzung,174
  - Datenbankserveroption,250
- gt, Option
  - Datenbankservernutzung,174
  - Datenbankserveroption,251
  - unter Windows Mobile nicht unterstützt,426
- gta, Option
  - Datenbankserveroption (dbsrv16),252
- gtc, Option
  - Datenbankservernutzung,174
  - Datenbankserveroption,253
  - unter Windows Mobile nicht unterstützt,426
- gu, Option
  - Datenbankserveroption,255
  - Privilegien zur Ausführung von Anweisungen in der Dienstprogrammdatenbank steuern,255
- h, Option
  - Sicherungsdienstprogramm (dbbackup),886
- host, Option
  - Interactive SQL (dbisql), Dienstprogramm,939
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
- i, Option
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Initialisierungsdienstprogramm (dbinit),927
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Windows, Dienstprogramm für Dienste (dbsvc),976
- ii, Option
  - Dienstprogramm zum Entladen (dbunload),1001
- im, Option
  - Datenbankserveroption,257
  - In-Memory-Modus,170
- io, Option
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- ip, Option
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
- ir, Option
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Transaktionslog-Dienstprogramm (dblog),998
- is, Option
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Transaktionslog-Dienstprogramm (dblog),998
- it, Option
  - Dienstprogramm zur Logkonvertierung (dbtran),948
- iu, Option
  - Dienstprogramm für Supportanfragen (dbsupport),987
- ix, Option
  - Dienstprogramm zum Entladen (dbunload),1001
- j, Option
  - Dienstprogramm zur Logkonvertierung (dbtran),948
- k, Option
  - Datenbankserveroption,259
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Initialisierungsdienstprogramm (dbinit),927
  - Sicherungsdienstprogramm (dbbackup),886
- kd, Option
  - Dienstprogramm zum Entladen (dbunload),1001
- kl, Option
  - Datenbankserveroption,260
- ko, Option
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- kp, Option
  - Datenbankserveroption,261
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- kr, Option
  - Datenbankserveroption,262
- krb, Option
  - Datenbankserveroption,263
- ks, Option
  - Datenbankserveroption,264
- ksc, Option
  - Datenbankserveroption,264
- ksd, Option
  - Datenbankserveroption,264
- l, Option
  - Datenquelle, Dienstprogramm (dbdsn),905

---

Dienstprogramm zum Entladen (dbunload),1001	-nr, Option
Dienstprogramm zur Serverlizenzierung (dblic),964	Dienstprogramm für Supportanfragen (dbsupport),993
Initialisierungsdienstprogramm (dbinit),927	-ns, Option
Linux, Dienstprogramm für Dienste (dbsvc),968	Datenquelle, Dienstprogramm (dbdsn),906
Ping-Dienstprogramm (dbping),955	-o, Option
Sicherung, Dienstprogramm (dbbackup),886	Datenbankserveroption,268
Windows, Dienstprogramm für Dienste (dbsvc),974	Datenquelle, Dienstprogramm (dbdsn),906
-lc, Option	dialogfreier Betrieb,170
Dienstprogramm für Supportanfragen (dbsupport),987	Dienstprogramm für Supportanfragen (dbsupport),987
-le, Option	Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
Initialisierungsdienstprogramm (dbinit),927	Dienstprogramm zum Entladen (dbunload),1001
-ls, Option	Dienstprogramm zum Upgrade (dbupgrad),1018
Dienstprogramm für Supportanfragen (dbsupport),987	Dienstprogramm zur Logkonvertierung (dbtran),948
-m, Option	Dienstprogramm zur Serverlizenzierung (dblic),964
Broadcast Repeater-Dienstprogramm (dbns16),892	Information, Dienstprogramm (dbinfo),926
Datenbankoption,327	Initialisierungsdienstprogramm (dbinit),927
Datenbankserveroption,265	Löschen-Dienstprogramm (dberase),916
Dienstprogramm zum Entladen (dbunload),1001	Ping-Dienstprogramm (dbping),955
Dienstprogramm zum Erstellen von Zertifikaten (createcert),894	Serverauflistung, Dienstprogramm (dblocate),961
Dienstprogramm zur Logkonvertierung (dbtran),948	Sicherungsdienstprogramm (dbbackup),886
Initialisierungsdienstprogramm (dbinit),927	SQL Anywhere-Skriptausführung, Dienstprogramm (dbrunsql),959
Ping-Dienstprogramm (dbping),955	Stopp-Dienstprogramm (dbstop),984
Sprache, Dienstprogramm (dblang),946	Transaktionslog-Dienstprogramm (dblog),998
Transaktionslog-Dienstprogramm (dblog),998	Validierungs-Dienstprogramm (dbvalid),1021
-n, Option	Windows, Dienstprogramm für Dienste (dbsvc),979
Datenbanknamen angeben,328	-od, Option
Datenbankoption,328	Linux, Dienstprogramm für Dienste (dbsvc),969
Dienstprogramm zum Entladen (dbunload),1001	-oe, Option
Dienstprogramm zur Logkonvertierung (dbtran),948	dialogfreier Betrieb,170
Histogramm-Dienstprogramm (dbhist),924	Startfehler protokollieren,269
Initialisierungsdienstprogramm (dbinit),927	-on, Option
Serverauflistung, Dienstprogramm (dblocate),961	Datenbankserveroption,269
Serveroption,266	-onerror, Option
Sicherungsdienstprogramm (dbbackup),886	Interactive SQL (dbisql), Dienstprogramm,939
Transaktionslog-Dienstprogramm (dblog),998	-op, Option
-nl, Option	Broadcast Repeater-Dienstprogramm (dbns16),892
Dienstprogramm zum Entladen (dbunload),1001	Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
-no, Option	-or, Option
Dienstprogramm zum Entladen (dbunload),1001	Datenquelle, Dienstprogramm (dbdsn),906
-nogui, Option	-os, Option
Interactive SQL (dbisql), Dienstprogramm,939	

- Datenbankserveroption,270
- ot, Option
  - Datenbankserveroption,271
- p, Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserveroption,271
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - Dienstprogramm zum Entladen (dbunload),1001
  - Initialisierungsdienstprogramm (dbinit),927
  - Serverauflistung, Dienstprogramm (dblocate),961
  - Sicherungsdienstprogramm (dbbackup),886
  - Spawn-Dienstprogramm (dbspawn),983
  - Windows, Dienstprogramm für Dienste (dbsvc),976
- p1, Option
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- pc, Option
  - Datenbankserveroption,272
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Ping-Dienstprogramm (dbping),955
- pd, Option
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Initialisierung, Dienstprogramm (dbinit),927
  - Ping-Dienstprogramm (dbping),955
- pe, Option
  - Datenquelle, Dienstprogramm (dbdsn),906
- port, Option
  - Interactive SQL (dbisql), Dienstprogramm,939
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
- pr, Option
  - Linux, Dienstprogramm für Dienste (dbsvc),969
- ps, Option
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Ping-Dienstprogramm (dbping),955
- pt, Option
  - Datenbankserveroption,273
- q, Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Dateien verbergen (dbfhide),922
  - Datenquelle, Dienstprogramm (dbdsn),906
  - Dienstprogramm dbisql,915
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Informationsdienstprogramm (dbinfo),926
  - Initialisierungsdienstprogramm (dbinit),927
  - Interactive SQL (dbisql), Dienstprogramm,939
  - Linux, Dienstprogramm für Dienste (dbsvc),972
  - Löschen-Dienstprogramm (dberase),916
  - Ping-Dienstprogramm (dbping),955
  - Serverauflistung, Dienstprogramm (dblocate),961
  - Sicherung, Dienstprogramm (dbbackup),886
  - Spawn-Dienstprogramm (dbspawn),983
  - Sprache, Dienstprogramm (dblang),946
  - SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
  - Stopp-Dienstprogramm (dbstop),984
  - Transaktionslog-Dienstprogramm (dblog),998
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Windows, Dienstprogramm für Dienste (dbsvc),979
- qc, Option
  - Dienstprogramm zum Entladen (dbunload),1001
  - SQL Anywhere-Skriptaufführung, Dienstprogramm (dbrunsql),959
- qi, Option
  - Datenbankserveroption,273
  - dialogfreier Betrieb,170
  - unter Windows Mobile nicht unterstützt,426
- qn, Option
  - Datenbankserveroption,274
- qp, Option
  - Datenbankserveroption,275
- qr, Option
  - Dienstprogramm zum Entladen (dbunload),1001
- qs, Option
  - Datenbankserveroption,275
  - dialogfreier Betrieb,170
- qw, Option
  - Datenbankserveroption,276

- 
- im stillen Modus arbeiten,170
  - r, Option
    - Datenbankoption,329
    - Datenbankserveroption,277
    - Dienstprogramm für Supportanfragen (dbsupport),993
    - Dienstprogramm zum Entladen (dbunload),1001
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Sicherung, Dienstprogramm (dbbackup),886
    - Transaktionslog-Dienstprogramm (dblog),998
  - rd, Option
    - Dienstprogramm für Supportanfragen (dbsupport),993
  - rg, Option
    - Windows, Dienstprogramm für Dienste (dbsvc),976
  - rl, Option
    - Linux, Dienstprogramm für Dienste (dbsvc),969
  - ro, Option
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - rr, Option
    - Dienstprogramm für Supportanfragen (dbsupport),993
  - rs, Option
    - Linux, Dienstprogramm für Dienste (dbsvc),969
    - Windows, Dienstprogramm für Dienste (dbsvc),976
  - s, Option
    - Broadcast Repeater-Dienstprogramm (dbns16),892
    - Datenbankserveroption,278
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Initialisierungsdienstprogramm (dbinit),927
    - Linux, Dienstprogramm für Dienste (dbsvc),969
    - Ping-Dienstprogramm (dbping),955
    - Serverauflistung, Dienstprogramm (dblocate),961
    - Sicherungsdienstprogramm (dbbackup),886
    - SQL Anywhere-Skriptausführung, Dienstprogramm (dbrunsql),959
    - unter Windows Mobile nicht unterstützt,426
    - Validierungs-Dienstprogramm (dbvalid),1021
    - Windows, Dienstprogramm für Dienste (dbsvc),976
  - sa, Option
    - Dienstprogramm für Supportanfragen (dbsupport),987
  - sb, Option
    - Datenbankserveroption,278
  - sbx, Option
    - Datenbankoption,330
    - Datenbankserveroption,279
  - sc, Option
    - Dienstprogramm für Supportanfragen (dbsupport),987
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - scn, Option
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - sd, Option
    - Dienstprogramm für Supportanfragen (dbsupport),987
    - Windows, Dienstprogramm für Dienste (dbsvc),976
  - sf, Option
    - Datenbankserveroption,280
  - sk, Option
    - Datenbankserveroption,288
  - sl, Option
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - sm, Option
    - Datenbankoption,331
    - für Zugriff auf Spiegeldatenbank verwenden,1473
  - sn, Option
    - Datenbankoption,332
    - Windows, Dienstprogramm für Dienste (dbsvc),976
  - so, Option
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - sou, Option
    - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - sr, Option
    - Dienstprogramm zur Logkonvertierung (dbtran),948
  - ss, Option
    - Dienstprogramm zum Entladen (dbunload),1001

- Serverauflistung, Dienstprogramm (dblocate),961
- sst, Option
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
- st, Option
  - Ping-Dienstprogramm (dbping),955
- status, Option
  - Linux, Dienstprogramm für Dienste (dbsvc),969
- su, Option
  - Datenbankserveroption,289
  - Verbindung mit der Dienstprogramm Datenbank,147
- t, Option
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Histogramm-Dienstprogramm (dbhist),924
  - Initialisierungsdienstprogramm (dbinit),927
  - Linux-Dienst, Dienstprogramm (dbsvc),969
  - Sicherungsdienstprogramm (dbbackup),886
  - Transaktionslog-Dienstprogramm (dblog),998
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Windows, Dienstprogramm für Dienste (dbsvc),976
- tdsl, Option
  - Datenbankserveroption,290
- ti, Option
  - Datenbankserveroption,291
- tl, Option
  - Datenbankserveroption,292
- tmf, Option
  - Datenbankserveroption,293
  - unter Windows Mobile nicht unterstützt,426
- tmt, Option
  - Datenbankserveroption,294
  - unter Windows Mobile nicht unterstützt,426
- tq, Zeioption
  - Datenbankserveroption,294
- ts, Option
  - Datenbankserveroption,294
- u, Option
  - Datenbankserveroption,296
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Histogramm-Dienstprogramm (dbhist),924
  - Informationsdienstprogramm (dbinfo),926
  - Linux, Dienstprogramm für Dienste (dbsvc),968
  - Sprache, Dienstprogramm (dblang),946
  - unter Windows Mobile nicht unterstützt,426
  - Windows, Dienstprogramm für Dienste (dbsvc),974
- ua, Option
  - Datenbankserveroption,297
  - unter Windows Mobile nicht unterstützt,426
- uc, Option
  - Datenbankserveroption,297
  - unter Windows Mobile nicht unterstützt,426
- ud, Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserveroption,298
  - unter Windows Mobile nicht unterstützt,426
- uf, Option
  - Datenbankserveroption,298
  - unter Windows Mobile nicht unterstützt,426
- ufd, Option
  - Datenbankserveroption,299
- ui, Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserveroption,300
  - unter Windows Mobile nicht unterstützt,426
- ul, Option
  - Interactive SQL (dbisql), Dienstprogramm,939
- um, Option
  - Datenbankserveroption,300
- ut, Option
  - Datenbankserveroption,301
  - unter Windows Mobile nicht unterstützt,426
- ux, Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserveroption,302
  - unter Windows Mobile nicht unterstützt,426
- v, Option
  - Datenbankserveroption,303
  - Datenquelle, Dienstprogramm (dbdsn),906
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - Serverauflistung, Dienstprogramm (dblocate),961

- 
- SQL Anywhere-Skriptaufführung,  
Dienstprogramm (dbrunsql),959
  - version  
Interactive SQL (dbisql), Dienstprogramm,939
  - vss, Option  
Datenbankserveroption,303
  - w, Option  
Dateien verbergen (dbfhide),922  
Datenquelle, Dienstprogramm (dbdsn),905  
Linux, Dienstprogramm für Dienste (dbsvc),968  
Windows, Dienstprogramm für Dienste (dbsvc),974
  - wa, Option  
Sicherungsdienstprogramm (dbbackup),886
  - wb, Option  
Sicherungsdienstprogramm (dbbackup),886
  - wc, Option  
Datenbankoption,334  
Datenbankserveroption,304
  - wm, Option  
Dateien verbergen (dbfhide),922
  - x, Option  
Broadcast Repeater-Dienstprogramm (dbns16),892  
Datenbankserveroption,305  
Dienstprogramm dbisqlc,915  
Dienstprogramm zum Erstellen von Zertifikaten (createcert),894  
Dienstprogramm zur Logkonvertierung (dbtran),948  
Interactive SQL (dbisql), Dienstprogramm,939  
Linux, Dienstprogramm für Dienste (dbsvc),968  
Sicherungsdienstprogramm (dbbackup),886  
Stopp-Dienstprogramm (dbstop),984  
Transaktionslog-Dienstprogramm (dblog),998  
Windows, Dienstprogramm für Dienste (dbsvc),974
  - xa, Option  
Datenbankserveroption (dbsrv16),306
  - xd, Option  
Datenbankserveroption,307
  - xf, Option  
Datenbankserveroption (dbsrv16),308
  - xi, Option  
Dienstprogramm zum Entladen (dbunload),1001
  - xm, Option  
Datenbankserveroption,309
  - xo, Option  
Sicherungsdienstprogramm (dbbackup),886
  - xp, Option  
Datenbankoption,335  
unter Windows Mobile nicht unterstützt,426
  - xs, Option  
Datenbankserveroption,310  
verwenden mit Cloud-Servern,310
  - xx, Option  
Dienstprogramm zum Entladen (dbunload),1001
  - y, Option  
Datenquelle, Dienstprogramm (dbdsn),906  
Dienstprogramm zum Entladen (dbunload),1001  
Dienstprogramm zur Logkonvertierung (dbtran),948  
Linux, Dienstprogramm für Dienste (dbsvc),972  
Löschen-Dienstprogramm (dberase),916  
Sicherungsdienstprogramm (dbbackup),886  
Stopp-Dienstprogramm (dbstop),984  
Windows, Dienstprogramm für Dienste (dbsvc),979
  - z, Option  
Broadcast Repeater-Dienstprogramm (dbns16),892  
Datenbankserveroption,312  
Dienstprogramm zur Logkonvertierung (dbtran),948  
Fehlersuche bei Problemen mit der  
Netzwerkkommunikation,1110  
Initialisierungsdienstprogramm (dbinit),927  
Ping-Dienstprogramm (dbping),955  
Transaktionslog-Dienstprogramm (dblog),998
  - ze, Option  
Datenbankserveroption,312  
Initialisierungsdienstprogramm (dbinit),927  
unter Windows Mobile nicht unterstützt,426
  - zl, Option  
Datenbankserveroption,313
  - zn, Option  
Datenbankserveroption,314  
Initialisierung, Dienstprogramm (dbinit),927
  - zo, Option  
Datenbankserveroption,315
  - zoc, Option  
Datenbankserveroption,315
  - zp, Option  
Datenbankserveroption,316
  - zr, Option  
Datenbankserveroption,317
  - zs, Option  
Datenbankserveroption,319

- zt, Option
  - Datenbankserveroption,319
- .dbr
  - Info,1016
- .logr
  - Info,1016
- .NET Compact Framework
  - mit SQL Anywhere für Windows Mobile verwenden,431
- .odbc.ini
  - Datenquellen erstellen,906
  - Datenquellen unter Mac OS X erstellen,45
  - im Verbindungsparameter DSN angeben,356
  - Info,49
  - Kennwörter speichern,378
  - verschlüsselt Kennwörter speichern,358
- .pid
  - Linux-Dienste,972
- 1254TRK-Kollation
  - Unterschiede zu 1254TRKALT,534
- 1254TRKALT-Kollation
  - verwenden ,534
- 32-Bit
  - Umgebungsvariable PATH,471
- 64-Bit
  - Umgebungsvariable PATH,471
- 7-Bit-Zeichen
  - Info,499
- @data, Option
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - unter Windows Mobile nicht unterstützt,426
- @data-Option
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserveroption ,214
  - Datenquelle, Dienstprogramm (dbdsn),905
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Histogramm-Dienstprogramm (dbhist),924
  - Info,882
  - Informationsdienstprogramm (dbinfo),926
  - Initialisierungsdienstprogramm (dbinit),927

- Interactive SQL (dbisql), Dienstprogramm,939
- Löschen-Dienstprogramm (dberase),916
- Ping-Dienstprogramm (dbping),953
- Serverauflistung, Dienstprogramm (dblocate),961
- Serverstopp-Dienstprogramm (dbstop),984
- Sicherungsdienstprogramm (dbbackup),886
- Spawn-Dienstprogramm (dbspawn),983
- SQL Anywhere-Konsolendienstprogramm (dbconsole),982
- Transaktionslog-Dienstprogramm (dblog),998
- Validierungs-Dienstprogramm (dbvalid),1021
- Windows, Dienstprogramm für Dienste (dbsvc),974

## A

- Abfolgepläne
  - Assistent Zeitplan erstellen,1090
- Abfolgeplanung
  - Definition,1087
  - Ereignisse,1087
  - Info,1089
  - Interna,1097
  - Server herunterfahren,294
  - Sicherungen,1063
- Abfrage- Editor
  - Info,835
- Abfrage-Editor
  - Abfragen erstellen,837
  - Ausdruck-Editor,838
  - Transact SQL nicht unterstützt,837
  - Vereinigungen nicht unterstützt,837
- Abfrageinterne Parallelität
  - Auswirkungen von Option -gna,245
  - Auswirkungen von Option -gnh,246
  - Auswirkungen von Option -gnl,247
  - max\_query\_tasks-Option,633
- Abfragen
  - Interactive SQL,819
  - lang laufende, mit -zp-Serveroption neueste Pläne erfassen,316
  - mit dem Abfrage-Editor erstellen,837
  - Optimierer, Bypass,649
- Abfrageoptimierung
  - aktuellsten Plan aufzeichnen,316
  - Optimierer, Bypass,649
- Abhängigkeiten
  - Dienstabhängigkeiten verwalten,191

- 
- Dienste,191
    - einstellen,976
    - für Linux-Dienste definieren,969
  - Ableitung
    - Login-Richtlinienoptionen,536
  - Abmelden
    - Server weiter ausführen,298
  - Abrufen
    - Anweisungen in Interactive SQL,822
  - AccentSensitive, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - AccentSensitive-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1248
  - ActiveReq-Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - ActiveReq-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1234
  - ActiveSync
    - erforderliche Version,430
  - ActiveSync-Provider-Installationsdienstprogramm (mlasinst)
    - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
  - Admin-Benutzer
    - Monitor, Info,1176
  - Administrationstools
    - Hardwareanforderungen für Mac OS X,5
    - Interactive SQL,814
    - Sybase Central,795
    - unter Windows Mobile nicht unterstützte Funktionen,423
  - Administratoren
    - Monitor-Benutzer,1175
  - ADO.NET Sample
    - verwenden,461
  - AES, Verschlüsselungsalgorithmus
    - Info,1425
    - Initialisierung, Dienstprogramm (dbinit),927
  - AES-Verschlüsselung, Algorithmus
    - Entladen, Dienstprogramm (dbunload),1001
  - AES256, Verschlüsselungsalgorithmus
    - Initialisierungsdienstprogramm (dbinit),927
  - AES256-Verschlüsselung, Algorithmus
    - Dienstprogramm zum Entladen (dbunload),1001
  - AES256\_FIPS, Verschlüsselungsalgorithmus
    - fips, Serveroption,237
    - Initialisierungsdienstprogramm (dbinit),927
  - AES256\_FIPS-Verschlüsselung, Algorithmus
    - Dienstprogramm zum Entladen (dbunload),1001
  - AES\_FIPS, Verschlüsselungsalgorithmus
    - fips, Serveroption,237
    - Initialisierungsdienstprogramm (dbinit),927
  - AES\_FIPS-Verschlüsselung, Algorithmus
    - Dienstprogramm zum Entladen (dbunload),1001
  - Agent für Vorgänge mit erweiterten Berechtigungen
    - Vista,202
    - Windows 7,202
    - Windows Server 2008,202
  - Agent, Tabelle
    - SQL Anywhere MIB-Datenbank,1230
  - Agenten
    - Info,1217
  - AIX
    - IPv6-Unterstützung,106
    - LIBPATH-Umgebungsvariable,470
    - mit einem LDAP-Server,109
  - Aktive Anforderungen
    - Info,175
  - Aktive Aufgaben
    - Info,175
  - Aktivieren
    - Tabellenverschlüsselung (dbinit),1440
    - Tabellenverschlüsselung (SQL),1438
  - Aktualisieren
    - automatisch,189
    - Inhalt des Hauptfensters,795
    - Intervall einstellen,189
    - Sybase Central,189
    - Werte in Interactive SQL,831
  - Aktualisierungen
    - ansi\_permissions-Option,577
    - ansi\_update\_constraints-Option,579
    - SQL Anywhere-Aktualisierungen suchen,879
    - SQL/2008-Verhalten,579
    - Transact-SQL-Privilegien,577
  - Akzent-Berücksichtigung
    - Datenbanken,927
    - französische Regeln verwenden,927
  - Alarm-Schwellenwerte
    - Monitor, angeben,1184

- Alarmer
  - Monitor, 1181
- Alias, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- Alias-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248
- ALL-Berechtigung (nicht mehr empfohlen)
  - konvertiert in SYS\_AUTH\_RESOURCE\_ROLE-Kompatibilitätsrolle, 1275
- ALL-Privileg
  - Info, 1305
- Allgemeine Tabellenausdrücke
  - max\_recursive\_iterations-Option, 634
- Allgemeiner Name
  - certificate\_name-Protokolloption, 393
- allow\_nulls\_by\_default, Option
  - ASE-Kompatibilität, 559
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
  - Transact-SQL-Kompatibilität, 560
- allow\_nulls\_by\_default-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- allow\_nulls\_by\_default-Option
  - Beschreibung, 572
  - Sybase Open Client, 1571
- allow\_read\_client\_file, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- allow\_read\_client\_file-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- allow\_read\_client\_file-Option
  - Beschreibung, 573
- allow\_snapshot\_isolation-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- allow\_snapshot\_isolation-Option
  - Beschreibung, 574
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- allow\_write\_client\_file, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- allow\_write\_client\_file-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- allow\_write\_client\_file-Option
  - Beschreibung, 575
- Als Dienst anmelden, Berechtigung
  - Linux, Dienstprogramm für Dienste (dbsvc), 969
  - Windows, Dienstprogramm für Dienste (dbsvc), 976
- Als ODBC-Datenquelle speichern
  - Info, 39
- ALTER ANY INDEX-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY MATERIALIZED VIEW-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY OBJECT OWNER-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY OBJECT-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY PROCEDURE-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY SEQUENCE-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY TABLE-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY TEXT CONFIGURATION-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY TRIGGER-Systemprivileg
  - Beschreibung, 1309
- ALTER ANY VIEW-Systemprivileg
  - Beschreibung, 1309
- ALTER DATABASE, Anweisung
  - Failover in einem Spiegelungssystem erzwingen, 1488
  - Primärserver herunterfahren, 1500
- ALTER DATABASE-Systemprivileg
  - Beschreibung, 1309
- ALTER DATATYPE-Systemprivileg
  - Beschreibung, 1309
- ALTER USER-Anweisung
  - Kennwörter ändern, 1369
- ALTER-Privileg
  - Info, 1305
- AlternateMirrorServerName, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- AlternateMirrorServerName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248
- AlternateServerName, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- AlternateServerName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248

---

Alternative Servernamen  
  Option -sn,332

Ändern der Einstellungen für die Logdatei, Assistent  
  Transaktionslog-Spiegel für vorhandene  
  Datenbanken starten,140

Anforderungen  
  Hardware,794  
  request\_timeout-Option,664  
  SQL Anywhere für Windows Mobile,430  
  Threads in SQL Anywhere,171  
  Veritas Cluster Server-Agenten,1527

Anforderungslog  
  Anzahl der Kopien,314  
  Größe begrenzen,319  
  max\_client\_statements\_cached-Einstellung,631  
  verwenden,315

Anforderungsprotokollierung  
  Anzahl der Anforderungslog-Kopien,314  
  Datenbankserveroption,317  
  Größe der Logdatei begrenzen,319  
  max\_client\_statements\_cached-Einstellung,631  
  Protokolldaten in einer Datei speichern,315

Anführungszeichen  
  in Verbindungszeichenfolgen verwenden,31

Anpassen von Kollationen  
  beschränkte Unterstützung für Windows  
  Mobile,439  
  ICU,517

ANSI  
  cooperative\_commits-Option,596  
  Cursor,576  
  Datenbankoptionen für Kompatibilität,559  
  delayed\_commits-Option,606  
  Konformität,671  
  Privilegien aktualisieren,577  
  Privilegien löschen,577  
  Verhalten der Variablen,575

ANSI, Codepages  
  Info,500

ansi\_blanks, Option  
  ASE-Kompatibilität,559  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

ansi\_blanks-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansi\_blanks-Option  
  Beschreibung,575

Sybase Open Client,1571

ansi\_close\_cursors\_on\_rollback, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

ansi\_close\_cursors\_on\_rollback-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansi\_close\_cursors\_on\_rollback-Option  
  Beschreibung,576

ansi\_permissions, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

ansi\_permissions-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansi\_permissions-Option  
  Beschreibung,577

ansi\_substring, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253

ansi\_substring-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansi\_substring-Option  
  ASE-Kompatibilität,559  
  Beschreibung,578

ansi\_update\_constraints, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

ansi\_update\_constraints-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansi\_update\_constraints-Option  
  Beschreibung,579

Ansichten  
  anzeigen,1348  
  Datenbankdokumentation erstellen,814  
  Privilegien erteilen,1305  
  Sicherheit,1403  
  Sicherheitsfunktionen,1402

ansinull, Option  
  ASE-Kompatibilität,559  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

ansinull-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

ansinull-Option  
  Beschreibung,580

- Sybase Open Client,1571
- Anweisungen
  - Caching für Clients,629
  - Datenbankoptionen,565
  - Dienstprogrammdatenbank,145
  - Einschränkungen,791
  - in Interactive bearbeiten,822
  - in Interactive erneut aufrufen,822
  - in Interactive SQL abbrechen,828
  - in Interactive SQL stoppen,828
  - in Interactive SQL unterbrechen,828
  - nicht unterstützte Anweisungen unter Windows Mobile,425
  - protokollieren,164
- Anweisungen ausführen
  - Authentifizierungsanweisung,198
- Anwendungen
  - SQL Anywhere OEM Editions,194
- Anwendungen authentifizieren
  - Info,197
- Anwendungen mit Threadverarbeitung
  - dbping\_r für Unix,955
- Anwendungsprofilerstellung
  - Einschränkungen unter Windows Mobile,423
- Anwendungsprofilerstellung, Modus
  - Info,808
- Anzeigen
  - TLS-Zertifikate,903
- Anzeigen von Diagnosedaten
  - dbmanageetd, Dienstprogramm,1105
- APIs
  - aus SQL Anywhere verbinden,50
- APP, Verbindungsparameter
  - Beschreibung,338
- AppInfo, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- AppInfo, Verbindungsparameter
  - Beschreibung,338
- ApproximateCPUTime, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ApproximateCPUTime-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237,1248
- Arbiterserver
  - Datenbanknamen liefern,306
  - Datenbankspiegelung, Übersicht,1467
  - Kopieknotten verwenden,1485
  - löschen,1490
  - Rolle in Datenbankspiegelungssystemen,1468
  - stoppen,1490
  - Verbindungszeichenfolgen liefern,306
- ArbiterState, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ArbiterState-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Archivsicherungen
  - BACKUP-Anweisung,1038
  - Datenbanken mit Interactive SQL wiederherstellen,1051
  - Datenbanken mit Sybase Central wiederherstellen,1050
  - Definition,1033
  - Info,1034
  - Sybase Central,1041
- ASCII
  - ServerName (Server)-Verbindungsparameter, Einschränkung,383
  - Zeichensatz,499
- ASE
  - alternative Zeichensatzlabels,501
- Assertierungen
  - uf, Serveroption,298
  - ufd, Serveroption,299
- Assistent zum Ändern der Einstellungen für die Logdatei
  - unter Windows Mobile nicht unterstützt,428
- Assistent zum Entladen einer Datenbank
  - unter Windows Mobile nicht unterstützt,428
- Assistent zum Erstellen der Datenbankdokumentation
  - Info,814
- Assistent zum Erstellen einer Datenbank
  - Liste der Kollationssequenzen,927
  - Windows Mobile,442
- Assistent zum Erstellen einer Login-Richtlinie
  - verwenden,540
- Assistent zum Erstellen von Benutzern
  - verwenden,1341
- Assistent zum Erstellen von Wartungsplänen
  - eingeschränkte Unterstützung unter Windows Mobile,428
- Assistent zum Löschen einer Datenbank
  - unter Windows Mobile nicht unterstützt,428
- Assistent zum Migrieren einer Datenbank

- 
- unter Windows Mobile nicht unterstützt,428
  - Assistent zum Sichern einer Datenbank
    - unter Windows Mobile nicht unterstützt,428
  - Assistent zum Übersetzen einer Logdatei
    - unter Windows Mobile nicht unterstützt,428
  - Assistent zum Upgrade einer Datenbank
    - unter Windows Mobile nicht unterstützt,428
  - Assistent zum Wiederherstellen einer Datenbank
    - unter Windows Mobile nicht unterstützt,428
  - Assistenten
    - unter Windows Mobile nicht unterstützte Sybase Central-Assistenten,428
  - ASTART, Verbindungsparameter
    - Beschreibung,341
  - ASTOP, Verbindungsparameter
    - Beschreibung,342
  - Asynchron, Modus
    - Datenbankspiegelung,1478
  - Asynchron-Ganzseiten-Modus
    - Datenbankspiegelung,1478
    - Fehlerbehandlung,1499
  - Asynchrone I/O-Vorgänge
    - Verwendung unter Linux deaktivieren,297
  - Asynchroner Modus
    - Fehlerbehandlung,1499
  - AUDITING
    - steuern,582
  - Auditing
    - aktivieren,1418,1419
    - Audit-Daten abrufen,1420
    - Beispiel,1422
    - conn\_auditing-Option,592
    - Datenbanken unter Windows Mobile,1442
    - deaktivieren,1418,1419
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - Dienstprogramm zur Logkonvertierung (dbtran), Vorgänge,1418
    - Info,1416
    - Kommentare,1417
    - nicht festgeschriebene Vorgänge mit der Befehlszeile wiederherstellen,1048
    - nicht festgeschriebene Vorgänge mit Sybase Central wiederherstellen,1048
    - Sicherheitsfunktionen,1402
    - Sybase Central,1418,1419
    - Transaktionslog-Dienstprogramm (dblog), Vorgänge,1418
    - Verbindungen,1417
  - auditing, Option
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - auditing- Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - auditing-Option
    - Beschreibung,582
  - auditing\_options, Option
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - auditing\_options-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - auditing\_options-Option
    - Beschreibung,583
  - Auditingmaßnahmen außerhalb des Datenbankservers
    - Info,1418
  - AuditingTypes, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - AuditingTypes-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
  - Auffüllen mit Leerzeichen
    - Info,927
  - Auffüllen mit Nullen
    - mit date\_format-Option steuern,600
    - mit sr\_time\_format-Option steuern,675
    - mit sr\_timestamp\_format-Option steuern,677
    - mit sr\_timestamp\_with\_time\_zone\_format-Option steuern,679
    - mit time\_format-Option steuern,691
    - mit timestamp\_format-Option steuern,694
    - mit timestamp\_with\_time\_zone\_format-Option steuern,696
  - Aufgaben
    - Threads in SQL Anywhere,171
  - Aufgaben mit Abfolgeplanung und Ereignissen automatisieren
    - Info,1087
  - Aufgaben steuern, die Benutzer ausführen können
    - Info,1409
  - Aufnahme
    - Wiederherstellungszeit für die Wiederaufnahme,294
  - Aufrufer
    - Systemprozeduren zum Ausführen als Aufrufer migrieren,1401
  - Ausdruck-Editor
-

- Abfrage-Editor,838
- Ausführbare Dateien
  - signiert für Vista,203
  - signiert für Windows 7,203
  - signiert für Windows Server 2008,203
- Ausführen
  - Anweisungen in Interactive SQL,819
  - Befehlsdateien,821
  - Event-Handler,1097
  - mehrere Anweisungen in Interactive SQL,819
  - SQL-Anweisungen,819
- Ausführlicher Modus
  - Dienstprogramm zum Entladen (dbunload),1001
- Ausführungs-Threads
  - gn dbsrv16-Serveroption,244
  - gna dbsrv16-Serveroption,245
  - gnh dbsrv16-Serveroption,246
  - gnl dbsrv16, Serveroption,247
- Ausführungspläne
  - Darstellung anpassen,840
- Ausführungsthreads
  - Info,171
- Ausführungszeit
  - isql\_command\_timing-Option,859
- Ausnahmebedingungsberichte
  - Monitor,1132
- authdn, Parameter
  - LDAP,110
- authenticate.sql
  - Upgrade authentifizierter Datenbanken,200
- Authenticated, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- Authenticated-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Authentifizierte Anwendungen
  - Authentifizierungssignaturen,195
  - connection\_authentication-Option,593
  - database\_authentication-Option,597
  - Datenbankauthentifizierung,195
  - entwickeln,194
  - Info,194
  - konfigurieren,197
  - Programmierschnittstelle, Beispiele,198
- Authentifizierte Datenbanken
  - database\_authentication-Option,597
  - Upgrade,200
- Authentifizierte Verbindungen
  - connection\_authentication-Option,593
- Authentifizierung
  - Datenbanken,597
  - Verbindungen,593
- Authentifizierungssignaturen
  - Info,195
- Authentifizierungssignaturen beziehen
  - Info,195
- AuthType-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- auto\_add\_fan\_out-Option
  - verwenden,1553
- auto\_commit, Option
  - Einstellungen von Interactive SQL,851
- auto\_commit-Option
  - Info,853
- auto\_commit\_on\_create\_local\_temp\_index-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- auto\_commit\_on\_create\_local\_temp\_index-Option
  - Beschreibung,583
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- auto\_refetch, Option
  - Einstellungen von Interactive SQL,851
- auto\_refetch-Option
  - Info,853
- automatic\_timestamp, Option
  - Transact-SQL-Kompatibilität,560
- Automation
  - Verwaltungsaufgaben,1087
- Automatische Wiederherstellung
  - Info,1027
- AutoMultiProgrammingLevel-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- AutoMultiProgrammingLevelStatistics-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- AutoStart, Verbindungsparameter
  - Beschreibung,341
- AutoStop, Verbindungsparameter
  - Beschreibung,342
- AvailIO, Eigenschaft
  - Servereigenschaft, Beschreibung,745

---

AvailIO-Statistik

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234

## B

background\_priority, Option

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253

background\_priority-Eigenschaft

Verbindungseigenschaft, Beschreibung,711

background\_priority-Option

Beschreibung [nicht mehr empfohlen],584

BACKUP DATABASE-Systemprivileg

Beschreibung,1309

erforderlich für Online-Sicherungen,1027

BACKUP-Anweisung

Archivsicherung erstellen,1038

Einschränkungen unter Windows Mobile,425

Sicherungskopie erstellen,1039

Transaktionslogs kürzen,1071

BACKUP-Berechtigung (nicht mehr empfohlen)

konvertiert in SYS\_AUTH\_BACKUP\_ROLE-

Kompatibilitätsrolle,1275

backup.syb

Speicherort bestimmen,474

BackupEnd, Systemereignis

Beschreibung,1091

Bandlaufwerke

Datenbanken mit SQL sichern,1038

Datenbanken mit Sybase Central sichern,1041

base\_tables\_in\_rlv\_store-Option

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253

basedn, Parameter

LDAP,110

Batchdateien

Datenbankserver mit dbspawn starten,213

Server starten,983

BCAST, Protokolloption

Beschreibung,390

IPv6-Adressen verwenden,107

Bearbeiten

Ergebnismengen in Interactive SQL,830

Bedingte syntaktische Analyse

Konfigurationsdateien,883

Beendigungscodes

Datenquellendienstprogramm (dbdsn),909

Dienstprogramm für den Serverstart im  
Hintergrund (dbspawn),984

Dienstprogramm zum Entladen (dbunload),1014

Dienstprogramm zum Upgrade (dbupgrad),1020

Dienstprogramm zur Logkonvertierung  
(dbtran),953

Dienstprogramm zur Serverlizenzierung  
(dblic),967

Histogramm, Dienstprogramm (dbhist),925

Information, Dienstprogramm (dbinfo),927

Initialisierungsdienstprogramm (dbinit),938

Interactive SQL (dbisql), Dienstprogramm,944

Löschen (dberase), Dienstprogramm,918

Performancestatistik-Dienstprogramm  
(dbstats),954

Ping-Dienstprogramm (dbping),958

Serverauflistung, Dienstprogramm (dblocate),963

Serverstopp-Dienstprogramm (dbstop),986

Sicherungen [dbbackup], Dienstprogramm,891

Sprache, Dienstprogramm (dblang),947

Transaktionslog-Dienstprogramm (dblog),1000

Validierung, Dienstprogramm [dbvalid],1024

Windows, Dienstprogramm für Dienste  
(dbsvc),980

Befehlsbegrenzer

Interactive SQL (dbisql), Dienstprogramm,939

Befehlsdateien

in Interactive SQL öffnen,817

Befehlsparameter, Dateien

Info,882

Befehlstrennzeichen

Dienstprogramm dbisqlc,915

Befehlszeile

Datenbankserver (Datenbank),203

Datenbankserver starten,212

Dienstprogramm dbconsole starten,877

Groß-/Kleinschreibung berücksichtigen,212

in Konfigurationsdatei,214

Interactive SQL starten,815

Konfigurationsdateien verwenden,882

Befehlszeilen-Dienstprogramme

Broadcast Repeater-Syntax (dbns16),891

createkey, Syntax,945

Datenquelle (dbdsn), Syntax,905

dbisqlc-Syntax,915

Entladen (dbunload), Syntax,1000

Erstellen von Zertifikaten (createcert), Syntax,894

Histogramm (dbhist), Syntax,923

- Information (dbinfo), Syntax,925
- Initialisierung (dbinit), Syntax,927
- Interactive SQL (dbisql), Syntax,939
- Linux-Dienst (dbsvc), Syntax,968
- Logkonvertierung (dbtran), Syntax,948
- Löschen (dberase), Syntax,916
- Performancestatistiken (dbstats), Syntax,953
- Ping (dbping), Syntax,955
- Serverauflistung (dblocate), Syntax,960
- Serverlizenzierung (dblic), Syntax,964
- Serverstart im Hintergrund (dbspawn), Syntax,983
- Serverstopp (dbstop), Syntax,984
- Sicherung (dbbackup), Syntax,886
- Sprachauswahl (dblang), Syntax,946
- SQL Anywhere-Konsole (dbconsole), Syntax,981
- SQL Anywhere-Skriptausführung (dbrunsql), Syntax,959
- Supportanfragen (dbsupport), Syntax,987
- Transaktionslog (dblog), Syntax,998
- Upgrade (dbupgrad), Syntax,1017
- Validierung (dbvalid), Syntax,1020
- Verbergen von Dateien (dbfhide), Syntax,922
- viewcert-Syntax,903
- Windows-Dienst (dbsvc), Syntax,974
- Begrenzer
  - Anweisungen,854
- Beispielanwendungen
  - ADO.NET Sample,461
  - ESQL Sample,463
  - ODBC Sample,464
  - Windows Mobile,432,461
- Beispieldatenbank
  - Herstellen einer Verbindung unter Mac OS X,9
  - Herstellen einer Verbindung unter Unix,7
  - praktische Einführung,1
  - verbinden (Dienstprogramm dbisql),7
  - Verbindung herstellen (Sybase Central),5
  - zwei Versionen unter Windows Mobile,432
- Beispiele
  - als Source nehmen,468
  - Speicherort,482
  - über das Windows-Startmenü aufrufen,483
  - Umgebungsvariable,478
- Beispiele, Verzeichnis
  - Info,483
- Beispielverzeichnis
  - Umgebungsvariable,478
- bell, Option
  - Einstellungen von Interactive SQL,851
- bell-Option
  - Info,854
- Benachrichtigungen
  - SNMP,1227
- Benannte Kollationen
  - Datenbanken erstellen,522
- Benennen
  - Tabellen und Spalten,122
  - Verbindungen,349
- Benutzer
  - automatisches Entsperrn von Benutzerkonten,544
  - Datenbankoptionen ändern,570
  - in benutzererweiterte Rollen konvertieren (SQL),1290
  - in benutzererweiterte Rollen konvertieren (Sybase Central),1289
  - in Sybase Central erstellen,1341
  - integrierte Login-Berechtigung erteilen,52
  - integrierte Logins erstellen (SQL),55
  - integrierte Logins erstellen (Sybase Central),54
  - integrierte Logins löschen (SQL),57
  - integrierte Logins löschen (Sybase Central),56
  - Kennwörter in Sybase Central ändern,1367
  - Kennwörter mit SQL ändern,1369
  - Kerberos-Logins erstellen,70
  - Kerberos-Logins löschen,71
  - Login-Richtlinien,535
  - Login-Richtlinien zuordnen,541
  - löschen,1345
  - mit SQL erstellen,1342
  - Monitor,1175
  - Privilegien,1340
  - Privilegien auf Objektebene entziehen,1339
  - Privilegien auf Objektebene erteilen (SQL),1335
  - Privilegien auf Objektebene in Sybase Central erteilen,1333
  - Privilegkonflikte,1331
  - Rollen in Sybase Central erteilen,1298
  - Rollen und Privilegien anzeigen (SQL),1344
  - Rollen und Privilegien anzeigen (Sybase Central),1343
  - Standardwerte,1340
  - Systemprivilegien erteilen (SQL),1332
  - Systemprivilegien in Sybase Central erteilen,1331
  - temporären Speicher limitieren,636
  - Verbindung mithilfe von Sybase Central trennen,100

- 
- verbundene Benutzer verwalten,99
  - verwalten,1340
  - Benutzer-ID
    - PUBLIC-Optionen,565
  - Benutzer-IDs
    - Guest,61
    - Info,1271,1340
    - Login-Richtlinien,535
    - maximale Länge,791
    - Sicherheitsfunktionen,1402
    - Sicherheitstipps,1406
    - verwalten,1271,1340
  - Benutzer-Trace-Ereignisse
    - erstellen,1102
    - Info,1101
  - Benutzerauthentifizierung
    - al, Datenbankoption,323
    - al, Serveroption,216
    - CloudAdmin,623
    - Fehler bei der Authentifizierung bei der Datenbank,323
    - Fehler bei der Authentifizierung beim Server,216
    - integriert,623
    - Kerberos,623
    - LDAPUA,623
    - login\_mode-Option,623
    - Standard,623
  - Benutzerdefinierte Eigenschaften
    - Info,789
    - Verwendungszweck,789
  - Benutzerdefinierte Rollen
    - Info,1285
  - Benutzerdefinierte Schlüssel für gesicherte Funktionen
    - Info,1414
  - Benutzerdefinierte Selektivitätsschätzungen
    - user\_estimates-Option,702
  - Benutzererweiterte Rollen
    - Benutzer in benutzererweiterte Rollen konvertieren (SQL),1290
    - Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central),1289
    - benutzererweiterte Rollen in Benutzer zurückkonvertieren (Sybase Central),1291
    - Info,1287
    - praktische Einführung (SQL),1378
    - praktische Einführung, Sybase Central,1371
    - Vererbung an Berechtigungsempfänger,1287
  - Benutzerkontensteuerung
    - SQL Anywhere unter Vista ausführen,202
    - SQL Anywhere unter Windows 2008 ausführen,202
    - SQL Anywhere unter Windows 7 ausführen,202
  - Benutzernamen
    - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Benutzerschätzungen
    - außer Kraft setzen,702
  - Berechnete Spalten
    - Datenbanken entladen,1014
    - in Interactive SQL aktualisieren,832
    - in Interactive SQL neu berechnen,832
    - in Interactive SQL zu neuen Zeilen hinzufügen,832
    - neu berechnen beim Datenbankentladen,1001
  - Berechtigungen
    - entziehen, SQL-Syntax (nicht mehr empfohlen),1397
    - erteilen, SQL-Syntax (nicht mehr empfohlen),1393
    - Kompatibilitätsrollen zuordnen,1386
    - Konflikte,1331
    - temporäre Dateien,476
  - Berücksichtigung
    - Akzent,523
    - Groß-/Kleinschreibung,523
    - Satzzeichen,523
  - Betreiben von Datenbankservern
    - Überblick,150
  - Bevorzugte Server
    - für Datenbankspiegelung festlegen,1484
  - Bezeichner
    - Groß-/Kleinschreibung berücksichtigen,505
    - internationale Aspekte,505
  - Bibliotheken
    - DYLD\_LIBRARY\_PATH-Umgebungsvariable [Mac OS X],469
    - für Dienstprogramm dbping laden,955
    - für ICU unter Windows Mobile erforderlich,430
    - Kerberos GSS-API-Bibliotheksdateien,64
    - Kerberos-Authentifizierung,64
    - LD\_LIBRARY\_PATH-Umgebungsvariable [Linux und Solaris],469
    - LIBPATH-Umgebungsvariable [IBM AIX],470
    - SHLIB\_PATH-Umgebungsvariable [HP-UX],477
    - Speicherort der Schnittstellenbibliothek ermitteln,80
  - Bilder

- in Interactive SQL anzeigen,841
- Binärdatentypen
  - maximale Größe,791
- Blackouts
  - Monitor,1145
- BlankPadding, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- BlankPadding-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- BLISTENER, Protokolloption
  - Beschreibung,391
- blob\_threshold-Option
  - SQL Remote, Beschreibung,585
  - SQL Remote-Replikationsoption,563
- BLOBs
  - gemeinsam nutzen,123
  - in der Datenbank speichern,123
  - Info,123
- BLOBs in der Datenbank speichern
  - Info,123
- BlockedOn-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- blocking
  - blocking\_others\_timeout-Option,586
- blocking, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- blocking-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- blocking-Option
  - Beschreibung,585
- blocking\_others\_timeout-Eigenschaft
  - Verbindungseigenschaft Beschreibung,711
- blocking\_others\_timeout-Option
  - Beschreibung,586
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- blocking\_timeout-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- blocking\_timeout-Option
  - Beschreibung,587
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- Boolesche Werte
  - Protokolloptionen,388
  - Verbindungsparameter,338
- Broadcast Repeater-Dienstprogramm (dbns16)
  - Syntax,891
  - verwenden,85
- Broadcast, Protokolloption
  - Beschreibung,390
  - IPv6-Adressen verwenden,107
- BroadcastListener, Protokolloption
  - Beschreibung,391
- Build-Nummer
  - SQL Anywhere,303
- BuildChange, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- BuildClient, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- BuildProduction, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- BuildReproducible, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- BytesReceived, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- BytesReceived-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- BytesReceived-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- BytesReceivedUncomp, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- BytesReceivedUncomp-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- BytesReceivedUncomp-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- BytesSent, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- BytesSent-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- BytesSent-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- BytesSentUnc-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- BytesSentUncomp, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- BytesSentUncomp-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244

---

## C

### Cache

- Datenbankserveroptionen,167
- Größenoption,167
- max\_plans\_cached-Option,632
- maximale Größe,791
- Mindestgröße,224
- Cache-Vorwärmung
  - Cache mit Seiten erneut laden,226
  - Datenbankseiten sammeln,220
  - Servermeldungen,227
- CacheAllocated, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CacheAllocated-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- CacheFile, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CacheFile-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- CacheFileDirty, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CacheFileDirty-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- CacheFree, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CacheFree-Statistik
  - SQL Anywhere SNMP Extension Agent OID,1234
- Cachegröße
  - anfängliche,218
  - einstellen,217
  - Höchstwert festlegen,221
  - im Meldungsfenster des Datenbankservers anzeigen,227
  - Limit,791
  - Mindestwert festlegen,224
  - Minimum,224
  - Standard,218
  - statisch,219
  - verschlüsselte Datenbanken,1433
- CacheHits, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Serveereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- CacheHits-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- CachePanics, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CachePanics-Statistik
  - SQL Anywhere SNMP Extension Agent OID,1234
- CachePinned, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- CachePinned-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- Cachepuffer
  - Performance,217
- CacheRead, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Serveereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- CacheRead-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- CacheReadIndInt, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- CacheReadIndInt-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CacheReadIndLeaf, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- CacheReadIndLeaf-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CacheReadTable, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- CacheReadTable-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CacheReadWorkTable, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- CacheReadWorkTable-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CacheReplacements, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,745
- CacheReplacements-Statistik

- SQL Anywhere SNMP-Erweiterungsagent,
  - OID,1234
- CacheScavenges, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CacheScavenges-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1234
- CacheScavengeVisited, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CacheScavengeVisited-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1234
- CacheSizingStatistics, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CacheSizingStatistics-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1237
- Caching
  - Servernamen,94
- Callback-Funktionen
  - Datenbankserveroption,235
- Capabilities, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- Capabilities-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1248
- CarverHeapPages, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CarverHeapPages-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- CarverHeapPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1234,1244
- CaseSensitive, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CaseSensitive-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1248
- CatalogCollation-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1248
- CBSIZE, Verbindungsparameter
  - Beschreibung,343
- CD-ROM
  - Deployment,277
- Certicom
  - Client/Server-Kommunikation verschlüsseln,230
- certificate\_company-Protokolloption
  - Beschreibung,392
- certificate\_name-Protokolloption
  - Beschreibung,393
- certificate\_unit-Protokolloption
  - Beschreibung,394
- chained, Option
  - ASE-Kompatibilität,559
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1253
  - Transact-SQL-Kompatibilität,560
- chained-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- chained-Option
  - Beschreibung,587
  - Sybase Open Client,1571
- CHANGE PASSWORD-Systemprivileg
  - Beschreibung,1309
- change\_password\_dual\_control-Option
  - Kennwörter für die Doppelkontrolle,1370
- CHAR, Datentyp
  - Kollationssequenz für neue Datenbanken,927
  - und Hostvariable,575
  - Zeichensatz für neue Datenbanken,927
- CHAR-Kollation
  - Info,515
- char\_charset, Alias
  - Info,501
- CharSet, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- CharSet, Verbindungsparameter
  - Beschreibung,343
- CharSet-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1237,1248
  - Verbindungseigenschaft, Beschreibung,711
- CHECK, Integritätsregeln
  - Datenbanken entladen,1014
- Check-In
  - Dateien von Interactive SQL,871
- CHECK-Integritätsregeln
  - Info,125
- Check-Out
  - Dateien von Interactive SQL,871
- Checkpoint-Logs
  - Info,143

---

CHECKPOINT-Systemprivileg  
  Beschreibung, 1309

checkpoint\_time, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1253  
  verwenden, 1077

checkpoint\_time-Eigenschaft  
  Verbindungseigenschaft, Beschreibung, 711

checkpoint\_time-Option  
  Beschreibung, 588

CheckpointLogCommitToDisk, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogCommitToDisk-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogPagesInUse, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogPagesInUse-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogPagesRelocated, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogPagesRelocated-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogPagesWritten, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogPagesWritten-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogSavePreimage, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogSavePreimage-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogSize, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogSize-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

CheckpointLogWrites, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointLogWrites-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

Checkpoints  
  checkpoint\_time-Option, 588  
  Dringlichkeit, 1077

Info, 141

Intervall, 239

Sicherungen, 1076

Transaktionslog nach Checkpoint löschen, 265

Unterschiede zwischen Personal Server und  
  Netzwerkserver, 151  
  während Sicherungen nicht zulässig, 1036

CheckpointUrgency, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

CheckpointUrgency-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

Checksum, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

Checksum-Eigenschaft  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1248

Chiffren  
  Transportschichtsicherheit, 1444

Chiffrieren  
  RAW-Verschlüsselung, 1436  
  Tabellenverschlüsselung aktivieren (dbinit), 1440  
  Tabellenverschlüsselung aktivieren (SQL), 1438

Chiffrierschlüssel  
  auswählen, 1432  
  DBKEY-Verbindungsparameter, 353  
  Dienstprogramm zum Entladen (dbunload), 1001  
  Dienstprogramm zur Logkonvertierung  
  (dbtran), 948  
  Initialisierung, Dienstprogramm (dbinit), 927  
  Löschen-Dienstprogramm (dberase), 916  
  mit der CREATE ENCRYPTED DATABASE-  
  Anweisung ändern, 1433  
  schützen, 1432  
  Transaktionslog-Dienstprogramm (dblog), 998

child\_creation-Option  
  verwenden, 1549

Chkpt, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

Chkpt-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

ChkptFlush, Eigenschaft  
  Datenbankeigenschaft, Beschreibung, 767

ChkptFlush-Statistik  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID, 1244

ChkptPage, Eigenschaft

- Datenbankeigenschaft, Beschreibung,767
- ChkptPage-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- cis\_option, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- cis\_option-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- cis\_option-Option
  - Beschreibung,589
- cis\_rowset\_size, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- cis\_rowset\_size-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- cis\_rowset\_size-Option
  - Beschreibung,589
- CleanablePagesAdded, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CleanablePagesCleaned, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CleanableRowsAdded, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CleanableRowsCleaned, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- Client-APIs
  - Zeichensatzkonvertierung,505
- Client-Dateien
  - allow\_read\_client\_file-Option,573
  - allow\_write\_client\_file-Option,575
- Client/Server
  - SQL-Anweisungen,503
  - Zeichensatzkonvertierung,503
- Client/Server-Kommunikation
  - Sprachen,498
- Clientdateien
  - isql\_allow\_read\_client\_file-Option [Interactive SQL],858
  - isql\_allow\_write\_client\_file-Option [Interactive SQL],859
  - read\_client\_file, gesicherte Funktion,280
  - write\_client\_file, gesicherte Funktion,280
- ClientLibrary-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ClientNodeAddress, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ClientPort, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ClientPort, Protokolloption
  - Beschreibung,395
- Clients
  - identifizieren,338
  - Kerberos,64
  - konfigurieren, um Zertifikat zu vertrauen,1453
  - mit gespiegelten Datenbanken verbinden,1472
  - SQL Anywhere mit Transportschichtssicherheit starten,1455
- Clients einrichten, um Zertifikat zu vertrauen
  - Transportschichtssicherheit,1453
- Clientseitig
  - DatabaseKey-Verbindungsparameter (DBKEY),353
  - Encryption-Verbindungsparameter (ENC),359
  - Sicherungen,1043
  - Sicherungen, Kurzeinführung,1028
- Clientseitiges Caching von Anweisungen
  - max\_client\_statements\_cached-Option einstellen,631
- clientseitiges Caching von Anweisungen
  - Info,629
- Clientsicherheit, trusted\_certificates-Protokolloption
  - MobiLink- Transportschichtssicherheit,1462
- ClientStmtCacheHits, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- ClientStmtCacheHits-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ClientStmtCacheHits-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- ClientStmtCacheMisses, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711,745
- ClientStmtCacheMisses-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ClientStmtCacheMisses-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- close\_on\_endtrans, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- close\_on\_endtrans-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- close\_on\_endtrans-Option
  - Beschreibung,590
  - Sybase Open Client,1571

---

- Cluster
  - Info,1527
- Clustered Hash Group By
  - optimization\_workload-Option,649
- Code-Editor
  - Erscheinungsbild anpassen,800
  - Info,800
  - öffnen,800
  - Schriften,800
  - Tastenkürzel,801
- Codepages
  - ANSI,500
  - default\_isql\_encoding-Option,856
  - für Unix-Plattformen empfohlene,531
  - für Windows-Plattformen empfohlene,530
  - Info,497
  - Interactive SQL (dbisql), Dienstprogramm,939
  - OEM,500
  - Überblick,499
  - Windows,500
- Collation-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- collect\_statistics\_on\_dml\_updates, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- collect\_statistics\_on\_dml\_updates-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- collect\_statistics\_on\_dml\_updates-Option
  - Beschreibung,591
- CollectStatistics, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CollectStatistics-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- command\_delimiter, Option
  - Einstellungen von Interactive SQL,851
- command\_delimiter-Option
  - Info,854
- CommandLine, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,745
- CommandLine-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- CommBufferSize, Verbindungsparameter
  - Beschreibung,343
- COMMENT ANY OBJECT-Systemprivileg
  - Beschreibung,1309
- COMMIT, Anweisung
  - auto\_commit-Option,853
- Commit, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Commit-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- Commit-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- commit\_on\_exit, Option
  - Einstellungen von Interactive SQL,851
- commit\_on\_exit-Option
  - Info,855
- CommitFile, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CommitFile-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CommLink, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- CommLinks, Verbindungsparameter
  - Beschreibung,345
  - Klammern,503
  - Optionen,103
- CommLinks-Verbindungsparameter
  - IPv6-Adressen,106
- CommNetworkLink, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- CommProtocol, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- COMP, Verbindungsparameter
  - Beschreibung,347
- CompactPlatformVer, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CompactPlatformVer-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- CompanyName, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CompanyName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- Compress, Verbindungsparameter
  - Beschreibung,347
- Compression, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711

- compression, Option
  - Beschreibung, 592
- compression-Option
  - SQL Remote-Replikationsoption, 563
- CompressionThreshold, Verbindungsparameter
  - Beschreibung, 348
- COMPTH, Verbindungsparameter
  - Beschreibung, 348
- CON, Verbindungsparameter
  - Beschreibung, 349
- conn\_auditing, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- conn\_auditing-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- conn\_auditing-Option
  - Beschreibung, 592
  - verwenden, 1417
- ConnCount, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- ConnCount-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1244
- Connect, Systemereignis
  - Beschreibung, 1091
- CONNECT-Privileg
  - Info, 1305
- ConnectedTime-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - Servereigenschaft, Beschreibung, 745
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237, 1248
  - Verbindungseigenschaft, Beschreibung, 711
- ConnectFailed, Systemereignis
  - Beispiel, 1094
  - Beschreibung, 1091
  - login\_procedure-Option, Beispiel, 627
- connection\_authentication, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
  - verwenden, 197
- connection\_authentication-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- connection\_authentication-Option
  - Beschreibung, 593
- CONNECTION\_PROPERTY, Funktion
  - Optionswerte abrufen, 567
- CONNECTION\_PROPERTY-Funktion
  - alphabetische Liste der Verbindungseigenschaften, 711
- ConnectionName, Verbindungsparameter
  - Beschreibung, 349
- ConnectionPool-Verbindungsparameter
  - unter Windows Mobile nicht unterstützt, 423
- ConnPoolCachedCount-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- ConnPoolCachedCount-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1244
- ConnPoolHits-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- ConnPoolHits-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1244
- ConnPoolMisses-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- ConnPoolMisses-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1244
- ConnsDisabled, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - Verbindungseigenschaft, Beschreibung, 745
- ConnsDisabled-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237, 1248
- ConsoleLogFile, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- ConsoleLogFile-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- ConsoleLogMaxSize, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- ConsoleLogMaxSize-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- CONSOLIDATE-Privileg
  - Info, 1305
- continue\_after\_raisererror, Option
  - ASE, Kompatibilität, 559
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
  - Transact-SQL-Kompatibilität, 560
- continue\_after\_raisererror-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- continue\_after\_raisererror-Option
  - Beschreibung, 594

---

conversion\_error, Option  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253  
     Transact-SQL-Kompatibilität,560  
 conversion\_error-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 conversion\_error-Option  
     Beschreibung,595  
 cooperative\_commit\_timeout-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 cooperative\_commit\_timeout-Option  
     Beschreibung,596  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253  
 cooperative\_commits, Option  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253  
 cooperative\_commits-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 cooperative\_commits-Option  
     Beschreibung,596  
 CopyNodeParent-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1248  
 CPOOL-Verbindungsparameter  
     unter Windows Mobile nicht unterstützt,423  
 CPORT, Protokolloption  
     Beschreibung,395  
 CPU  
     Serveroption -gt,251  
     Serveroption -gta,252  
     verwendete Anzahl,169  
 Crashes  
     berichten,1108  
 CREATE ANY INDEX-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY MATERIALIZED VIEW-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY OBJECT-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY PROCEDURE-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY SEQUENCE-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY TABLE-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY TEXT CONFIGURATION-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY TRIGGER-Systemprivileg  
     Beschreibung,1309  
 CREATE ANY VIEW-Systemprivileg  
     Beschreibung,1309  
 CREATE DATABASE, Anweisung  
     Dienstprogrammdatenbank,145  
 CREATE DATABASE-Anweisung  
     Datenbanken für Windows Mobile erstellen,445  
     Einschränkungen unter Windows Mobile,425  
     Privilegien,170  
     Privilegien für Anweisungen zur Dateiverwaltung,255  
 CREATE DATATYPE-Systemprivileg  
     Beschreibung,1309  
 CREATE DBSPACE-Anweisung  
     verwenden,131  
 CREATE DECRYPTED DATABASE-Anweisung  
     Verwendung,1431  
 CREATE DECRYPTED FILE-Anweisung  
     Datenbanken für den technischen Kundendienst entschlüsseln,1431  
 CREATE ENCRYPTED DATABASE-Anweisung  
     verglichen mit CREATE ENCRYPTED FILE,1427  
     Verwendung,1430  
 CREATE ENCRYPTED FILE-Anweisung  
     Datenbanken für den technischen Kundendienst verschlüsseln,1109  
     verglichen mit CREATE ENCRYPTED DATABASE,1427  
 CREATE EVENT-Anweisung  
     Einschränkungen unter Windows Mobile,425  
 CREATE EXISTING TABLE, Anweisung  
     unter Windows Mobile nicht unterstützt,425  
 CREATE EXTERNAL REFERENCE-Systemprivileg  
     Beschreibung,1309  
 CREATE EXTERNLOGIN-Anweisung  
     unter Windows Mobile nicht unterstützt,425  
 CREATE FUNCTION-Anweisung  
     Einschränkungen unter Windows Mobile,425  
 CREATE LOGIN POLICY, Anweisung  
     Kennwortsicherheit erhöhen,1410  
 CREATE MATERIALIZED VIEW-Systemprivileg  
     Beschreibung,1309  
 CREATE MESSAGE-Systemprivileg  
     Beschreibung,1309

- CREATE MIRROR SERVER-Anweisung
  - Datenbankspiegelung einrichten,1480
- CREATE ON-Privileg
  - Info,1305
- CREATE PROCEDURE-Systemprivileg
  - Beschreibung,1309
- CREATE PROXY TABLE-Systemprivileg
  - Beschreibung,1309
- CREATE ROLE-Anweisung
  - benutzererweiterte Rollen,1287
- CREATE SERVER-Anweisung
  - unter Windows Mobile nicht unterstützt,425
- CREATE TABLE-Anweisung
  - Einschränkungen unter Windows Mobile,425
- CREATE TABLE-Systemprivileg
  - Beschreibung,1309
- CREATE TEXT CONFIGURATION-Systemprivileg
  - Beschreibung,1309
- CREATE USER-Anweisung
  - verwenden,1342
- CREATE VIEW-Systemprivileg
  - Beschreibung,1309
- CREATE-Privileg
  - DBSpaces,129
- createcert, Dienstprogramm
  - Syntax,894
  - Verwendung,1447
- createkey, Dienstprogramm
  - Syntax,945
- CS, Verbindungsparameter
  - Beschreibung,343
- CSFC5KTNAME, Umgebungsvariable
  - Kerberos,64
- CSV-Dateien
  - Monitor,1138
- CURRENT USER
  - Umgebungseinstellungen,488
- CurrentCacheSize, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- CurrentCacheSize-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- CurrentLineNumber, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- CurrentMultiProgrammingLevel-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- CurrentProcedure, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- CurrentRedoPos, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CurrentRedoPos-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- CurrIO, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CurrIO-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CurrRead, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CurrRead-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- CurrWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- CurrWrite-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Cursor
  - ansi\_close\_cursors\_on\_rollback-Option,576
  - close\_on\_endtrans-Option,590
  - Datenbankoptionen,564
  - max\_cursor\_count-Option,631
  - und Transaktionen,590
- Cursor, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Cursor-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- Cursor-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- CursorOpen, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- CursorOpen-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- CursorOpen-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- CyberSafe, Kerberos-Client
  - Unix-Unterstützung,64
  - Windows-Unterstützung,64

---

## D

### DAC

- Regeln für verschachtelte Ansichten und Tabellen,1365

### Daemon

- ud, Datenbankserveroption,298
- Datenbankserver ausführen,192

### database\_authentication, Option

- SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- verwenden,195

### database\_authentication-Eigenschaft

- Verbindungseigenschaft, Beschreibung,711

### database\_authentication-Option

- Beschreibung,597

### DatabaseCleaner, Eigenschaft

- Datenbankeigenschaft, Beschreibung,767

### DatabaseCleaner-Eigenschaft

- SQL Anywhere SNMP-Erweiterungsagent, OID,1248

### DatabaseFile, Verbindungsparameter

- Beschreibung,351
- eingebettete Datenbanken,28

### DatabaseKey, Verbindungsparameter

- Beschreibung,353

### DatabaseName, Protokolloption

- Beschreibung,397

### DatabaseName, Verbindungsparameter

- Beschreibung,354

### DatabaseStart, Systemereignis

- Beschreibung,1091

### DatabaseSwitches, Verbindungsparameter

- Beschreibung,355

### DataSourceName, Verbindungsparameter

- Beschreibung,356
- Windows Mobile,48

### date\_format, Option

- Beschreibung,599
- SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- Transact-SQL-Kompatibilität,560

### date\_format-Eigenschaft

- Verbindungseigenschaft, Beschreibung,711

### date\_format-Option

- Sybase Open Client,1571

### date\_order, Option

- Beschreibung,601

- SQL Anywhere SNMP-Erweiterungsagent, OID,1253

- Transact-SQL-Kompatibilität,560

### date\_order-Eigenschaft

- Verbindungseigenschaft, Beschreibung,711

### date\_order-Option

- Sybase Open Client,1571

### Dateidatenquellen

- erstellen,46

### Dateien

- Check-In von Interactive SQL,871

- Check-Out von Interactive SQL,871

- Interactive SQL-Versionsverwaltung konfigurieren,869

- Position,483

- verschlüsseln,1426

- Versionsverwaltungsintegration von Interactive SQL verwenden,868

- von Interactive SQL aus aktualisieren,873

### Dateien als Source nehmen

- Unix/Mac,468

### Dateien verbergen, Dienstprogramm (dbfhide)

- Syntax,922

### Dateigröße

- reduziert nach Neuaufbau,1012

### Dateistandorte

- Windows Mobile,430

### Daten

- nearest\_century-Option,640

### Daten entladen

- berechnete Spalten neu berechnen,1001

- Sicherheit,1408

- Zeichensätze angeben,343

### Daten exportieren

- Ausgabeformat,866

### Daten laden

- Sicherheit,1408

### Daten sichern und wiederherstellen

- Strategien für Windows Mobile,449

### Datenbank

- dokumentieren,814

- Kollationen,515

### Datenbank dokumentieren

- Info,814

### Datenbank erstellen, Assistent

- verwenden,125

### Datenbank löschen, Assistent

- verwenden,149

- Datenbank validieren, Assistent
  - Tabellen validieren,1086
  - Vorgehensweise,1081
- Datenbank wiederherstellen, Assistent
  - verwenden,1050
- Datenbank, Dienstprogramme
  - Datenquelle (dbdsn),905
  - Dienst (dbsvc),974
  - Information (dbinfo),925
  - Initialisierung (dbinit),927
  - Sicherung (dbbackup),886
  - Skriptausführung (dbrunsql),959
  - Sprachauswahl (dblang),946
  - Verbergen von Dateien (dbfhide),922
- Datenbank-Dienstprogramme
  - Entladen (dbunload),1000
  - Histogramm (dbhist),923
  - Interactive SQL (dbisql),939
  - Logkonvertierung (dbtran),948
  - Performancestatistiken (dbstats),953
  - Ping (dbping),955
  - Serverauflistung (dblocate),960
  - Serverlizenzierung (dblic),964
  - Serverstart im Hintergrund (dbspawn),983
  - Serverstopp (dbstop),984
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),981
  - Transaktionslog (dblog),998
  - Upgrade (dbupgrad),1017
  - Validierung (dbvalid),1020
  - Versionsdiagnose (dbversion), Syntax,1024
- Datenbank-Informationen
  - mit dbinfo abrufen,925
- Datenbank-Monitoring
  - Info,1115
- Datenbankdatei, Verschlüsselung
  - Initialisierung, Dienstprogramm (dbinit),927
- Datenbankdateien
  - Datenträgerfehler,1047
  - Fehlerbehandlung, internes Entladen,1016
  - Grenze,130
  - Info,119
  - maximale Größe,791
  - minimale Größe,927
  - mit dberase löschen,916
  - mit dbinit verschlüsseln,927
  - NDS,213
  - Pfade,213
  - Position,213
  - Sicherheit,1407
  - Sicherungen,1076
  - UNC-Dateinamen,213
  - verschlüsseln,1424
  - Vorgänge mit Lese-/Schreibzugriff einschränken,1411
  - Zeitstempel,136
- Datenbankdienstprogramme
  - Datenverbindungen,30
- Datenbankeigenschaften
  - alphabetische Liste,767
  - Berichte,955
  - Groß-/Kleinschreibung,766
  - mit dem SQL Anywhere SNMP-Erweiterungsagenten abfragen,1225
  - mit dem SQL Anywhere SNMP-Erweiterungsagenten setzen,1226
  - OIDs für den SQL Anywhere SNMP-Erweiterungsagenten,1248
- Datenbanken
  - Abnahme der Dateigröße nach Neuaufbau,1012
  - alphabetische Liste der Eigenschaften,767
  - Auditing unter Windows Mobile,1442
  - auf Ihr Windows Mobile-Gerät kopieren,446
  - aus Archivsicherungen mit Interactive SQL wiederherstellen,1051
  - aus Archivsicherungen mit Sybase Central wiederherstellen,1050
  - aus Sicherungskopien wiederherstellen,1049
  - aus Sybase Central validieren,1081
  - Ausführen vollständiger Sicherungen,1030
  - authentifizierte, Upgrade von,200
  - Authentifizierung,597
  - automatisch stoppen,238
  - Behandlung von Verbindungsfehlern,79
  - Beispieldatenbank, praktische Einführung,1
  - Dateikompatibilität,121
  - DBSpaces ändern,132,133
  - DBSpaces löschen,134,135
  - den vorhandenen Diensten hinzufügen,188
  - Dienstprogramme,145,882
  - entschlüsseln,1431
  - erstellen,121
  - erstellen von der Befehlszeile aus,126,149
  - erstellen von Sybase Central aus,125
  - Fehlerbehandlung,1107
  - Fehlerbehandlung, internes Entladen,1016

---

- Funktionen sichern,1415
- für Kerberos konfigurieren,67
- für nicht-englische Sprachen erstellen,522
- für Windows Mobile erstellen,441
- für Windows Mobile konfigurieren,439
- Gesundheit und Statistik,812
- große Datenbanken,128
- Größenänderungen,1107
- Hinweise zur Planung,121
- Informationen,925
- initialisieren,121
- initialisieren von Sybase Central aus,125
- inkrementelle Sicherungen durchführen,1031
- Kollationen ändern,527
- lokale Datenbank starten und Verbindung herstellen (Dienstprogramm dbisql),18
- lokale Datenbanken starten und Verbindungen herstellen,16
- löschen,149
- Löschen unter Windows Mobile über die Benutzeroberfläche des Geräts,450
- maximale Größe,791
- maximale Namenslänge,791
- Mehrfachdatei,128
- minimale Größe,927
- mit authentifizierten Anwendungen verwenden,194
- mit dberase löschen,916
- mit dbinit erstellen,927
- mit dbunload entladen,1000
- mit dem Windows-Explorer unter Windows Mobile löschen,450
- mit einer lokalen Datenbank verbinden (Dienstprogramm dbisql),18
- mit lokalen Datenbanken verbinden,17
- mit Netzwerkdatenbanken verbinden,23
- mit Netzwerkdatenbanken verbinden (Dienstprogramm dbisql),24
- Namenseinschränkungen,329
- ohne Verbindung starten,157
- Optionen einrichten,566
- planen,121
- Privilegien,1271,1340
- Privilegien zum Entladen,242
- Privilegien zum Laden,242
- Privilegien zum Starten,240
- Prüfsummen validieren,1021
- Schemata konvertieren,810
- schreibgeschützt,170
- Seitenbelegung,925
- Sicherheit unter Windows Mobile,1442
- Sicherung,1027
- Speicherplatz zuweisen,132,133
- starten,156
- stoppen,158,159
- Transaktionslog,121
- über Live-Sicherungen neu starten,1052
- über ODBC verbinden,19
- unter Windows Mobile erstellen (Dienstprogramm dbinit),444
- unter Windows Mobile erstellen (Interactive SQL),445
- unter Windows Mobile neu aufbauen,447
- Upgrade mit dbupgrad,1017
- Validieren mit dbvalid,1020
- verbinden mit,5
- verbinden über TCP/IP,25
- verbinden von Interactive SQL,15
- verbinden von Sybase Central,14
- verbinden, vom SQL Anywhere-Konsolendienstprogramm,15
- Verbindung trennen (dbconsole),102
- Verbindung trennen (SQL),101
- Verbindungsszenarien,30
- vergleichen,809
- verschlüsseln,1424
- Verschlüsselte Dateien komprimieren,1424
- Wiederherstellung,1027
- Zeichensatz,502
- Zeitstempel,136
- zum Starten erforderliche Privilegien,240
- zum Stoppen erforderliche Privilegien,240,242
- Datenbanken auf anderen Computern starten und Verbindungen herstellen
  - Beispiel,26
- Datenbanken authentifizieren
  - Info,195
  - überprüfen,196
- Datenbanken entladen
  - berechnete Spalten neu berechnen,1001
- Datenbanken erstellen
  - Assistent zum Erstellen einer Datenbank,125
  - Info,121
  - Optionen,927
  - praktische Einführung,114
  - Sicherheit,1408
  - Windows Mobile ,441

- Datenbanken für Windows Mobile erstellen
  - Sybase Central,442
- Datenbanken initialisieren
  - Sybase Central,125
- Datenbanken konfigurieren
  - Windows Mobile,439
- Datenbanken kopieren
  - Sicherheitsprobleme,76
- Datenbanken löschen
  - Info,916
  - Sicherheit,1408
  - Sybase Central,149
- Datenbanken neu aufbauen
  - Kollationen ändern,527
  - Windows Mobile ,447
- Datenbanken starten
  - Beispiele,153
  - Info,156
  - ohne Verbindung,157
- Datenbanken stoppen
  - Info,158,159
- Datenbanken unter Windows Mobile neu aufbauen
  - Info,447
- Datenbanken vergleichen
  - Vorgehensweise,809
- Datenbanken vergleichen, Fenster
  - verwenden,809
- Datenbanken, beschädigte
  - Info,1080
- Datenbankfunktionen deaktivieren
  - Schlüssel für gesicherte Funktionen verwenden,669
- Datenbankfunktionen sichern
  - sf, Serveroption,280
  - Info,1415
  - Schlüssel für gesicherte Funktionen angeben,288
- Datenbankgröße
  - Lösen von unerwarteten Änderungen,1107
  - unerwartete Erhöhung,1107
- Datenbankgrößen
  - Grenze,791
  - unerwartete Herabsetzung,1107
- Datenbanknamen
  - DatabaseName-Verbindungsparameter,354
  - festlegen,328
  - Groß-/Kleinschreibung berücksichtigen,162
  - Maximale Länge,791
  - Option,161
- Datenbankobjekte
  - DBSpace festlegen,128
  - in Sybase Central suchen,799
  - Typfilter konfigurieren,797
- Datenbankobjektprivilegien
  - Info,1305
- Datenbankoptionen
  - alphabetische Liste der Datenbankoptionen,544
  - alphabetische Liste der JDBC-Kompatibilitätsoptionen,559
  - alphabetische Liste der Open Client-Kompatibilitätsoptionen,559
  - alphabetische Liste der SQL Remote-Optionen,563
  - alphabetische Liste der Synchronisationsoptionen,562
  - alphabetische Liste der Transact-SQL-Kompatibilitätsoptionen,560
  - ASE, Kompatibilitätsoptionen,559
  - Bereich und Dauer,564
  - Command Sequence-Kommunikationsprotokoll,572
  - Datenbankserver (Datenbank),203
  - einrichten,566
  - einstellen,566
  - Einstellungen beim Start,1572
  - Einstellungen für SQL-Anweisungen,565
  - Einstellungen löschen,567
  - Einstellungen überwachen,569
  - für SQL Anywhere MobiLink-Clients setzen,562
  - Groß-/Kleinschreibung,567
  - Info,544
  - Interactive SQL-Optionen definieren,851
  - isolation\_level-Datenbankoption,619
  - Klassifizierung,559
  - mit dem SQL Anywhere SNMP-Erweiterungsagenten abfragen,1225
  - mit dem SQL Anywhere SNMP-Erweiterungsagenten setzen,1226
  - mit Sybase Central ändern,570
  - OIDs für den SQL Anywhere SNMP-Erweiterungsagenten,1253
  - Optionen für Interactive SQL,851
  - read\_past\_deleted,661
  - SQL Remote-Replikationsoptionen,563
  - Sybase Open Client,1571
  - TDS-Kommunikationsprotokoll,572
  - Transact-SQL, Kompatibilitätsoptionen,560
  - truncate\_timestamp\_values,697
  - trusted\_certificates\_file-Option,696

- 
- Überblick,544
  - Werte finden,567
  - Datenbankschemas
    - Vergleich,809
  - Datenbankseiten
    - Datenbankcache vorwärmen,226
    - Größe anzeigen,925
    - zur Cachevorwärmung sammeln,220
  - Datenbankserver
    - Aktionen protokollieren,163
    - alphabetische Liste der Eigenschaften,745
    - als Daemon ausführen,192
    - alternative Namen angeben,332
    - Anzahl der verwendeten Kerne,253
    - automatisch starten,83
    - Beispieldatenbank, praktische Einführung,1
    - bevorzugte Server bei der
      - Datenbankspiegelung,1484
    - Datenbankfunktionen sichern,1415
    - dialogfrei,170
    - dialogfreier Betrieb,170
    - Dienste,180
    - Eigenschaften,745
    - Eingabe alternativer Namen für einen Spiegelserver,331
    - Fehlerbehandlung beim Serverstart,1109
    - herunterfahren,294
    - hohe Verfügbarkeit bei Datenbankspiegelung,1467
    - im Hintergrund ausführen,180
    - maximale Namenslänge,791
    - mit dbping suchen,95
    - mit LDAP verwenden,109
    - mit Transportschichtssicherheit starten,1454
    - mit UNC-Verbindungsparameter stoppen,386
    - Multiprogramming-Stufe,175
    - Multiprogramming-Stufe einstellen,244
    - Name,266
    - Namen-Kürzungslänge,267
    - Namenseinschränkungen,267
    - Namensoption,161
    - Namenszwischenspeicherung,94
    - nicht als Standardserver,307
    - Optionen,203
    - Performancewarnungen,1110
    - SATMP -Umgebungsvariable,475
    - Sicherheit,1408
    - Speicherort temporärer Dateien,120,475
    - Standard,266
    - starke Verschlüsselungsalgorithmen mit FIPS-Bestätigung verwenden,237
    - starten,153
    - Starten verhindern,341
    - stoppen,154
    - suchen,83
    - Syntax,203
    - TCP/IP starten,305
    - temporäre Verbindungen,78
    - unter Vista betreiben,202
    - unter Windows 7 ausführen,202
    - unter Windows Mobile starten,434
    - unter Windows Vista automatisch starten,358
    - Unterschiede zwischen Personal Server und Netzwerkserver,151
    - Windows Mobile,451
    - zum Stoppen erforderliche Privilegien,242
  - Datenbankserver kann nicht gefunden werden
    - Speicherort eines Datenbankservers ermitteln,83
  - Datenbankserver nicht gefunden, Fehler
    - Ursache diagnostizieren,98
  - Datenbankserver stoppen
    - Spiegelungssystem,1490
  - Datenbankserver, Meldungsfenster
    - Performance-Meldungen unterdrücken,275
    - unterdrücken,276
  - Datenbankserver-Meldungslog
    - Datei angeben,268
    - für Datenbankserver konfigurieren,163
    - Größe begrenzen,270
    - Info,163
    - kürzen,271
    - Name,268
    - Performancewarnungen,1110
    - Statistik zur Multiprogramming-Stufe,248
    - umbenennen und neu starten,269
  - Datenbankservereigenschaften
    - Groß-/Kleinschreibung,744
  - Datenbankservermeldungen, Fenster
    - Info,163
    - unter Linux verwenden,302
  - Datenbanksicherung, Assistent
    - verwenden,1041
  - Datenbankspiegelung
    - sm, Option,331
    - Asynchron-Ganzseiten-Modus,1478
    - asynchroner Modus,1478
    - bevorzugte Server,1484
-

- Clientverbindungen,1472
- Datenbankserver stoppen,1490
- den Primärserver bestimmen,1483
- Einschränkungen,1475
- Failover erzwingen,1488
- Info,1467
- konfigurieren,1480
- Kopieknoten,1536
- Logdateien,1484
- Login-Richtlinien verwalten,543
- mit Scale-Out mit Schreibschutz verwenden,1538
- mit Webdiensten verwenden,1540
- nach einem Primärserver-Ausfall wiederherstellen,1499
- Netzwerk-Datenbankserver erforderlich,1475
- NodeType-Verbindungsparameter (NODE),375
- nur TCP/IP-Verbindungen unterstützt,1475
- Option -sn,332
- Option -xa,306
- Option -xf,308
- Option -xp,335
- Partnerserver,1468
- Performance,1476
- Praktische Einführung,1509
- praktische Einführung mit gemeinsamem Arbiterserver,1516
- Primärserver herunterfahren,1500
- Quorum,1469
- Rolle des Arbiterservers,1468
- Rollenwechsel,1487
- schreibgeschützter Zugriff auf Spiegelserver,1473
- Server ändern,1490
- Server löschen,1490
- Sicherungen,1487
- Statusinformationsdateien,1498
- Synchroner Modus,1478
- Synchronisationsmodi,1477
- Synchronisationsstatus,1480
- synchronize\_mirror\_on\_commit-Option setzen,688
- Systemereignisse,1093
- Szenarien,1501,1504
- Transaktionslog nicht zu kürzen,1475
- Trap des SQL Anywhere SNMP-Erweiterungsagenten,1227
- übergeordneten Knoten für Kopieknoten ermitteln,1551
- unter Windows Mobile nicht unterstützt,423
- Unterschiede zwischen Personal Server und Netzwerkserver,151
- Datenbankspiegelungsmodus wählen Info,1477
- Datenbankstatistiken
  - mit dem SQL Anywhere SNMP-Erweiterungsagenten abfragen,1225
  - OIDs für den SQL Anywhere SNMP-Erweiterungsagenten ,1244
  - SQL Anywhere MIB,1244
- Datenbankvalidierung
  - Info,1080
  - Validierungs-Dienstprogramm verwenden,1020
- Datenbankverbindungen
  - Kopieknoten,1545
  - Ping-Dienstprogramm (dbping),955
  - Scale-Out mit Schreibschutz,1545
- Datenbankverschlüsselung
  - Info,1424
  - Windows Mobile,441
- Datenbankzugriff
  - Aufgaben steuern, die Benutzer ausführen können,1409
  - kontrollieren,1409
  - Sicherheitsfunktionen,1402
- Datenintegrität
  - Spalten-Integritätsregeln,125
- Datenquelle, Dienstprogramm (dbdsn)
  - Beendigungscode,909
  - Syntax,905
- Datenquelle-Dienstprogramm (dbdsn)
  - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
- Datenquellen
  - (dbdsn), Dienstprogramm,905
  - Beispiel,20
  - Datei,46
  - Embedded SQL,39
  - für Windows Mobile erstellen,435
  - Info,38
  - Interactive SQL (dbisql), Dienstprogramm,939
  - Mac OS X,45
  - mit dem ODBC-Datenquellen-Administrator erstellen,41

- 
- mithilfe des Fensters Verbinden erstellen,39
  - ODBC,38
  - ODBC mit dbdsn erstellen,905
  - ODBC-Verbindungsparameter,911
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
  - Unix,49
  - unter Windows Mobile verwenden,48
  - Verbindungsparameter,31
  - zusätzliche Verbindungsparameter angeben,22
  - Datenquellendienstprogramm (dbdsn)
    - Systeminformationsdatei,908
  - Datensicherheit gewährleisten
    - Übersicht,1402
  - Datenträgerfehler
    - Info,1067
    - Schutz,1067
    - Transaktionslogspiegel,1059
  - Datentypen
    - auswählen,122
    - Einschränkungen,791
  - Datentypkonvertierungen
    - Fehler,595
  - Datenwiederherstellung
    - Info,1027
  - Datumsangaben
    - date\_order-Option,601
  - db\_charset
    - Info,500
  - DB\_PROPERTY-Funktion
    - alphabetische Liste der Datenbankeigenschaften,767
  - db\_publisher-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - db\_publisher-Option
    - Beschreibung,602
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - DBA
    - Angabe für neue Datenbanken,927
    - Superuser erstellen,1295
  - DBA-Berechtigung (nicht mehr empfohlen)
    - konvertiert in SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle,1275
  - dbbackup, Dienstprogramm
    - Beendigungscode,891
    - clientseitige Sicherungen,1043
    - Fehlermeldungen,886
    - inkrementelle Sicherungen,1031
    - Live-Sicherung,1032
    - Syntax,886
    - Transaktionslogs kürzen,1072
    - vollständige Sicherungen,1030
  - dbcapi.dll
    - Client-APIs und Zeichensatzkonvertierung,505
  - dbconsole, Dienstprogramm
    - Benutzer trennen,102
    - Fenster konfigurieren,878
    - Software-Updates,879
    - starten,877
    - Suchfunktion für Updates konfigurieren,881
    - Syntax,981
    - verwenden,877
  - dbctrs16.dll
    - erweiterte Privilegien unter Vista erforderlich,202
    - erweiterte Privilegien unter Windows 7 erforderlich,202
    - erweiterte Privilegien unter Windows Server 2008 erforderlich,202
  - DBDiskSpace, Systemereignis
    - Beispiel,1094
    - Beschreibung,1092
  - dbdsn, Dienstprogramm
    - Beendigungscode,909
    - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Vista und späteren Versionen von Windows erforderlich,202
    - Syntax,905
    - Systeminformationsdatei,908
    - verwenden,43
  - dbelevat16.exe
    - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Vista und späteren Versionen von Windows erforderlich,202
    - für Deployments auf Vista erforderlich,203
    - für Deployments auf Windows 7 erforderlich,203
    - für Deployments auf Windows Server 2008 erforderlich,203

- dbeng16
  - Ausführung als Linux-Dienst,968
  - Ausführung als Windows-Dienst,974
  - Lizenzierung,964
  - Personal Datenbankserver,150
  - Syntax,203
- dberase, Dienstprogramm
  - Beendigungscodes,918
  - Syntax,916
- dbExpress
  - Client-APIs und Zeichensatzkonvertierung,505
- DBF, Verbindungsparameter
  - Beschreibung,351
  - eingebettete Datenbanken,28
- dbfhide, Dienstprogramm
  - Syntax,922
- DBFileFragments, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- DBFileFragments-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- dbhist, Dienstprogramm
  - Beendigungscodes,925
  - Syntax,923
- dbicu16.dll
  - Datenbanken für Windows Mobile erstellen,442
  - eine Datenbank unter Windows Mobile entladen,447
  - ICU unter Windows Mobile vermeiden,442
- dbicudt16.dat
  - Datenbanken für Windows Mobile erstellen,442
  - Datenbanken unter Windows Mobile entladen,447
  - ICU unter Windows Mobile vermeiden,442
- dbinfo, Dienstprogramm
  - Beendigungscodes,927
  - Größe einer Tabelle auf der Festplatte festlegen,926
  - Syntax,925
- dbinit, Dienstprogramm
  - Beendigungscodes,938
  - Datenbanken für Windows Mobile erstellen,444
  - Syntax,927
  - verwenden,126
- dbisql, Dienstprogramm
  - Beendigungscodes,944
  - Info,814
  - Syntax,939
  - über Datenquellen verbinden,20
  - unterstützte Plattformen,944
- dbisql.com
  - Info,944
- dbisql.exe
  - Info,944
  - Schnelllader-Option,876
- dbisqlc, Dienstprogramm
  - Syntax,915
  - unterstützte Plattformen,916
- DBKEY, Verbindungsparameter
  - Beschreibung,353
- dblang, Dienstprogramm
  - Beendigungscodes,947
  - Info,946
  - Syntax,946
- DBLauncher
  - Datenbankserver unter Mac OS X starten,9
- dbngen16.res
  - Speicherort ermitteln,484
- DBLIB
  - Client-APIs und Zeichensatzkonvertierung,505
- dblic, Dienstprogramm
  - Beendigungscodes,967
  - erweiterte Berechtigungen eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und späteren Versionen von Windows erforderlich,202
  - Syntax,964
- dblocate, Dienstprogramm
  - Beendigungscodes,963
  - Syntax,960
- dblog, Dienstprogramm
  - Auditing,1418
  - Beendigungscodes,1000
  - Befehlszeile,998
  - Syntax,998
  - Transaktionslog-Spiegel,140
- dblsn, Dienstprogramm
  - als Windows-Dienst ausführen,974
- dbmanageetd, Dienstprogramm
  - Diagnosedaten anzeigen,1105
  - Syntax,918
- dbmlsync, Dienstprogramm
  - als Linux-Dienst ausführen,968
  - als Windows-Dienst ausführen,974

---

TLS,1463  
 DBN, Protokolloption  
     Beschreibung,397  
 DBN, Verbindungsparameter  
     Beschreibung,354  
 DBNS  
     Definition,85  
 dbns16, Dienstprogramm  
     als Linux-Dienst ausführen,968  
     als Windows-Dienst ausführen,974  
     Syntax,891  
     verwenden,85  
 DBNumber-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 dbo, Benutzer  
     Systemobjekte und das Dienstprogramm zum  
     Entladen,1013  
 DBO-Systemrolle  
     Info,1272  
 dbodbc16.dll  
     erweiterte Privilegien eventuell unter Windows 7  
     erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Server 2008 erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Vista und später erforderlich,202  
 dboledb16.dll  
     erweiterte Privilegien eventuell unter Windows 7  
     erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Server 2008 erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Vista und später erforderlich,202  
 dboledba16.dll  
     erweiterte Privilegien eventuell unter Windows 7  
     erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Server 2008 erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
     Vista und später erforderlich,202  
 dbping, Dienstprogramm  
     Beendigungscodes,958  
     Syntax,955  
     Verwendung,95  
 dbping\_r, Dienstprogramm  
     unter Unix verwenden,955  
 dbremote, Dienstprogramm  
     als Linux-Dienst ausführen,968  
     als Windows-Dienst ausführen,974  
 dbrunsql, Dienstprogramm  
     Syntax,959  
 DBS, Verbindungsparameter  
     Beschreibung,355  
 dbsnmp16.dll  
     Info,1216  
 DBSpace erstellen, Assistent  
     verwenden,130  
 DBSpaces  
     ändern,132,133  
     CREATE ON-Privileg,1305  
     Dateinamenänderung beim Entladen,1001  
     default\_dbpace-Option,604  
     erstellen,130  
     erstellen (SQL),131  
     erstellen (Sybase Central),130  
     für große Datenbanken verwenden,128  
     Grenze,791  
     Info,128  
     löschen,134,135  
     Privilegien,129,1305  
     Standort mit Serveroption -ds angeben,325  
     vordefiniert,127  
 dbspawn, Dienstprogramm  
     Beendigungscodes,984  
     Syntax,983  
 dbsrv16  
     Ausführung als Linux-Dienst,968  
     Ausführung als Windows-Dienst,974  
     Lizenzierung,964  
     Netzwerk-Datenbankserver,150  
     Syntax,203  
     Transportschichtsicherheit,1454  
     Windows Mobile,451  
 dbstats, Dienstprogramm  
     Beendigungscodes,954  
     Syntax,953  
 dbstop, Dienstprogramm  
     Beendigungscodes,986  
     mit SQLCONNECT verwenden,986  
     Privilegien,242  
     Syntax,984  
     verwenden,154  
 dbsupport, Dienstprogramm  
     SADIAGDIR-Umgebungsvariable,473  
     Syntax,987  
     verwenden,1108

- dbsupport.ini
  - Info,991
- dbsvc, Dienstprogramm
  - Beendigungscodes,980
  - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
  - Linux, Optionen,968
  - Linux, Syntax,968
  - Windows, Optionen,974
  - Windows-Syntax,974
- DBTools, Schnittstelle
  - Client-APIs und Zeichensatzkonvertierung,505
- dbtran, Dienstprogramm
  - Audit-Daten abrufen,1421
  - Auditing,1418
  - Beendigungscodes,953
  - Befehlszeile,948
  - nicht festgeschriebene Änderungen,1048
  - Syntax,948
  - Transaktionslogs,1048
  - verwenden,1053
- dbunload, Dienstprogramm
  - Beendigungscodes,1014
  - DBSpace-Dateinamen,1001
  - Syntax,1000
- dbupgrad, Dienstprogramm
  - Beendigungscodes,1020
  - Syntax,1017
- dbvalid, Dienstprogramm
  - Beendigungscodes,1024
  - Syntax,1020
- dbversion, Dienstprogramm
  - Syntax,1024
- dbvss16.exe
  - Ausführung als Windows-Dienst,974
- dbvss16.exe
  - vss, Datenbankserveroption,303
  - SQL Anywhere VSS-Schreibprogramm,1042
- dbxtract, Dienstprogramm
  - unter Windows Mobile nicht unterstützt,429
- Deadlock, Systemereignis
  - Beschreibung,1091
- Deadlocks
  - Deadlock-Systemereignis,1091
  - log\_deadlocks-Option,623
- Deadlocks, melden
  - log\_deadlocks-Option,623
- Deaktivieren
  - Tabellenbearbeitung in Interactive SQL,832
- DEBUG ANY PROCEDURE-Systemprivileg
  - Beschreibung,1309
- Debug-Modus
  - Info,808
- debug\_messages, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- debug\_messages-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- debug\_messages-Option
  - Beschreibung,602
- Debuggen
  - SQL-Skripten,939
- DebuggingInformation, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- DebuggingInformation-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- DECRYPT-Funktion
  - für RAW-Entschlüsselung von Spalten verwenden,1436
  - zur Entschlüsselung von Spalten,1435
- dedicated\_task, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- dedicated\_task-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- dedicated\_task-Option
  - Beschreibung,603
- default\_dbspace, Option
  - Speicherort von Datenbankobjekten angeben,128
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- default\_dbspace-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- default\_dbspace-Option
  - Beschreibung,604
- default\_isql\_encoding, Option
  - Einstellungen von Interactive SQL,851
- default\_isql\_encoding-Option
  - Syntax,856
- default\_timestamp\_increment, Option
  - in MobiLink-Synchronisation verwenden,605

---

<p>SQL Anywhere SNMP-Erweiterungsagent, OID,1253</p> <p>default_timestamp_increment-Eigenschaft Verbindungseigenschaft, Beschreibung,711</p> <p>default_timestamp_increment-Option Beschreibung,605</p> <p>DefaultCollation-Eigenschaft Info,146 Servereigenschaft, Beschreibung,745 SQL Anywhere SNMP-Erweiterungsagent, OID,1237</p> <p>DefaultNcharCollation-Eigenschaft Servereigenschaft, Beschreibung,745 SQL Anywhere SNMP-Erweiterungsagent, OID,1237</p> <p>Definierer Systemprozeduren zum Ausführen als Definierer migrieren,1401</p> <p>delayed_commit_timeout-Eigenschaft Verbindungseigenschaft, Beschreibung,711</p> <p>delayed_commit_timeout-Option Beschreibung,606 SQL Anywhere SNMP-Erweiterungsagent, OID,1253</p> <p>delayed_commits, Option SQL Anywhere SNMP-Erweiterungsagent, OID,1253</p> <p>delayed_commits-Eigenschaft Verbindungseigenschaft, Beschreibung,711</p> <p>delayed_commits-Option Beschreibung,606</p> <p>DELETE ANY TABLE-Systemprivileg Beschreibung,1309</p> <p>DELETE-Anweisung in Interactive SQL generieren,829</p> <p>DELETE-Privileg Info,1305</p> <p>delete_old_logs, Option Kürzungs-Offset zurücksetzen,998 Transaktionslogoptionen,998</p> <p>delete_old_logs-Option SQL Remote, Beschreibung,607 SQL Remote-Replikations- und Synchronisationsoption,563</p> <p>Delphi binäre Spalten,642</p> <p>Delphi, Verbindungsparameter ODBC-Verbindungsparameter, Beschreibung,911</p>	<p>demo.db praktische Einführung,1</p> <p>Deployment Hinweise zu Vista,203 Hinweise zu Windows 7,203 Hinweise zu Windows Server 2008,203</p> <p>Deploymentsoftware unterstützte Plattformen,495</p> <p>DER-kodierte PKI-Objekte anzeigen,903</p> <p>DescribeCursor, Verbindungsparameter ODBC-Verbindungsparameter, Beschreibung,911</p> <p>Description, Verbindungsparameter ODBC-Verbindungsparameter, Beschreibung,911</p> <p>Dezimale Gesamtstellenzahl Datenbankoption,653</p> <p>DFÜ-Netzwerk Verbindungen,109</p> <p>Diagnosedaten anzeigen (dbmanageetd),1105</p> <p>Diagnoselogdateien Info,1101</p> <p>Diagnoseverzeichnis SADIAGDIR-Umgebungsvariable,473</p> <p>DIAGNOSTICS-Systemrolle Info,1272</p> <p>Dialogfrei Datenbankserver,170</p> <p>Dialogfreier Betrieb Datenbankserver,170</p> <p>Dialogfreier Modus Datenquelle, Dienstprogramm (dbdsn),906 Dienstprogramm dbisqlc,915 Dienstprogramm zum Entladen (dbunload),1001 Dienstprogramm zum Upgrade (dbupgrad),1018 Dienstprogramm zur Logkonvertierung (dbtran),948 Dienstprogramm zur Serverlizenzierung (dblic),964 Informationsdienstprogramm (dbbackup),926 Initialisierung, Dienstprogramm (dbinit),927 Interactive SQL (dbisql), Dienstprogramm,939 Löschen-Dienstprogramm (dberase),916 Ping-Dienstprogramm (dbping),955 Serverauflistung, Dienstprogramm (dblocate),961 Sicherungsdienstprogramm (dbbackup),886 Spawn-Dienstprogramm (dbspawn),983 Sprache, Dienstprogramm (dblang),946</p>
---	--

- SQL Anywhere-Skriptausführung,
  - Dienstprogramm (dbrunsql),959
  - Stopp-Dienstprogramm (dbstop),984
  - Transaktionslog-Dienstprogramm (dblog),998
  - Validierungs-Dienstprogramm (dbvalid),1021
- Dienst erstellen, Assistent
  - Vorgehensweise,182
- Dienste
  - Abhängigkeiten,191
  - Abhängigkeiten definieren,976
  - aktualisieren,189
  - auflisten,974
  - ausführbare Datei,187
  - ausführen unter Vista,203
  - ausführen unter Windows 7,203
  - ausführen unter Windows Server 2008,203
  - Datenbanken hinzufügen,188
  - Datenbankserver,180,744
  - Dienstprogramm für Dienste (dbsvc),974
  - Ereignisprotokoll,167
  - erstellen von Sybase Central aus,182
  - für Windows hinzufügen,182,183
  - Gruppen,190
  - Gruppenabhängigkeiten definieren,976
  - Info,180
  - konfigurieren,185
  - Konto,187
  - Linux, Abhängigkeiten definieren,969
  - Linux, auflisten,968
  - Linux, starten,968
  - löschen,184,185
  - mehrere,191
  - neue Datenbanken hinzufügen,188
  - nutzbare Programme,181
  - Optionen,186
  - Parameter,185
  - PID-Dateien,972
  - Registrierungseinstellungen,488
  - Sicherheit,187
  - Start fehlgeschlagen,186
  - starten,189
  - Startoptionen,186
  - Startreihenfolge,191
  - stoppen,189
  - Symbole auf dem Desktop,187
  - Terminaldienste,104
  - Typen unter Linux einstellen,969
  - Typen unter Windows einstellen,976
  - Windows,181
  - Windows-Dienste-Manager verwenden,190
- Dienstgruppen
  - Info,190
- Dienstprogramm für Dienste (dbsvc)
  - Beendigungscode,980
  - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
  - Linux, Optionen,968
  - Linux, Syntax,968
  - Windows, Optionen,974
  - Windows, Syntax,974
- Dienstprogramm für Supportanfragen (dbsupport)
  - Syntax,987
  - verwenden,1108
- Dienstprogramm zum Anzeigen von Zertifikaten (viewcert)
  - Syntax,903
- Dienstprogramm zum Entladen (dbunload)
  - Beendigungscode,1014
  - DBSpace-Dateinamen,1001
  - Syntax,1000
- Dienstprogramm zum Erstellen von Zertifikaten (createcert)
  - Syntax,894
- Dienstprogramm zum Upgrade (dbupgrad)
  - Beendigungscode,1020
  - Syntax,1017
- Dienstprogramm zur Logkonvertierung (dbtran)
  - Audit-Daten abrufen,1421
  - Auditing,1418
  - Beendigungscode,953
  - nicht festgeschriebene Vorgänge wiederherstellen,1048
  - Syntax,948
  - verwenden,1053
- Dienstprogramm zur Serverlizenzierung (dblic)
  - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und späteren Versionen von Windows erforderlich,202

---

Dienstprogrammbefehle  
     Privilegien,255

Dienstprogrammdatenbank  
     Info,145  
     Kennwort einrichten,289  
     Meldungen zum Verarbeitungsfortschritt,658  
     Privilegien zur Ausführung von Anweisungen steuern,255  
     Sicherheit,255  
     Unterschiede zwischen Personal Server und Netzwerkserver,151  
     util\_db.ini file,146  
     Verbindung herstellen,147  
     zulässige SQL-Anweisungen,146

Dienstprogramme  
     bedingte syntaktische Analyse in Konfigurationsdateien verwenden,883  
     Broadcast Repeater-Syntax (dbns16),891  
     Datenquelle (dbdsn), Syntax,905  
     dbisqlc-Syntax,915  
     Dienstprogramm für Supportanfragen (dbsupport), Syntax,987  
     Einführung,882  
     Entladen (dbunload), Syntax,1000  
     Erstellen von Zertifikaten (createcert), Syntax,894  
     ETD-Dateien, Dienstprogramm für die Verwaltung (dbmanageetd),918  
     Histogramm (dbhist), Syntax,923  
     Information (dbinfo), Syntax,925  
     Initialisierung (dbinit), Syntax,927  
     Interactive SQL (dbisql), Syntax,939  
     Konfigurationsdateien verwenden,882  
     Linux-Dienst (dbsvc), Syntax,968  
     Logkonvertierung (dbtran), Syntax,948  
     Löschen (dberase), Syntax,916  
     mit authentifizierten Anwendungen verwenden,195  
     Performancestatistiken (dbstats), Syntax,953  
     Ping (dbping), Syntax,955  
     Schlüsselpaargenerator-Dienstprogramm (createkey), Syntax,945  
     Serverauflistung (dblocate), Syntax,960  
     Serverlizenzierung (dblic), Syntax,964  
     Serverstart im Hintergrund (dbspawn), Syntax,983  
     Serverstopp (dbstop), Syntax,984  
     Sicherung (dbbackup), Syntax,886  
     Sprachauswahl (dblang), Syntax,946  
     SQL Anywhere-Konsole (dbconsole), Syntax,981

    SQL Anywhere-Skriptausführung (dbrunsql), Syntax,959  
     Syntax zum Anzeigen von Zertifikaten (viewcert),903  
     Transaktionslog (dblog), Syntax,998  
     unter Unix als Source nehmen,468  
     unterstützte Plattformen,882  
     Upgrade (dbupgrad), Syntax,1017  
     Validierung (dbvalid), Syntax,1020  
     Verbergen von Dateien (dbfhide), Syntax,922  
     Versionsdiagnose (dbversion), Syntax,1024  
     Windows-Dienst (dbsvc), Syntax,974

Dienstprogramme für die Datenbankadministration  
     Info,882

Digitale Signaturen  
     MobiLink-Transportschichtsicherheit,1461  
     SQL Anywhere-Transportschichtsicherheit,1455

Digitale Zertifikate  
     erstellen, bei Transportschichtsicherheit,1447  
     Transportschichtsicherheit,1447

Dirty Pages  
     Info,143

DisableMultiRowFetch, Verbindungsparameter  
     Beschreibung,357

Disconnect, Systemereignis  
     Beschreibung,1092

DISCONNECT-Anweisung  
     verwenden,101

disk full  
     Callback-Funktion,235

disk\_sandbox  
     gesicherte Funktion,1413

disk\_sandbox-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711

disk\_sandbox-Funktion  
     -sf, Serveroption,280

disk\_sandbox-Option  
     Beschreibung,608  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253

DiskRead, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
     Servereigenschaft, Beschreibung,745

DiskRead-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711

DiskRead-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244

- DiskReadHint, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadHintPages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadHintScatterLimit, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- DiskReadIndInt, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadIndInt-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- DiskReadIndLeaf, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadIndLeaf-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- DiskReadTable, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadTable-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- DiskReadWorkTable, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- DiskReadWorkTable-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- DiskReadWorkTable-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- DiskRetryRead, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- DiskRetryReadScatter, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- DiskRetryWrite, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- DiskSandbox-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237,1248
- DiskSyncRead, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskSyncWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskWaitRead, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskWaitWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskWrite-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- DiskWriteHint, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- DiskWriteHintPages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- Distributed Transaction Coordinator
  - Wiederherstellung ohne DTC,293
- divide\_by\_zero\_error, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- divide\_by\_zero\_error-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- divide\_by\_zero\_error-Option
  - Beschreibung,609
- DLLs
  - Speicherort,483
- DMRF, Verbindungsparameter
  - Beschreibung,357
- DOBROAD, Protokolloption
  - Beschreibung,398
- DoBroadcast, Protokolloption
  - Beschreibung,398
- Dokumentation
  - Datenbank dokumentieren,814
- DriveBus-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- DriveModel-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767

- 
- SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248
  - Driver, Verbindungsparameter
    - ODBC-Verbindungsparameter, Beschreibung,911
  - DriveType, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - DriveType-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248
  - DROP ANY INDEX-Systemprivileg
    - Beschreibung, 1309
  - DROP ANY MATERIALIZED VIEW-  
Systemprivileg
    - Beschreibung, 1309
  - DROP ANY OBJECT-Systemprivileg
    - Beschreibung, 1309
  - DROP ANY PROCEDURE-Systemprivileg
    - Beschreibung, 1309
  - DROP ANY SEQUENCE-Systemprivileg
    - Beschreibung, 1309
  - DROP ANY TABLE-Systemprivileg
    - Beschreibung, 1309
  - DROP ANY TEXT CONFIGURATION-  
Systemprivileg
    - Beschreibung, 1309
  - DROP ANY VIEW-Systemprivileg
    - Beschreibung, 1309
  - DROP CONNECTION-Anweisung
    - verwenden,101
  - DROP CONNECTION-Systemprivileg
    - Beschreibung, 1309
  - DROP DATABASE-Anweisung
    - unter Windows Mobile nicht unterstützt,425
  - DROP DATATYPE-Systemprivileg
    - Beschreibung, 1309
  - DROP MESSAGE-Systemprivileg
    - Beschreibung, 1309
  - DROP MIRROR SERVER-Anweisung
    - Kopieknotten löschen,1552
    - Spiegelserver löschen,1490
  - DROP ROLE-Anweisung
    - benutzererweiterte Rollen,1287
  - DROP SERVER-Anweisung
    - unter Windows Mobile nicht unterstützt,425
  - DSEdit, Dienstprogramm
    - Info,1571
    - nicht in SQL Anywhere enthalten,1571
  - DSN, Verbindungsparameter
    - Beschreibung,356
    - Info,38
    - Windows Mobile,48
  - DSN-Verbindungsparameter
    - verbinden,20
  - DYLD\_LIBRARY\_PATH-Umgebungsvariable
    - Beschreibung,469
  - Dynamische Cachebelegung
    - für Datenbankserver deaktivieren,219
  - Dynamische Cachegrößendimensionierung
    - Maximum einstellen,221
    - Mindestwert festlegen,224
  - Dynamische Traps
    - Info,1228
- ## E
- E-Mail-Versand
    - Monitor-Benutzer,1178
  - E-Mails
    - Monitor-Alarmbenachrichtigung,1188
  - Echo, Befehl
    - echo-Option,857
  - echo, Option
    - Einstellungen von Interactive SQL,851
  - echo-Option
    - Info,857
  - Editionen
    - SQL Anywhere OEM Edition,194
  - Eigenschaften
    - alphabetische Liste der  
Datenbankeigenschaften,767
    - alphabetische Liste der Servereigenschaften,744
    - alphabetische Liste der  
Verbindungseigenschaften,711
    - Datenbankeigenschaften in SQL Anywhere  
MIB,1248
    - Datenbanken,766
    - Servereigenschaft-OIDs in SQL Anywhere  
MIB,1237
    - Verbindungen,711
    - Zugriff auf Datenbankeigenschaften,766
    - Zugriff auf Datenbankservereigenschaften,744
    - Zugriff auf Verbindungseigenschaften,710
  - Eigentümer
    - Info,1348
  - Einbyte-Zeichensätze
    - Info,499

- Eine Datenbank auf diesem Computer starten und eine Verbindung herstellen
  - Verbinden-Fenster,14
- Eine Datenbank auf einem anderen Computer starten und eine Verbindung herstellen
  - Verbinden-Fenster,14
- Einfache Verschlüsselung
  - Info,1424
  - SQL Anywhere-Datenbanken unter Windows Mobile,1443
- Einfügen
  - Zeilen in Interactive SQL,832
- Eingabe
  - Interactive SQL, Befehle eingeben,819
- Eingebettete Datenbanken
  - Datenbankservernamen angeben,28
  - starten,28
  - verbinden,28
- Einrichten
  - Datenbankoptionen,566
- Einschränkungen
  - Bezeichner,791
  - Chiffrierschlüssel,1432
  - Datenbankspiegelung,1475
  - des Abfrage-Editors,837
  - Kennwörter,1367
  - Monitor,1118
  - Speicher,794
  - SQL Anywhere,791
  - SQL Anywhere unter Windows Mobile 5 für Smartphones,431
  - SQL Anywhere unter Windows Mobile ausführen,423
  - temporäre Datei,689
  - während der Wiederherstellung,1036
  - während Sicherungen,1036
- Einsenden
  - Fehlerberichte an den technischen Support,1108
- Einstellung
  - Aktualisierungsintervall,189
- Einstellungen der Logdatei ändern, Assistent
  - verwenden,136
- Einzug
  - Interactive SQL, Tastenkürzel,845
- Embedded SQL
  - Schnittstellenbibliothek,80
  - Verbindungen,50
  - Verbindungsperformance,96
  - Verbindungsperformance testen,96
- ENC, Verbindungsparameter
  - Beschreibung,359
  - Client/Server-Kommunikationen sichern,1455
- ENCRYPT-Funktion
  - für die Spaltenverschlüsselung,1435
  - für RAW-Verschlüsselung von Spalten verwenden,1436
- EncryptedPassword, Verbindungsparameter
  - Beschreibung,358
- Encryption
  - Kennwörter,1410
- Encryption, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- Encryption, Verbindungsparameter
  - Beschreibung,359
  - Client/Server-Kommunikationen sichern,1455
- Encryption-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- EncryptionScope, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- EncryptionScope-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- ENG-Verbindungsparameter
  - veraltet, stattdessen Server verwenden,383
- EngineName-Verbindungsparameter
  - veraltet, stattdessen ServerName verwenden,383
- ENP, Verbindungsparameter
  - Beschreibung,358
- Entfernt
  - REMOTE DBA erteilen (nicht mehr empfohlen),1400
- Entfernte Datenbanken
  - Hochverfügbarkeit,1470
- Entfernte IDs
  - in SQL Anywhere-Datenbanken einstellen,639
- Entity-Relationship-Diagramme
  - Info,811
- Entladen
  - Fehlerbehandlung,1016
  - Sicherheit,1408
- Entladen von Datenbanken
  - Fehlerbehandlung, fehlgeschlagenes Entladen,1016
- Entladen, Datenbanken
  - Dienstprogramm zum Entladen (dbunload),1000
- Entschlüsseln

- 
- Datenbanken,1431
  - Datenbanken für den technischen Kundendienst,1431
  - Tabellen,1437
  - Entwickeln, Anwendungen
    - Info,194
  - Entziehen
    - Berechtigungen, SQL-Syntax (nicht mehr empfohlen),1397
    - Mitgliedschaft in Gruppen mit REVOKE GROUP (nicht mehr empfohlen),1397
    - Mitgliedschaft in Gruppen mit REVOKE MEMBERSHIP IN GROUP (nicht mehr empfohlen),1397
  - ER-Diagramm, Registerkarte
    - Info,811
  - Erben
    - Privilegien,1349
  - Ereignis erstellen, Assistent
    - verwenden,1098
  - Ereignis-Handler
    - ausblenden,1100
  - Ereignisplanung
    - Definition,1090
  - Ereignisprotokoll
    - Nachrichten unterdrücken,167
  - Ereignisprotokollierung
    - Diagnosedaten anzeigen,1105
    - Info,1101
    - Schweregrade,1102
    - Sitzungen erstellen,1103
    - Sitzungen starten,1104
    - Sitzungen stoppen,1104
    - Systemereignisse auflisten,1106
  - Ereignisprotokollierung, Datendateien
    - Info,1101
  - Ereignisse
    - Assistent Zeitplan erstellen,1090
    - bedingte,1089
    - behandeln,1087
    - Datenbankdokumentation erstellen,814
    - Datenbankspiegelung,1476
    - Debugging,1099
    - Definition,1087
    - Ereignis-Handler ausblenden,1100
    - erstellen,1098
    - geplante,1089
    - Info,1088
    - manuell auslösen,1099
    - manuelle,1089
    - Systemereignisse,1089
    - Zeitplan definieren,1090
  - Ereignistypen
    - Info,1096
  - Ergebnismengen
    - Interactive SQL, Text,817
    - sortieren,830
    - Tabellenbearbeitung in Interactive SQL deaktivieren,832
    - Tabellenwerte in Interactive SQL bearbeiten,830
    - Zeilen einfügen,832
    - Zeilen kopieren,834
    - Zeilen löschen,833
  - Ergebnisse
    - unerwartete Symbole bei der Anzeige von Daten,504
  - Erneutes Aufrufen
    - Anweisungen in Interactive SQL,822
  - ERRORLEVEL, Umgebungsvariable
    - Interactive SQL-Rückgabecode,939
  - Ersatzzeichen
    - on\_charset\_conversion\_failure-Option,645
  - Erstellen
    - Datenbank mit verschlüsselten Tabellen auf der Basis einer vorhandenen Datenbank,1438,1440
    - Datenbanken für Windows Mobile ,441
    - Datenbanken mit dbinit,927
    - Datenbanken von der Befehlszeile aus,126
    - neue Zertifikate,894
    - ODBC-Datenquellen mit dbdsn,905
    - ODBC-Datenquellen mit dem ODBC-Datenquellen-Administrator,41
    - ODBC-Datenquellen mithilfe des Fensters Verbinden,39
    - praktische Einführung in Datenbanken,114
    - stark verschlüsselte Datenbank,1426
    - stark verschlüsselte Datenbank mit vorhandener Datenbank,1426
  - Erstellen entfernter IDs
    - SQL Anywhere-Datenbanken,639
  - Erstellen von Login-Richtlinien
    - Info,540
  - Erteilen
    - Berechtigungen, SQL-Syntax (nicht mehr empfohlen),1393

- Mitgliedschaft in Gruppen mit GRANT GROUP (nicht mehr empfohlen),1393
- Mitgliedschaft in Gruppen mit GRANT MEMBERSHIP IN GROUP (nicht mehr empfohlen),1393
- Erweiterte Zeichen
  - Info,499
- ESC-Schlüssel
  - Interactive SQL,845
- Escape-Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- escape\_character, Option
  - ASE-Kompatibilität,559
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- escape\_character-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- escape\_character-Option
  - Beschreibung,609
  - Sybase Open Client,1571
- Escapezeichen
  - Dienstprogramm zum Entladen (dbunload),1001
  - Konfigurationsdateien,883
  - ODBC-Datenquellen,911
- ESQL Sample
  - verwenden,463
- ETD-Dateien
  - dbmanagetd, Dienstprogramm,918
  - Info,1101
- ETD-Dateien, Dienstprogramm für die Verwaltung (dbmanagetd)
  - Syntax,918
  - verwenden,1105
- Ethernet
  - Info,98
- Event-Handler
  - Auswirkung auf lizenzierte Verbindungen,1097
  - Definition,1087
  - Fehlersuche,1095
  - Interna,1097
  - Transaktionsverhalten,1098
- EventName-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- EventTypeDesc-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- EventTypeName-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- ExchangeTasks, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,745
- ExchangeTasks-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- ExchangeTasksCompleted, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- exclude\_operators, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- exclude\_operators-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- exclude\_operators-Option
  - Beschreibung,610
- EXECUTE ANY PROCEDURE-Systemprivileg
  - Beschreibung,1309
- EXECUTE LOGIN
  - GRANT-Anweisung, Syntax (nicht mehr empfohlen),1393
  - REVOKE-Anweisungssyntax (nicht mehr empfohlen),1397
- EXECUTE-Privileg
  - Info,1305
- Explizite Selektivitätsschätzungen
  - user\_estimates-Option,702
- Exportieren
  - Monitor-Metriken,1174
  - Verbindungsprofile,13
- ExprCacheAbandons, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheDropsToReadOnly, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheEvicts, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheHits, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheInserts, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheLookups, Eigenschaft

- Datenbankeigenschaft, Beschreibung,767
- Verbindungseigenschaft, Beschreibung,711
- ExprCacheResumesOfReadWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExprCacheStarts, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- ExtendDB, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ExtendDB-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- extended\_join\_syntax, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- extended\_join\_syntax-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- extended\_join\_syntax-Option
  - Beschreibung,610
- ExtendTempWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ExtendTempWrite-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- extern\_login\_credentials-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- extern\_login\_credentials-Option
  - Beschreibung,611
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- external\_remote\_options, Option
  - SQL Remote-Option,611
- Externe Entladevorgänge
  - Vorgehensweise,1014
- Externe Funktionen
  - Stackgröße,241
- Externe gespeicherte Prozeduren
  - unter Windows Mobile nicht unterstützt,423
- Externe Logins
  - löschen,1345
- Externe Umgebungen
  - unter Windows Mobile nicht unterstützt,423
- Extraktionsdienstprogramm (dbxtract)
  - unter Windows Mobile nicht unterstützt,429

## F

- Failover
  - Cluster,1527
  - Datenbank-Spiegelungsszenarien,1501,1504
  - Datenbankspiegelung,1467
  - Veritas Cluster Server und SQL Anywhere,1527
- Favoritenliste
  - bearbeiten,825
  - exportieren,826
  - gemeinsam nutzen,826
  - hinzufügen,824
  - importieren,826
  - Info,824
- Federal Information Processing Standard (FIPS)
  - Info,1445
- Fehler
  - Berichte an den technischen Support senden,1108
  - Event-Handler-Verhalten,1098
  - in Interactive SQL,828
  - Transact-SQL-Prozeduren,646
- Fehler melden
  - Info,1108
- Fehler-Berichterstellung
  - Dienstprogramm für Supportanfragen (dbsupport),987
- Fehlerbehandlung
  - Clientanwendungen identifizieren,338
  - Datenbanken,1107
  - Datenbankserver,315
  - Datenbankspiegelung,1497
  - Datenbankverbindungen,79
  - Ergebnisse,504
  - fehlgeschlagenes Entladen,1016
  - HTTP-Clients,315
  - Info,1087,1107
  - Interactive SQL,865
  - Kerberos-Verbindungen,73
  - Monitor,1198
  - Netzwerkverbindungen,1113
  - ODBC,955
  - Performancewarnungen des Datenbankservers,1110
  - Ping-Dienstprogramm (dbping),955
  - Protokolle,1113
  - Serverauflistung, Dienstprogramm (dblocate),960
  - Serverstartprozedur,1109
  - Sicherungen,141

- SQL Anywhere,1107
- Timeout,1114
- Transact-SQL-Prozeduren,646
- Verbindungen,79
- Verbindungen (Netzwerk),98
- Fehlerbehandlung von unerwarteten Symbolen bei der Ergebnisanzeige
  - Info,504
- Fehlerberichte
  - Info,1108
  - Monitor, Alarme,1185
- Fehlersuche
  - Datenbankserver,
    - Anforderungsprotokollierung,317
  - debug\_messages-Option,602
  - Event-Handler,1095
  - Performance verschlüsselter Datenbanken,1433
  - SQL-Anweisungen in Interactive SQL,819
  - Webdienst-Clients,315
- Ferndatenzugriff
  - cis\_option-Option,589
  - cis\_rowset\_size-Option,589
  - unter Windows Mobile nicht unterstützt,423
- Festplatte voll
  - Fehler beim Schreiben in das Transaktionslog,139
- Festplatte, Sandboxing
  - Info,1411
- Festplatten
  - Fragmentierung und Performance,132,133
  - Wiederherstellung nach Plattenfehler,1047
- Festplattencache
  - Betriebssystem,296
- Festplattencontroller
  - Transaktionslog-Verwaltung,139
- Festplattenspeicher
  - Beispiel für ein Ereignis,1094
- Festplattenstörung
  - Info,1067
- Festschreibungen
  - cooperative\_commit\_timeout-Option,596
  - cooperative\_commits-Option,596
  - delayed\_commit\_timeout-Option,606
  - delayed\_commits-Option,606
- File, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- File-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- FileDataSourceName, Verbindungsparameter
  - Beschreibung,362
  - Datei-Datenquellen referenzieren,38
  - Windows Mobile,48
- FILEDSN, Verbindungsparameter
  - Beschreibung,362
  - Datei-Datenquellen referenzieren,38
  - Windows Mobile,48
- FILEDSN-Verbindungsparameter
  - Info,46
  - verbinden,20
- FileSize, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- FileSize-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Finder
  - Umgebungsvariablen setzen,468
- FIPS
  - ec, Datenbankserveroption,230
  - fips, Datenbankserveroption,237
  - dbinit -ea,927
  - FIPS-Protokolloption,404
  - Info,1445
  - SQL\_FLAGGER\_ERROR-Option,671
  - Unterstützung,1445
  - Verschlüsselung von Datenbankdateien,1001
  - Webdienste,310
- FIPS 140-2-Zertifizierung
  - Info,1445
- FIPS-Option
  - AES256\_FIPS-Verschlüsselungsalgorithmus,237
  - AES\_FIPS-Verschlüsselungsalgorithmus,237
  - Datenbankserveroption,237
- FIPS-Protokolloption
  - ec, Datenbankserveroption,230
  - Beschreibung,404
- FipsMode, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- FipsMode-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- fire\_triggers, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- fire\_triggers-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711

---

fire\_triggers-Option  
     Beschreibung,612  
 Firewalls  
     BroadcastListener-Protokolloption  
         (BLISTENER),391  
     ClientPort-Protokolloption (CPORT),395  
     Host-Protokolloption (IP),399  
     LDAP, Protokolloption,406  
     Serverauflistung, Dienstprogramm (dblocate),963  
     ServerPort-Protokolloption (PORT),416  
     überwinden,107  
     Verbinden mit LDAP,109  
 Firmennamen  
     Dienstprogramm zur Serverlizenzierung  
         (dblic),964  
 First-row, Optimierungsoption  
     optimization\_goal,647  
 first\_day\_of\_week, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 first\_day\_of\_week-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 first\_day\_of\_week-Option  
     Beschreibung,613  
 FirstOption, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 FirstOption-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 FIXED, Dateiformat  
     input\_format-Option,857  
     Interactive SQL, Ausgabe,866  
 Folgebytes  
     Info,500  
     Verbindungszeichenfolge,503  
 for\_xml\_null\_treatment, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 for\_xml\_null\_treatment-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 for\_xml\_null\_treatment-Option  
     Beschreibung,614  
 FORCE, Verbindungsparameter  
     Beschreibung,362  
 force\_view\_creation, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 force\_view\_creation-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 force\_view\_creation-Option  
     Beschreibung,614  
 ForceStart, Verbindungsparameter  
     Beschreibung,362  
 Format  
     Eingabedatei,857  
 Fragen  
     Zeichensätze,502  
 Fragmentierung  
     Performance,132,133  
 Frame-Typ  
     Info,98  
 FreeBuffers, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 FreeBuffers-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1234  
 FreePages, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 FreePages-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1248  
 Frei bestimmbare Zugriffssteuerung  
     Regeln für verschachtelte Ansichten und  
     Tabellen,1365  
 Führende Leerzeichen  
     in Verbindungszeichenfolgen verwenden,31  
 FullCompare, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
     Verbindungseigenschaft, Beschreibung,711  
 FullCompare-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 FunctionMaxParms, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 FunctionMinParms, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 FunctionName, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 Funktionen  
     Datenbankdokumentation erstellen,814  
     mit SQL Anywhere SNMP-Erweiterungsagenten  
     ausführen,1226  
 Funktionstasten  
     Interactive SQL,845

**G**

- Gemeinsam genutzter Speicher
  - Info,103
  - Unix-Konfiguration temporärer Dateien,476
- Generieren
  - RSA-Zertifikate,894
  - SQL-Anweisungen in Interactive SQL,829
- Geplante Ereignisse
  - Assistent Zeitplan erstellen,1090
  - Datenbankspiegelung,1476
  - Info,1089
  - Sommerzeit,1097
- Gesicherte Funktionen
  - aktivieren,1415
  - Funktionen, standardmäßig gesichert,1413
  - Info,1413
  - maximale Anzahl von Schlüsseln,791
  - mit -sf angeben,280
  - Schlüssel für gesicherte Funktionen mit -sk angeben,288
- Gespeicherte Prozeduren
  - Datenbankdokumentation erstellen,814
  - mit SQL Anywhere SNMP-Erweiterungsagenten ausführen,1226
  - Privilegien festlegen,1305
  - Sicherheitsfunktionen,1402
- Gesundheit und Statistik
  - anzeigen,812
- Gesundheit und Statistiken von Datenbanken anzeigen
  - Info,812
- GetData, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- GetData-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- GetTypeInfoChar, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- Gleichzeitige Verbindungen
  - Einstellung der maximalen Anzahl,244
- Global signierte Zertifikate
  - Transportschichtssicherheit,1451
- global\_database\_id, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- global\_database\_id-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- global\_database\_id-Option
  - Beschreibung,614
- GlobalAutoIncrement, Systemereignis
  - Beschreibung,1092
- GlobalDBID, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- GlobalDBID-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Globale Administratoren
  - Info,1293
  - MANAGE ROLES-Systemprivileg,1294
- Globale Prüfsummen
  - Info,1084
  - Validierung,1086
  - Validierungs-Dienstprogramm (dbvalid),1021
- Globale Zertifikate
  - als Serverzertifikat für Transportschichtssicherheit verwenden,1452
- go
  - Interactive SQL-Begrenzer,854
  - Syntax,819
- Grafische Pläne
  - Darstellung anpassen,840
  - erstellen,839
  - öffnen,839
  - speichern,839
- GRANT GROUP-Anweisung
  - Syntax (nicht mehr empfohlen),1393
- GRANT MEMBERSHIP IN GROUP-Anweisung
  - Syntax (nicht mehr empfohlen),1393
- GRANT REMOTE DBA-Anweisung (nicht mehr empfohlen)
  - stattdessen GRANT ROLE
  - SYS\_RUN\_REPLICATION\_ROLE
  - verwenden ,1400
- GRANT-Anweisung
  - Berechtigungen und Gruppen (nicht mehr empfohlen),1393
  - Vergleich der Syntax für Berechtigungen und Rollen,1391
- Groß-/Kleinschreibung
  - dbinit, Dienstprogramm,927
  - Initialisierungsdienstprogramm (dbinit),927
  - Türkische Datenbank, Groß-/Kleinschreibung berücksichtigen,532
  - Türkische Datenbank, Groß-/Kleinschreibung nicht berücksichtigen,534

---

## Groß-/Kleinschreibung berücksichtigen

- Befehlszeile, 212
- Datenbankname, 162
- Datenbankoptionen, 567
- internationale Aspekte, 505
- Protokolloptionen, 388
- Servername, 162
- Verbindungsparameter, 338

## GrowDB, Systemereignis

- Beschreibung, 1092

## GrowLog, Systemereignis

- Beispiel, 1093
- Beschreibung, 1092

## GrowTemp, Systemereignis

- Beschreibung, 1092

## Gruppen

- Abhängigkeiten definieren, 976
- Dienste, 190
- entziehen, REVOKE GROUP-Syntax (nicht mehr empfohlen), 1397
- entziehen, REVOKE MEMBERSHIP IN GROUP-Syntax (nicht mehr empfohlen), 1397
- erstellen, 1346
- erteilen, GRANT GROUP-Syntax (nicht mehr empfohlen), 1393
- erteilen, GRANT MEMBERSHIP IN GROUP-Syntax (nicht mehr empfohlen), 1393
- Info, 1346
- integrierte Login-Berechtigung erteilen, 52
- integrierte Logins erstellen (SQL), 55
- integrierte Logins erstellen (Sybase Central), 54
- integrierte Logins löschen (SQL), 57
- integrierte Logins löschen (Sybase Central), 56
- Login-Richtlinien können nicht abgeleitet werden, 535
- mit benutzererweiterten Rollen erzeugt, 1346
- mit eigenständigen Rollen erzeugt, 1346

## Gruppen-Abhängigkeiten

- einstellen, 976

## GSS-API, Bibliotheksdateien

- Kerberos, 64

## Guest, Benutzer

- einrichten, 61

# H

## Hardware

- Anforderungen, 794

## Hardwarespiegelung

- Transaktionslogs, 139

## HasCollationTailoring-Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- SQL Anywhere SNMP-Erweiterungsagent, OID, 1248

## HasEndianSwapFix, Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767

## HasEndianSwapFix-Eigenschaft

- SQL Anywhere SNMP-Erweiterungsagent, OID, 1248

## HashForcedPartitions, Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- Verbindungseigenschaft, Beschreibung, 711

## HashRowsFiltered, Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- Verbindungseigenschaft, Beschreibung, 711

## HashRowsPartitioned, Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- Verbindungseigenschaft, Beschreibung, 711

## HashWorkTables, Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- Verbindungseigenschaft, Beschreibung, 711

## HasNCHARLegacyCollationFix-Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767
- SQL Anywhere SNMP-Erweiterungsagent, OID, 1248

## HasTornWriteFix-Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767

## Hauptfenster

- Inhalt aktualisieren, 795

## Header

- hinzufügen, SQL-Anweisungen, 844

## HeapsCarver, Eigenschaft

- Servereigenschaft, Beschreibung, 745
- Verbindungseigenschaft, Beschreibung, 711

## HeapsCarver-Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767

## HeapsCarver-Statistik

- SQL Anywhere SNMP-Erweiterungsagent, OID, 1234, 1244

## HeapsLocked, Eigenschaft

- Servereigenschaft, Beschreibung, 745
- Verbindungseigenschaft, Beschreibung, 711

## HeapsLocked-Eigenschaft

- Datenbankeigenschaft, Beschreibung, 767

## HeapsLocked-Statistik

- SQL Anywhere SNMP-Erweiterungsagent,
  - OID,1234,1244
- HeapsQuery, Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- HeapsQuery-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- HeapsQuery-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1234,1244
- HeapsRelocatable, Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- HeapsRelocatable-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- HeapsRelocatable-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1234,1244
- Heimdal, Kerberos-Client
  - Unix-Unterstützung,64
- Herunterfahren
  - Zeitpunkt festlegen,294
- Hierarchie
  - Kopieknoten verschieben,1551
- Hintergrund
  - Datenbankserver ausführen,180
- Hinzufügen
  - RSA-Zertifikate,894
- Hiragana
  - Kollationsanpassung,523
- Histogramm, Dienstprogramm (dbhist)
  - Beendigungs\_codes,925
  - Syntax,923
- Histogramme
  - mit dbhist ansehen,923
- HKEY\_CURRENT\_USER
  - Registrierungseinträge,488
- HKEY\_LOCAL\_MACHINE
  - Registrierungseinträge,488
- Hochverfügbarkeit
  - Info,1467
  - MobiLink,1470
- Hohe Verfügbarkeit
  - Datenbankspiegelung,1467
  - Live-Sicherungen,1032
  - mit Webdiensten verwenden,1540
  - NodeType-Verbindungsparameter (NODE),375
- SQL Anywhere Veritas Cluster Server-
  - Agenten,1527
- Host, Protokolloption
  - IPv6-Adressen verwenden,107
- Host-Protokolloption
  - Beschreibung,399
- Host-Verbindungsparameter
  - Beschreibung,363
  - Fehlerbehandlung,87
  - Syntax,363
- HP-UX
  - IPv6-Unterstützung,106
  - SHLIB\_PATH-Umgebungsvariable,477
- HTML
  - in Interactive SQL anzeigen,843
- HTML, Dateiformat
  - Interactive SQL, Ausgabe,866
- HTTP
  - Client-APIs und Zeichensatzkonvertierung,505
  - Protokolloptionen,389
  - Server-Logformat,408
  - Serveranforderungen protokollieren,408
  - Serverkonfiguration,310
- http\_connection\_pool\_basesize-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- http\_connection\_pool\_basesize-Option
  - Beschreibung,615
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1253
- http\_connection\_pool\_timeout-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- http\_connection\_pool\_timeout-Option
  - Beschreibung,616
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1253
- http\_session\_timeout-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- http\_session\_timeout-Option
  - Beschreibung,617
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1253
- HttpAddresses, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- HttpAddresses-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1237
- HttpConnPoolCachedCount-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767

HttpConnPoolCachedCount-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 HttpConnPoolHits-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 HttpConnPoolHits-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 HttpConnPoolMisses-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 HttpConnPoolMisses-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 HttpConnPoolSteals-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 HttpConnPoolSteals-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 HttpNumActiveReq, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 HttpNumActiveReq-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpNumConnections, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 HttpNumConnections-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpNumSessions, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 HttpNumSessions-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpPorts-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HTTPS  
     Client-APIs und Zeichensatzkonvertierung,505  
     MobiLink-TLS für UltraLite-Clients,1464  
     MobiLink-Transportschichtssicherheit,1463  
     Protokolloptionen,389  
     Serverkonfiguration,310  
 HttpsAddresses-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpServiceName, Eigenschaft

    Verbindungseigenschaft, Beschreibung,711  
 HttpsNumActiveReq-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpsNumConnections-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 HttpsPorts-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237

## I

IANA  
     alternative Zeichensatzlabels,501  
     Portnummer,416  
 IANA-Labels  
     Zeichensätze,530  
 iAnywhere.mib  
     Beschreibung,1217  
     Info,1216  
     Speicherort,1230  
 IBM AIX  
     LDAP ausführen,112  
 ICU  
     alternative Zeichensatzlabels,501  
     feststellen, wenn ICU erforderlich ist,495  
     in Zeichensatzkonvertierung verwendet,502  
     Info,495  
     internationale Komponenten für Unicode,495  
     Syntax zum Anpassen,517  
     Unicode-Kollationsalgorithmus (UCA),516  
     unter Windows Mobile verwenden,430  
 ICU, Bibliothek  
     unter Windows Mobile vermeiden,442  
 ICU-Bibliothek  
     Datenbanken für Windows Mobile erstellen,442  
     eine Datenbank unter Windows Mobile  
     entladen,447  
 Identifizierung  
     Clientanwendungen,338  
 Identitätsdateien  
     Info,1454  
 Identity, Protokolloption  
     Beschreibung,402

- identity-Protokolloption
  - ec, Datenbankserveroption,230
- identity\_password, Protokolloption
  - Beschreibung,403
- identity\_password-Protokolloption
  - ec, Datenbankserveroption,230
- IdentitySignature, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- IdentitySignature-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Idle Time, Ereignistyp
  - abfragen,1096
- Idle-Verbindungsparameter
  - Beschreibung,365
- IdleCheck, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- IdleCheck-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- IdleChkpt, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- IdleChkpt-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- IdleChkTime, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- IdleChkTime-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- IdleTimeout-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
  - Verbindungseigenschaft, Beschreibung,711,745
- IdleWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- IdleWrite-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Impersonierung
  - ausführliche Erläuterung der Mindestkriterien,1360
  - GRANT SET USER erneut erteilen, um Einstellungen zu aktualisieren,1358
  - SET USER-Systemprivileg,1358
- Importieren
  - Verbindungsprofile,13
- IN, Schlüsselwort
  - CREATE TABLE-Anweisung,128
- In-Memory-Modus
  - Konfiguration,257
- Inaktiver Server
  - Beispiel für ein Ereignis,1094
- IndAdd, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- IndAdd-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Indizes
  - Einschränkungen,791
- IndLookup, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- IndLookup-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Information, Dienstprogramm (dbinfo)
  - Syntax,925
- Informationsdienstprogramm (dbinfo)
  - Beendigungscodes,927
- INI-Dateien
  - einfache Verschlüsselung hinzufügen mit dbfhide,922
  - Info,487
- Initialisieren
  - Datenbanken,121
- Initialisieren von Datenbanken mit dbinit
  - Info,927
- Initialisierung (dbinit), Dienstprogramm
  - Datenbanken für Windows Mobile erstellen,444
- Initialisierung der Benutzeroberfläche fehlgeschlagen
- UI (Typ 4)
  - Benutzeroberfläche unter Linux anzeigen,302
- Initialisierung, Dienstprogramm (dbinit)
  - Syntax,927
  - verwenden,126
- Initialisierungsdienstprogramm (dbinit)
  - Beendigungscodes,938
- InitString, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- Inkrementelle Sicherungen
  - Info,1031
  - Sicherungsdienstprogramm (dbbackup),1040
- INPUT-Anweisung
  - Format,857
  - in Interactive SQL neue Zeilen einfügen,832

---

    Einstellungen von Interactive SQL,851  

     Info,857  
 INSERT ANY TABLE-Systemprivileg  
     Beschreibung,1309  
 INSERT, Anweisung  
     in Interactive SQL generieren,829  
     kürzen von Zeichenfolgen,685  
 INSERT-Privileg  
     Info,1305  
 INSTALL JAVA-Anweisung  
     unter Windows Mobile nicht unterstützt,425  
 Installation  
     Registrierungseinstellungen,490  
     Speicherort,482  
     SQL Anywhere unter Windows Mobile,430  
     Windows Mobile,430  
 Installationsverzeichnis  
     Info,482  
     SQLANY16,477  
 Installieren  
     Monitor auf einem separaten Computer,1194  
 installulnet.exe  
     erweiterte Privilegien eventuell unter Windows 7  
         erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
         Server 2008 erforderlich,202  
     erweiterte Privilegien eventuell unter Windows  
         Vista und später erforderlich,202  
 INT, Verbindungsparameter  
     Beschreibung,366  
 INTEGRATED LOGIN-Privileg  
     Info,1305  
 Integrated, Verbindungsparameter  
     Beschreibung,366  
 integrated\_server\_name, Option  
     Domain Controller-Server für integrierte Logins  
         angeben,58  
     SQL Anywhere SNMP-Erweiterungsagent,  
         OID,1253  
 integrated\_server\_name-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 integrated\_server\_name-Option  
     Beschreibung,618  
 Integrierte Benutzerauthentifizierung  
     integrated\_server\_name-Option,618  
 Integrierte Logins  
     aktivieren,53  
     Betriebssysteme,52  
     Clientanwendungen,57  
     erstellen (SQL),55  
     erstellen (Sybase Central),54  
     Info,52  
     integrated\_server\_name-Option,618  
     login\_mode-Option,623  
     Netzwerkaspekte,61  
     Privilegien entziehen (SQL),57  
     Privilegien entziehen (Sybase Central),56  
     Sicherheitsfunktionen,75  
     Sicherheitsprobleme,62  
     Standardbenutzer,61  
     Verbindungen verhindern,59  
     Windows-Benutzergruppen,58  
 Integriertes Login erstellen, Assistent  
     verwenden,54  
 Integritätsregeln  
     Spalten und Tabellen,125  
     wählen,125  
 Interactive SQL  
     Abfrage-Editor anzeigen,845  
     alphabetische Liste der Interactive SQL-  
         Optionen,851  
     anpassen,817  
     Anweisungen abbrechen,828  
     Anweisungen ausführen,819  
     Anweisungen erneut aufrufen,822  
     Anweisungen protokollieren,826  
     Anweisungen stoppen,828  
     Anweisungen unterbrechen,828  
     ausgewählte Anweisungen ausführen,819  
     Befehlszeile,944  
     berechnete Spalten aktualisieren,832  
     berichtete Fehler,828  
     Bilder anzeigen,841  
     Check-In von Dateien,871  
     Check-Out von Dateien,871  
     Codepage zum Lesen und Schreiben von Dateien  
         angeben,856  
     Daten anzeigen,819  
     Datenbanken für Windows Mobile erstellen,445  
     dbisql-Syntax,939  
     Dienstprogramm (dbisql),939  
     Einzelschritt ausführen,819  
     Ergebnismenge sortieren,830  
     Favoriten,824

- Funktionstasten,845
- grafische Pläne,839
- Hardwareanforderungen für Mac OS X,814
- Header hinzufügen, SQL-Anweisungen,844
- HTML-Daten anzeigen,843
- Info,814
- mehrere Anweisungen ausführen,819
- mehrere Fenster öffnen,844
- mehrere Verbindungen,844
- mit authentifizierten Anwendungen verwenden,195
- mit Datenbanken verbinden (Linux),815
- mit Datenbanken verbinden (Mac OS X),815
- mit Datenbanken verbinden (Unix),815
- mit Datenbanken verbinden (Windows),815
- mit Datenbanken verbinden mit der Befehlszeile,815
- mit Datenbanken verbinden mit Sybase Central,815
- mit der Befehlszeile starten,815
- mit Sybase Central starten,815
- Optionen,851
- Optionen einstellen,851
- Prozeduren nachschlagen,828
- Schnelllader konfigurieren,876
- Skriptdateien ausführen,821
- Software-Updates,879
- Spalten nachschlagen,828
- SQL-Anweisungen,821
- SQL-Anweisungen Schritt für Schritt,819
- Standard-Editor für .sql-Dateien,817
- starten (Linux),815
- starten (Mac OS X),815
- starten (Unix),815
- starten (Windows),815
- Suchfunktion für Updates konfigurieren,880
- SVGs anzeigen,841
- Syntax,939
- Tabellen nachschlagen,828
- Tabellenbearbeitung deaktivieren,832
- Tabellenwerte bearbeiten,830
- Tastenkürzel,845
- Textvervollständigung,873
- unerwartete Symbole bei der Anzeige von Daten,504
- Verlauf, Fenster,822
- Versionsverwaltung konfigurieren,869
- Versionsverwaltungsintegration,868
- Versionsverwaltungsprojekte öffnen,871
- Warnmeldungen deaktivieren,817
- Windows Mobile, praktische Einführung,457
- XML-Daten anzeigen,843
- Zeilen einfügen,832
- Zeilen kopieren,834
- Zeilen löschen,833
- Zeilennummern,817
- Interactive SQL (dbisql), Dienstprogramm
  - Beendigungs\_codes,944
  - Syntax,939
  - über Datenquellen verbinden,20
  - unterstützte Plattformen,944
- Interactive SQL, Optionen
  - bell,854
  - command\_delimiter,854
  - echo,857
  - isql\_allow\_read\_client\_file,858
  - isql\_allow\_write\_client\_file,859
- Interactive SQL-Optionen
  - alphabetische Liste der Interactive SQL-Optionen,851
  - auto\_commit,853
  - auto\_refetch,853
  - commit\_on\_exit,855
  - default\_isql\_encoding,856
  - input\_format,857
  - isql\_command\_timing,859
  - ISQL\_ESCAPE\_CHARACTER,860
  - isql\_field\_separator,861
  - isql\_maximum\_displayed\_rows,862
  - isql\_print\_result\_set,863
  - isql\_quote,863
  - isql\_show\_multiple\_result\_sets,864
  - Klassifizierung,559
  - nulls,865
  - on\_error,865
  - output\_format-Option,866
  - output\_length,867
  - output\_nulls,867
  - truncation\_length,868
- Interna
  - Abfolgeplanung,1097
  - Ereignisse,1096
  - Event-Handler,1097
- Internationale Sprachen und Zeichensätze
  - Überblick,491
- Internationale Sprachunterstützung
  - Info,493

---

Interne Abläufe  
     Sicherungen,1075  
 Internes Entladen  
     Fehlerbehandlung,1016  
     verwenden,1014  
 Internet SCSI  
     Datenbankdateien speichern,136  
 IOParallelism, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 IOParallelism-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1248  
 IOToRecover, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 IOToRecover-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 IP, Protokolloption  
     IPv6-Adressen verwenden,107  
 IP-Adresse  
     von Windows Mobile-Geräten ermitteln,438  
 IP-Protokolloption  
     Beschreibung,399  
 IPAddressMonitorPeriod-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 IPv4  
     Info,105  
 IPv6  
     Info,106  
     mit BCAST-Protokolloption verwenden,107  
     mit Broadcast-Protokolloption verwenden,107  
     mit Host-Protokolloption verwenden,107  
     mit IP-Protokolloption verwenden,107  
     mit ME-Protokolloption verwenden,107  
     mit MyIP-Protokolloption verwenden,107  
     Schnittstellenbezeichner,107  
     Schnittstellennamen,107  
     unterstützte Plattformen,106  
 IQStore, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 IQStore-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1248  
 IsAesniAvailable-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 iSCSI  
     Datenbankdateien speichern,136  
 IsDebugger-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 IsFipsAvailable, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 IsFipsAvailable-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 IsIQ, Eigenschaft  
     Verbindungseigenschaft, Beschreibung,745  
 IsIQ-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 IsNetworkServer, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
 IsNetworkServer-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 isolation\_level, Option  
     Beschreibung,619  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
     Transact-SQL-Kompatibilität,560  
 isolation\_level-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 isolation\_level-Option  
     Sybase Open Client,1571  
 IsolationLevel, Verbindungsparameter  
     ODBC-Verbindungsparameter, Beschreibung,911  
 Isolationsstufen  
     einstellen,619  
     Spiegeldatenbanken abfragen,1473  
     Standardwert,619  
 IsPortableDevice-Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 isql\_allow\_read\_client\_file-Option  
     Einstellungen von Interactive SQL,851  
     Info,858  
 isql\_allow\_write\_client\_file-Option  
     Einstellungen von Interactive SQL,851  
     Info,859  
 isql\_command\_timing, Option  
     Einstellungen von Interactive SQL,851

- isql\_command\_timing-Option
  - Info,859
- isql\_escape\_character, Option
  - Einstellungen von Interactive SQL,851
- isql\_escape\_character-Option
  - Daten kopieren,834
  - Info,860
- isql\_field\_separator, Option
  - Einstellungen von Interactive SQL,851
- isql\_field\_separator-Option
  - Daten kopieren,834
  - Info,861
- isql\_maximum\_displayed\_rows, Option
  - Einstellungen von Interactive SQL,851
- isql\_maximum\_displayed\_rows-Option
  - Info,862
- isql\_print\_result\_set, Option
  - Einstellungen von Interactive SQL,851
- isql\_print\_result\_set-Option
  - Info,863
- isql\_quote, Option
  - Einstellungen von Interactive SQL,851
- isql\_quote-Option
  - Daten kopieren,834
  - Info,863
- isql\_show\_multiple\_result\_sets, Option
  - Einstellungen von Interactive SQL,851
- isql\_show\_multiple\_result\_sets-Option
  - Info,864
- IsRsaAvailable, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- IsRsaAvailable-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- IsRuntimeServer, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- IsRuntimeServer-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- IsService, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- IsService-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- J**
- JAVA**
  - alternative Zeichensatzlabels,501
  - Java
    - cp, Serveroption,225
    - java\_class\_path-Option,620
    - java\_location-Option,621
    - java\_vm\_options,622
  - Java in der Datenbank
    - cp, Serveroption,225
  - Java-Verzeichnis
    - Info,482
  - java\_class\_path-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - java\_class\_path-Option
    - Beschreibung,620
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - java\_location, Option
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - java\_location-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - java\_location-Option
    - Beschreibung,621
  - java\_main\_userid-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - java\_main\_userid-Option
    - Beschreibung,622
  - java\_vm\_options, Option
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - java\_vm\_options-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - java\_vm\_options-Option
    - Beschreibung,622
  - JavaVM, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - JavaVM-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
  - jConnect
    - Dienstprogramm zum Upgrade (dbupgrad),1018
    - eingeschränkte Funktionalität unter Windows Mobile,423
    - Initialisierung, Dienstprogramm (dbinit),927
    - Kerberos-Authentifizierung,69
    - TDS,1569
    - Windows Mobile,440
  - jConnect, Metadatenunterstützung

- 
- Windows Mobile,440
  - JDBC
    - ASE, Kompatibilitätsoptionen,559
    - Client-APIs und Zeichensatzkonvertierung,505
    - Kompatibilitäts-Datenbankoptionen,559
  - K**
  - Katakana
    - Kollationsanpassung,523
  - Keepalive-Anforderungen, Headerfeld
    - KeepaliveTimeout-Wert setzen,405
  - KeepaliveTimeout-Protokolloption
    - Beschreibung,405
  - Kennwortablauf
    - NewPassword-Verbindungsparameter,372
  - Kennwörter
    - Ablauf,372
    - authentifizieren,1411
    - Dienstprogrammdatenbank,147
    - für Dienstprogrammdatenbank einrichten,289
    - für Superuser,1406
    - in Sybase Central ändern,1367
    - Info,1367
    - Kennwortänderung mit Doppelkontrolle,1370
    - Länge,1406
    - Login-Richtlinien,535
    - maximale Länge,791
    - minimale Länge,637
    - mit Kennwortteilen ändern,1370
    - mit SQL ändern,1369
    - Monitor,1175
    - NEWPD-Verbindungsparameter,372
    - post\_login\_procedure-Option,651
    - PWD-Verbindungsparameter,378
    - Sicherheitsfunktionen,1410
    - Sicherheitstipps,1406
    - SQL Remote-Speicherung,668
    - SQL-Anweisungsverlauf,822
    - überprüfen,1411
    - verify\_password\_function-Option,704
    - verschlüsseln,358
  - Kennwörter für die Doppelkontrolle
    - festlegen,1370
    - Info,1370
    - Kennwortteile ändern,1370
  - Kennwortregeln
    - login\_procedure,625
    - verify\_password\_function-Option,704
  - Kennwortüberprüfung
    - Info,1411
  - Kerberos
    - krp-Option,261
    - Clients,64
    - CSFC5KTNNAME-Umgebungsvariable,64
    - einrichten,66
    - Fehlerbehandlung bei Verbindungen,73
    - GSS-API-Bibliothekskdateien,64
    - Info,63
    - jConnect-Verbindungen,69
    - Kerberos-Prinzipal,66
    - Kerberos-Verbindungsparameter (KRB),367
    - Key Distribution Center (KDC),66
    - Keytab-Dateien,64
    - KRB5\_KTNNAME-Umgebungsvariable,64
    - login\_mode-Option,623
    - Option -kl,260
    - Option -kr,262
    - Option -krb,263
    - Privileg entziehen,71
    - Privileg erteilen,70
    - Sicherheitsprobleme,62
    - SSPI unter Windows verwenden,72
    - Sybase Open Client-Verbindungen,69
    - temporäre Optionen,76
    - Ticket-erteilende Tickets,67
    - unter Windows Mobile nicht unterstützt,423
  - Kerberos, Key Distribution Center (KDC)
    - Info,66
  - Kerberos, Prinzipal
    - Info,66
  - Kerberos, Verbindungsparameter
    - Beschreibung,367
  - Kerberos-Authentifizierung
    - SSPI von SQL Anywhere-Clients unterstützt,64
    - SSPI von SQL Anywhere-Server nicht unterstützt,64
  - Kerberos-Login-Privilegien entziehen
    - Info,71
  - Kerberos-Login-Zuordnungen erstellen
    - Info,70
  - KERBEROS-Privileg
    - Info,1305
  - Kerne
    - vom Datenbankserver verwendete Anzahl festlegen,253

- Key Distribution Center
  - Kerberos-Authentifizierung verwenden,66
- KeysInSQLStatistics, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- Keytab-Dateien
  - Standardspeicherorte,64
- Kodieren
  - Zeichensätze,497
- Kodierung
  - Info,497
  - PKI-Objekte,903
- Kodierungen
  - für Mac OS X empfohlen,530
- Kollationen
  - Adaptive Server Enterprise-Kollationen,520
  - alternativ,518
  - ändern,527
  - CHAR-Kollation bestimmen,512
  - Datenbanken erstellen,522
  - für Mac OS X empfohlen,530
  - für Unix-Plattformen empfohlen,531
  - für Windows-Plattformen empfohlen,530
  - Info,497
  - Liste der unterstützten Kollationen,518
  - Mehrbyte,514
  - NCHAR-Kollation bestimmen,512
  - SQL Anywhere-Datenbanken,515
  - Standard,146
  - Standard bestimmen,527
  - Standard für deutsche Datenbanken,514
  - türkische Datenbanken,532
  - Unterschiede zwischen unterstützten türkischen Kollationen,534
  - wählen,522
  - während Initialisierung anpassen,927
  - Zeichen sortieren mit,514
- Kollationen wählen
  - Hinweise,522
  - Info,522
- Kollationsanpassung
  - beschränkte Unterstützung für Windows Mobile,439
  - dbinit, Dienstprogramm,927
  - Hiragana,523
  - Info,523
  - japanisch,523
  - Katakana,523
  - Optionen,523
  - schwedisch,523
- Kollationssequenzen
  - Initialisierung, Dienstprogramm (dbinit),927
- Kombinieren
  - mehrere Anweisungen in Interactive SQL,819
- Kommagetrennte Dateien
  - input\_format-Option,857
  - output\_format-Option,866
- Kommentare
  - Auditing,1417
- Kommerzielle Zertifizierungsstellen
  - Transportschichtssicherheit,1447
- Kommerzielles Und
  - in Konfigurationsdateien verwenden,882
- Kommunikation
  - ec, Serveroption,230
  - x, Datenbankserveroption,305
  - DatabaseKey-Verbindungsparameter (DBKEY),353
  - Encryption-Verbindungsparameter (ENC),359
  - Fehlerbehandlung,1113
  - Fehlersuche,312
  - Info,102
  - unterstützte,102
- Kommunikationskomprimierung
  - Compress-Verbindungsparameter (COMP),347
  - CompressionThreshold-Verbindungsparameter (COMPTH),348
- Kompatibilität
  - ANSI,559
  - SQL,559
  - Transact-SQL-Kompatibilitätsoptionen,559
- Kompatibilitätsoptionen
  - allow\_nulls\_by\_default,572
  - alphabetische Liste der Datenbank-Kompatibilitätsoptionen,559
  - ansi\_blanks,575
  - ansi\_close\_cursors\_on\_rollback,576
  - ansi\_permissions,577
  - ansi\_substring,578
  - ansinull,580
  - ASE, Kompatibilitätsoptionen,559
  - close\_on\_endtrans,590
  - continue\_after\_raisererror,594
  - conversion\_error,595
  - divide\_by\_zero\_error,609
  - escape\_character,609
  - fire\_triggers,612

- 
- isolation\_level,619
  - Klassifizierung,559
  - non\_keywords,641
  - on\_tsq\_error,646
  - quoted\_identifier,660
  - sql\_flagger\_error\_level,671
  - sql\_flagger\_warning\_level,672
  - string\_truncation,685
  - time\_format,690
  - timestamp\_format,692
  - Transact-SQL, Kompatibilitätsoptionen,560
  - tsql\_outer\_joins,699
  - tsql\_variables,699
  - Kompatibilitätsrollen
    - aus Berechtigungen migrieren,1386
    - Berechtigungen zuordnen,1386
    - Info,1275
    - Liste,1275
    - nach dem Löschen in Sybase Central wiederherstellen,1283
    - nach dem Löschen wiederherstellen ( SQL),1284
    - nach dem Migrieren in Sybase Central wiederherstellen,1283
    - nach dem Migrieren wiederherstellen (SQL),1284
    - Vererbung,1358
    - Zuordnung zu Berechtigungen vor Version 16.0,1275
  - Komprimieren
    - Pakete,272
  - Komprimierte Spalten
    - Info,124
  - Komprimierung
    - Performance,112
    - Spalten,124
    - Verschlüsselte Datenbankdateien,1424
  - Konfiguration von SQL Anywhere-Clients für Transportschichtssicherheit
    - Info,1463
  - Konfigurationsdateien
    - bedingte syntaktische Analyse,883
    - einfache Verschlüsselung hinzufügen mit dbfhide,922
    - Escapezeichen,883
    - Info,882
    - Option,214
    - verbergen,922
  - Konfigurieren
    - Datenbanken für Windows Mobile,439
    - ODBC-Datenquellen,41
    - Textvervollständigung,873
  - Konfigurieren von Datenquellen
    - mit dem ODBC-Datenquellen-Administrator,41
  - Konsolendienstprogramm (dbconsole)
    - Syntax,981
    - verwenden,877
  - Konsolidierte Datenbanken
    - Hochverfügbarkeit,1470
  - Konvertierung
    - PKI-Objekt-Kodierung,903
  - Kopieknoten
    - als Arbiter verwenden,1485
    - automatisch erstellen,1548
    - Info,1536
    - löschen,1552
    - manuell hinzufügen,1548
    - mehr untergeordnete Knoten als erwartet,1553
    - neuen übergeordneten Knoten zuweisen,1551
    - praktische Einführung,1556
    - Status der Transaktionslogverarbeitung,1553
    - übergeordnete Knoten automatisch zuweisen,1550
    - übergeordneten Knoten ermitteln,1551
    - Unterschiede zu Spiegelknoten,1539
    - Verbindungen,1545
    - Verbindungsparameter NodeType (NODE),375
    - Verlust von Verbindungen zu übergeordneten Knoten,1553
  - Kopieren
    - Datenbanken auf Ihr Windows Mobile-Gerät,446
    - Datenbankobjekte,795
    - Zeilen in Interactive SQL,834
  - Kopieren ausgewählter Zeilen
    - in Interactive SQL,834
  - Kopieren von Knoten
    - xp, Option,335
  - Kopierknoten
    - Login-Richtlinien verwalten,543
  - KRB, Verbindungsparameter
    - Beschreibung,367
  - KRB5\_KTNAME, Umgebungsvariable
    - Kerberos,64
  - KTO, Protokolloption
    - Beschreibung,405
  - Kurzeinführung
    - clientseitige Sicherungen,1028
    - serverseitige Sicherungen,1027
    - Sicherungen,1027
-

Kürzen

Zeichenfolgen,685

## L

Labels

Werte der Sprachen-Labels,510

Zeichensätze,530

Lang laufende Abfragen

mit -zp-Serveroption neueste Pläne erfassen,316

LANG, Verbindungsparameter

Beschreibung,368

Lange Servernamen

mit dblocate anzeigen,961

Language, Eigenschaft

Datenbankeigenschaft, Beschreibung,767

Servereigenschaft, Beschreibung,745

Language, Verbindungsparameter

Beschreibung,368

Language-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237,1248

Verbindungseigenschaft, Beschreibung,711

LastCheckpointTime-Eigenschaft

Datenbankeigenschaft, Beschreibung,767

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248

LastCommitRedoPos-Eigenschaft

Datenbankeigenschaft, Beschreibung,767

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248

Verbindungseigenschaft, Beschreibung,711

LastConnectionProperty, Eigenschaft

Servereigenschaft, Beschreibung,745

LastConnectionProperty-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237

LastDatabaseProperty, Eigenschaft

Servereigenschaft, Beschreibung,745

LastDatabaseProperty-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237

LastIdle, Eigenschaft

Verbindungseigenschaft, Beschreibung,711

LastOption, Eigenschaft

Servereigenschaft, Beschreibung,745

LastOption-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237

LastPlanText, Eigenschaft

Verbindungseigenschaft, Beschreibung,711

LastReqTime, Eigenschaft

Verbindungseigenschaft, Beschreibung,711

LastServerProperty, Eigenschaft

Servereigenschaft, Beschreibung,745

LastServerProperty-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237

LastStatement, Eigenschaft

Verbindungseigenschaft, Beschreibung,711

LastSyncedRedoPos-Eigenschaft

Datenbankeigenschaft, Beschreibung,767

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248

LastWrittenRedoPos-Eigenschaft

Datenbankeigenschaft, Beschreibung,767

SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248

LazyAutocommit, Verbindungsparameter

ODBC-Verbindungsparameter, Beschreibung,911

LazyClose, Verbindungsparameter

Beschreibung,369

LCLOSE, Verbindungsparameter

Beschreibung,369

LD\_LIBRARY\_PATH, Umgebungsvariable

Beschreibung,469

LDAP

AIX,109

Benutzer authentifizieren,63

LDAP-Protokolloption,406

LDAPUA, login\_mode-Option,623

Serverauflistung, Dienstprogramm (dblocate),963

unter Windows Mobile nicht unterstützt,423

Unterschiede zwischen Personal Server und  
Netzwerkserver,151

LDAP-Benutzerauthentifizierung

login\_mode-Option,623

LDAP-Namensserver

LDAP-Protokolloption,406

saldap.ini,109

unter IBM AIX ausführen,112

Verbindung herstellen,109

LDAP-Protokolloption

Beschreibung,406

LDAP-Systemprivileg

Beschreibung,1309  
 LDAPUA  
   login\_mode-Option,623  
 Leerstellen  
   Verbindungszeichenfolgen,36  
 Leerzeichen  
   ANSI-Verhalten,575  
 Leerzeichen auffüllen  
   Initialisierung, Dienstprogramm (dbinit),927  
 LegalCopyright, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LegalCopyright-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 LegalTrademarks, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LegalTrademarks-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 Lesen  
   TLS-Zertifikate,903  
 LF, Protokolloption  
   Beschreibung,408  
 LIBPATH, Umgebungsvariable  
   Beschreibung,470  
 LicenseCount, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LicenseCount-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 LicensedCompany, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LicensedCompany-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 LicensedUser, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LicensedUser-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 LicenseKey-Eigenschaft  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 LicenseType, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 LicenseType-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 LINKS, Verbindungsparameter  
   Beschreibung,345  
   Klammern,503  
   Optionen,103  
 LINKS-Verbindungsparameter  
   IPv6-Adressen,106  
 Linux  
   Anzeigen von Servermeldungen, das Fenster  
   Server-Startoptionen,300  
   asynchrone I/O-Vorgänge deaktivieren,297  
   Dienstprogramm dbconsole starten,877  
   Fenster Server-Startoptionen verwenden,302  
   Interactive SQL starten,815  
   IPv6-Unterstützung,106  
   LD\_LIBRARY\_PATH-Umgebungsvariable,469  
   Meldungsfenster des Datenbankservers  
   anzeigen,302  
   Schnittstellenbezeichner für IPv6-Adressen  
   erforderlich,107  
   SELinux-Richtlinien,1403  
   Servermeldungen im Shell-Modus anzeigen,297  
   Sybase Central starten,5  
   Thread-Verhalten,173  
   Verbindung mit der Beispieldatenbank herstellen,7  
 Linux-Dienste  
   Datenbankserver,180  
 Listen  
   Überwachung von Datenbankoptionen,569  
 Live-Sicherung  
   durchführen,1032  
 Live-Sicherungen  
   Datenbanken neu starten,1052  
   erstellen,1044  
   Info,1032  
   Unterschiede zu Transaktionslog-  
   Spiegeldateien,1033  
 LivenessTimeout-Eigenschaft  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
   Verbindungseigenschaft, Beschreibung,711  
 LivenessTimeout-Verbindungsparameter  
   Beschreibung,370  
 Lizenzdateien  
   Info,966  
 Lizenzen

- mit Serverlizenzierungs-Dienstprogramm hinzufügen (dblic),964
- Lizenzierung
  - Auswirkung auf Serveroption -gm,244
  - Auswirkung auf Serveroption -gt,251
  - Auswirkung auf Serveroption -gta,252
  - Auswirkung auf Serveroption -gtc,253
  - Auswirkungen auf Threading,174
  - Perseat-Lizenzen,964
  - Programme,966
  - Prozessor-Lizenzen,964
  - Serverlizenzierung (dblic), Syntax,964
  - Unterschiede zwischen Personal Server und Netzwerkserver,151
  - Verbindungsbegrenzung und Event-Handler,1097
- Lizenztyp
  - Dienstprogramm zur Serverlizenzierung (dblic),964
- LO-Protokolloption
  - Beschreibung,407
- LOAD ANY TABLE-Systemprivileg
  - Beschreibung,1309
- LOAD TABLE-Anweisung
  - Sicherheit,1408
- Local Machine
  - Umgebungseinstellungen,488
- localhost
  - Angabe von,435
  - Host-Protokolloption (IP),399
  - Proxy-Port,437
  - Verbindungsparameter Host,363
  - Verbindungsszenarien,32
- LocalOnly, Protokolloption
  - Beschreibung,407
- LocalSystem, Konto
  - Info,182
  - Optionen,187
- Location, Registrierungseintrag
  - Dateisuche unter Windows,484
- LOCK TABLE-Anweisung
  - blocking\_others\_timeout-Option,586
- lock\_rejected\_rows, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- lock\_rejected\_rows-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockCount, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LockCount-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockCount-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- LockedCursorPages, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- LockedCursorPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- LockedHeapPages, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- LockedHeapPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- LockIndexID, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockName, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockRowID, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockTableOID-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LockTablePages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LockTablePages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- LOG, Protokolloption
  - Beschreibung,408
- LOG, Verbindungsparameter
  - Beschreibung,371
- Log-Viewer
  - Info,805
  - Meldungen konfigurieren,805
  - Meldungsdetails anzeigen,805
  - öffnen,805
- log\_deadlocks, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- log\_deadlocks-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- log\_deadlocks-Option
  - Beschreibung,623
- Logdateien
  - Auditing,1418
  - Checkpoint-Log,143
  - Datenbankserver-Meldungslog,163

---

- Datenbankspiegelung,1484
- echo-Option,857
- Transaktion,135
- Transaktionslog-Dienstprogramm (dblog),998
- Transaktionslog-Spiegel,138
- zurücksetzen,1079
- LogDiskSpace, Systemereignis
  - Beschreibung,1092
- Logeinträge
  - suchen,805
- LogFile, Protokolloption
  - Beschreibung,408
- LogFile, Verbindungsparameter
  - Beschreibung,371
- LogFileFragments, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LogFileFragments-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- LogFormat, Protokolloption
  - Beschreibung,408
- LogFreeCommit, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LogFreeCommit-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LogFreeCommit-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Login-Modi
  - integrierte Windows-Logins,52
  - login\_mode-Option,623
- Login-Prozeduren
  - ausgeführt für Webdienste,626
  - Info,625
- Login-Richtlinien
  - ändern,541
  - automatisches Entsperren von Benutzerkonten,544
  - bestehenden Benutzern zuordnen,541
  - erstellen,540
  - Info,535
  - löschen,542
  - Richtlinienoptionen in der Root-Richtlinie außer Kraft setzen,535
  - Root-Login-Richtlinie,535
  - Root-Richtlinie ändern,541
  - schreibgeschützte Datenbanken,543
  - von der Root-Richtlinie ableiten,536
- Login-Richtlinien für einzelne Benutzer
  - Entladen(dbunload), Dienstprogramm,1013
- Login-Richtlinien verwalten
  - Info,535
  - schreibgeschützte Datenbanken,543
- Login-Zuordnungen
  - Integrierte Logins,52
  - Kerberos,63
- login\_mode, Option
  - integrierte Logins,53
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- login\_mode-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- login\_mode-Option
  - Beschreibung,623
  - Integrated-Verbindungsparameter (INT),366
- login\_procedure, Option
  - Kennwortablauf implementieren,1411
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Verbindungen mit RAISERROR sperren,626
- login\_procedure-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- login\_procedure-Option
  - Beschreibung,625
- Logins
  - integrierte,52
  - Kerberos,63
- LoginTime, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- LogMaxSize, Protokolloption
  - Beschreibung,410
- LogMirrorName, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LogMirrorName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- LogName, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- LogName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- LogOptions, Protokolloption
  - Beschreibung,410
- LogWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- LogWrite-Statistik

- SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Lokalisierte Versionen von SQL Anywhere Info,493
- LOPT, Protokolloption Beschreibung,410
- Löschen
  - Datenbankdateien,149
  - Datenbanken,149
  - Datenbanken (Befehlszeile),149
  - Datenbanken (Sybase Central),149
  - DBSpaces,134,135
  - DBSpaces (SQL),135
  - DBSpaces (Sybase Central),134
  - Dienste,974
  - Linux, Dienste,968
  - Löschen-Dienstprogramm (dberase),916
  - Windows Mobile-Datenbanken mit dem Windows-Explorer,450
  - Windows Mobile-Datenbanken über die Benutzeroberfläche des Geräts,450
- Löschen von Login-Richtlinien Info,542
- Löschen, Dienstprogramm verwenden,149
- Löschen, Dienstprogramm (dberase) verwenden,149
- Löschen-Dienstprogramm (dberase)
  - Beendigungscodes,918
  - Syntax,916
- Löschungen
  - ANSI-Verhalten,577
  - Transact-SQL-Privilegien,577
- LSIZE, Protokolloption Beschreibung,410
- LTMGeneration, Eigenschaft Datenbankeigenschaft, Beschreibung,767
- LTMGeneration-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- LTMTrunc, Eigenschaft Datenbankeigenschaft, Beschreibung,767
- LTMTrunc-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- LTO, Verbindungsparameter Beschreibung,370

## M

- Mac OS X
  - Beispiele,468
  - Dateien als Source nehmen,468
  - dbconsole-Dienstprogramm starten,877
  - Dienstprogramm dbconsole, Hardwareanforderungen,877
  - DYLD\_LIBRARY\_PATH-Umgebungsvariable,469
  - empfohlene Kollationen,530
  - Interactive SQL starten,815
  - Interactive SQL, Hardwareanforderungen,814
  - IPv6-Unterstützung,106
  - Konfigurieren von Beispielen,468
  - ODBC-Datenquellen erstellen,45
  - Servermeldungen anzeigen,300
  - Sybase Central starten,5
  - Sybase Central, Hardwareanforderungen,5
  - Umgebungsvariablen setzen,467
  - Verbindung mit der Beispieldatenbank herstellen,9
- MachineName, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- MachineName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- MAGIC
  - user\_estimates-Option,702
- MainHeapBytes, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- MainHeapBytes-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- MainHeapPages, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- MainHeapPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- MANAGE ANY DBSPACE-Systemprivileg Beschreibung,1309
- MANAGE ANY EVENT-Systemprivileg Beschreibung,1309
- MANAGE ANY EXTERNAL ENVIRONMENT-Systemprivileg Beschreibung,1309
- MANAGE ANY EXTERNAL OBJECT-Systemprivileg Beschreibung,1309

---

MANAGE ANY LDAP SERVER-Systemprivileg	manage_server-Funktion
Beschreibung, 1309	-sf, Serveroption, 280
MANAGE ANY LOGIN POLICY-Systemprivileg	Manager
Beschreibung, 1309	Info, 1217
MANAGE ANY MIRROR SERVER-Systemprivileg	MapPhysicalMemoryEng, Eigenschaft
Beschreibung, 1309	Servereigenschaft, Beschreibung, 745
MANAGE ANY OBJECT PRIVILEGE-Systemprivileg	MapPhysicalMemoryEng-Statistik
Beschreibung, 1309	SQL Anywhere SNMP-Erweiterungsagent, OID, 1234
MANAGE ANY SPATIAL OBJECT-Systemprivileg	Massenimport von Daten
Beschreibung, 1309	Optionen, 170
MANAGE ANY STATISTICS-Systemprivileg	Massenmaterialisierungsvorgänge
Beschreibung, 1309	-b-Serveroption, 216
MANAGE ANY TRACE SESSION-Systemprivileg	Materialisierte Ansichten
Beschreibung, 1309	materialized_view_optimization-Option, 628
MANAGE ANY USER-Systemprivileg	max_client_statements_cached-Option, 629
Beschreibung, 1309	materialized_view_optimization, Option
MANAGE ANY WEB SERVICE-Systemprivileg	SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
Beschreibung, 1309	materialized_view_optimization-Eigenschaft
MANAGE AUDITING-Systemprivileg	Verbindungseigenschaft, Beschreibung, 711
Beschreibung, 1309	materialized_view_optimization-Option
MANAGE CERTIFICATES-Systemprivileg	Beschreibung, 628
Beschreibung, 1309	MatView-Verbindungsparameter
MANAGE PROFILING-Systemprivileg	Beschreibung, 374
Beschreibung, 1309	max_client_statements_cached, Option
MANAGE REPLICATION-Systemprivileg	SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
Beschreibung, 1309	max_client_statements_cached-Eigenschaft
MANAGE ROLES-Systemprivileg	Verbindungseigenschaft, Beschreibung, 711
Beschreibung, 1309	max_client_statements_cached-Option
Rollen erteilen, 1294	Beschreibung, 629
manage_disk_sandbox	mit clientseitigem Caching von Anweisungen verwenden, 631
gesicherte Funktion, 1413	max_cursor_count, Option
manage_disk_sandbox-Funktion	SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
-sf, Serveroption, 280	max_cursor_count-Eigenschaft
manage_features	Verbindungseigenschaft, Beschreibung, 711
gesicherte Funktion, 1413	max_cursor_count-Option
manage_features-Funktion	Beschreibung, 631
-sf, Serveroption, 280	max_hash_size, Option
manage_keys	SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
gesicherte Funktion, 1413	max_hash_size-Eigenschaft
manage_keys-Funktion	Verbindungseigenschaft, Beschreibung, 711
-sf, Serveroption, 280	max_plans_cached, Option
manage_security	Beschreibung, 632
gesicherte Funktion, 1413	
manage_security-Funktion	
-sf, Serveroption, 280	
manage_server	
gesicherte Funktion, 1413	

- SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_plans\_cached-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_priority, Option
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_priority-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_priority-Option
  - Beschreibung,632
- max\_query\_tasks, Option
  - Beschreibung,633
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_query\_tasks-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_recursive\_iterations, Option
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_recursive\_iterations-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_recursive\_iterations-Option
  - Beschreibung,634
- max\_retry\_connect\_time-Option
  - verwenden,1553
- max\_statement\_count, Option
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_statement\_count-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_statement\_count-Option
  - Beschreibung,635
- max\_temp\_space, Option
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253
- max\_temp\_space-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- max\_temp\_space-Option
  - Beschreibung,636
- MaxCacheSize, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- MaxCacheSize-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234
- MAXCONN, Protokolloption
  - Beschreibung,412
- MaxConnections, Protokolloption
  - Beschreibung,412
- MaxConnections-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- MaxEventType-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- Maximum
  - Datenbankdateigröße,791
  - Datenbankgröße,791
- MaxIO, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MaxIO-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1244
- MaxMessage-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- MaxMultiProgrammingLevel-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- MaxRead, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MaxRead-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1244
- MaxRemoteCapability, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- MaxRemoteCapability-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- MaxRequestSize, Protokolloption
  - Beschreibung,412
- MaxRequestVars-Protokolloption
  - Beschreibung,413
- MAXSIZE, Protokolloption
  - Beschreibung,412
- MAXVARS-Protokolloption
  - Beschreibung,413
- MaxWrite, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MaxWrite-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1244

---

ME, Protokolloption  
 Beschreibung,414  
 IPv6-Adressen verwenden,107

Mehrbyte, Zeichensätze  
 Info,500  
 verwenden,514

Mehrere Ergebnismengen  
 Interactive SQL-Optionen,864  
 isql\_show\_multiple\_result\_sets,864

Mehrfachprozessorsysteme  
 Thread-Verhalten steuern,171

Mehrprozessor, Support  
 Serveroptionen,167  
 Thread-Verhalten steuern,171

Meldungen  
 Änderungen der Multiprogramming-Stufe,248  
 Log-Viewer-Liste konfigurieren,805

Meldungen zum Verarbeitungsfortschritt  
 Dienstprogrammdatenbank,658

Meldungsfenster des Datenbankservers  
 anzeigen,273  
 maximiert belassen,274  
 Statistik zur Multiprogramming-Stufe,248

Meldungslog  
 für Datenbankserver konfigurieren,163  
 im Monitor anzeigen,1132  
 Info,163  
 Performancewarnungen des  
 Datenbankservers,1110

MESSAGE, Anweisung  
 Option debug\_messages festlegen,602

Message-Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237

MessageCategoryLimit-Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237

MessageReceived-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

MessageText, Eigenschaft  
 Servereigenschaft, Beschreibung,745

MessageText-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237

MessageTime, Eigenschaft  
 Servereigenschaft, Beschreibung,745

MessageTime-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237

MessageWindowSize, Eigenschaft  
 Servereigenschaft, Beschreibung,745

MessageWindowSize-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237

Metadatentabellen  
 SQL Anywhere MIB-Datenbank,1231

Metriken  
 Monitor,1149

MIB-Datenbanken  
 von SQL Anywhere SNMP-Erweiterungsagent  
 unterstützt,1217

MIBs  
 Definition,1217

Microsoft Access  
 TIMESTAMP-Vergleich,605

MIME  
 alternative Zeichensatzlabels,501

min\_password\_length, Option  
 Kennwortsicherheit erhöhen,1410  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253

min\_password\_length-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

min\_password\_length-Option  
 Beschreibung,637

min\_role\_admins-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

min\_role\_admins-Option  
 Beschreibung,638  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253

MinCacheSize, Eigenschaft  
 Verbindungseigenschaft, Beschreibung,745

MinCacheSize-Statistik  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1234

Mindestanforderungen  
 Hardware,794

Mindestkriterien  
 Info,1358

Mindestkriterien, Impersonierung  
 ausführliche Erläuterung,1360

MinMultiProgrammingLevel-Eigenschaft  
 Servereigenschaft, Beschreibung,745

- SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- MirrorFailover, Systemereignis
  - Beschreibung,1093
  - verwenden,1093
- MirrorMode, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MirrorMode-Eigenschaft
  - Datenbankspiegelungs-Synchronisationsmodus ermitteln,1478
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- MirrorRole-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- MirrorServerDisconnect, Systemereignis
  - Beschreibung,1093
  - verwenden,1093
- MirrorServerName, Parameter
  - verwenden,1489
- MirrorServerState-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- MirrorServerWaits-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MirrorServerWaits-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- MirrorState, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- MirrorState-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- Mit einer laufenden Datenbank auf diesem Computer verbinden
  - Verbinden-Fenster,14
- Mit einer laufenden Datenbank auf einem anderen Computer verbinden
  - Verbinden-Fenster,14
- Mit einer ODBC-Datenquelle verbinden
  - Beispieldatenbank-Fenster,30
  - Verbinden-Fenster,14
- MIT, Kerberos-Client
  - Unix-Unterstützung,64
  - Windows-Unterstützung,64
- Mithilfe einer Verbindungszeichenfolge verbinden
  - Verbinden-Fenster,14
- ml\_remote\_id-Option
  - Beschreibung,639
- mlasinst, Dienstprogramm
  - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
  - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
- mlsrv16
  - Ausführung als Linux-Dienst,968
  - Ausführung als Windows-Dienst,974
  - Lizenzierung,964
  - mit Transportschichtsicherheit starten,1460
- MobiLink
  - Datenbankoptionen,562
  - Hochverfügbarkeit,1470
- MobiLink, Transportschichtsicherheit
  - Info,1444
- MobiLink-Client/Server-Kommunikation verschlüsseln
  - Info,1458
- MobiLink-Clients
  - Datenbankoptionen,562
- MobiLink-Clients konfigurieren, für die Verwendung von Transportschichtsicherheit
  - Info,1461
- MobiLink-Dienstprogramme
  - Erstellen von Zertifikaten (createcert), Syntax,894
  - Syntax zum Anzeigen von Zertifikaten (viewcert),903
- MobiLink-Server
  - überwachen,1135
- MobiLink-Server starten
  - Transportschichtsicherheit,1460
- MobiLink-Server überprüfen
  - MobiLink-Transportschichtsicherheit,1461
- MobiLink-Serverfarm
  - überwachen,1115
- MobiLink-Serverfarmen
  - überwachen,1137
- MobiLink-Serverüberwachung
  - Info,1115
- MobiLink-Synchronisation
  - default\_timestamp\_increment einstellen,605
  - Sicherungen,1068
  - truncate\_timestamp\_values einstellen,698

- 
- Modi
    - SQL Anywhere 16-Plug-In,808
    - Synchronisation in der Datenbankspiegelung,1477
  - Monitor
    - Abmelden ,1123
    - Admin-Benutzer,1176
    - Administration-Fenster,1131
    - Alarm-Definitionen und -Schwellenwerte,1186
    - Alarm-E-Mails,1189
    - Alarm-Schwellenwerte,1184
    - Alarmer,1181
    - Alarmschweregrad,1125
    - Alarmsymbole,1125
    - Anforderungen,1117
    - auf einem separaten Computer installieren,1194
    - Ausnahmebedingungsberichte,1132
    - Benutzertypen,1175
    - Blackouts,1145
    - Dashboard-Vorlagen,1127
    - Dashboards,1126
    - E-Mail-Benachrichtigung,1188
    - Einschränkungen,1118
    - Fehlerbehandlung,1198
    - FIPS,1197
    - Info,1115
    - installierte Objekte,1193
    - Installierte Objekte löschen,1194
    - Meldungslog,1132
    - Metriken,1149
    - Metriken - MobiLink,1153
    - Metriken - MobiLink-Serverfarm,1162
    - Metriken exportieren,1174
    - Metrikenliste,1150
    - migrieren und Upgrade,1197
    - praktische Einführung,1200
    - Produktionsumgebung,1194
    - Relay Server-Farm, Metrikenliste,1171
    - Ressourcen,1132
    - Sammlungsintervalle,1173
    - samonitor.bat,1120
    - samonitor.sh,1120
    - sichern,1191
    - SQL Anywhere, Metrikenliste,1150
    - starten,1120
    - Stopp der Ressourcenüberwachung,1144
    - stoppen,1121
    - TLS-Kommunikationsverschlüsselung,1197
    - Übersicht, Dashboard,1124
    - Überwachungsstatus,1125
    - Verbindungen schließen,1130
    - von einem entfernten Computer aus anmelden,1122
    - Widgets,1127
    - Zeit,1131
  - Monitor Production Edition
    - installieren (Linux),1196
    - installieren (Windows),1195
  - Monitor, installierte Objekte
    - Monitor, Fehler beheben,1147
  - MONITOR-Systemprivileg
    - Beschreibung,1309
  - Multi-Tasking
    - Thread-Verhalten steuern,171
  - MultiByteCharSet, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - MultiByteCharSet-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
  - Multicast, Adressen
    - IPv6-Unterstützung,107
  - MultiPacketsReceived, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - MultiPacketsReceived-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
  - MultiPacketsSent, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - MultiPacketsSent-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
  - MultiPageAllocs, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - MultiPageAllocs-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
  - Multiprogramming Stufe
    - manuell anpassen,179
  - Multiprogramming-Stufe
    - automatische Anpassungsinformationen anzeigen,248
    - automatische Optimierung,175
    - Datenbankserver,175
    - dynamische Optimierung,245
    - erhöhen,178
    - Optimierung,176
    - vermindern,179

MultiProgrammingLevel-Eigenschaft  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1237  
  Verbindungseigenschaft, Beschreibung,745

MyIP, Protokolloption  
  Beschreibung,414  
  IPv6-Adressen verwenden,107

## N

Nach Software-Updates suchen  
  Info,879

Nach Updates suchen  
  Info,879

Nachgestellte Leerzeichen  
  in Verbindungszeichenfolgen verwenden,31

Nachrichten  
  Datenbankserver-Performance,1110  
  Sprachen-Ressourcebibliothek,498

Nachrichtenagent (dbremote)  
  Transaktionslogverwaltung,1069

Nachrichtenverbindungsparameter  
  SQL Remote, external\_remote\_options,611

Nachschlagen  
  Prozeduren in Interactive SQL,828  
  Spalten in Interactive SQL,828  
  Tabellen in Interactive SQL,828

Name  
  in MobiLink-Transportschichtssicherheit  
  überprüfen,1462

Name, Eigenschaft  
  Datenbankeigenschaft, Beschreibung,767  
  Verbindungseigenschaft, Beschreibung,711,745

Name-Eigenschaft  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1237,1248

Namen  
  Datenbank,328  
  Verbindungen,349

NAS  
  Datenbankdateien speichern,136

Nationale Sprachunterstützung  
  Info,493

  Mehrbyte-Zeichensätze,514

NativeProcessorArchitecture, Eigenschaft  
  Verbindungseigenschaft, Beschreibung,745

NativeProcessorArchitecture-Eigenschaft

  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1237

Navigation in der Plananzeige  
  Info,839

NCHAR-Datentyp  
  Kollationssequenzen,927

NCHAR-Kollation  
  Info,515

nchar\_charset  
  Info,500

nchar\_charset, Alias  
  Info,501

NcharCharSet, Eigenschaft  
  Datenbankeigenschaft, Beschreibung,767  
  Verbindungseigenschaft, Beschreibung,711

NcharCharSet-Eigenschaft  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1248

NcharCollation-Eigenschaft  
  Datenbankeigenschaft, Beschreibung,767  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1248

NDS  
  Dateinamen,167  
nearest\_century, Option  
  SQL Anywhere SNMP-Erweiterungsagent,  
  OID,1253  
  Transact-SQL-Kompatibilität,560

nearest\_century-Eigenschaft  
  Verbindungseigenschaft, Beschreibung,711

nearest\_century-Option  
  Beschreibung,640

Negative Privilegien  
  nicht unterstützt,1348

net.cfg  
  Fehlerbehandlung bei Client/Server-  
  Kommunikation,98

Network Attached Storage (NAS)  
  Datenbankdateien speichern,136

Netzwerk-Protokolloptionen  
  alphabetische Liste,388

Netzwerkkommunikation  
  Datei sasrv.ini,95  
  Fehlersuche bei Startproblemen,1110

Netzwerkprotokolle  
  -x, Datenbankserveroption,305  
  alphabetische Liste,388  
  Clientoptionen,388

- 
- Fehlerbehandlung,1113
  - Info,102
  - unterstützte,102
  - Netzwerkserver
    - Einstellungen der Multiprogramming-Stufe,177
    - Info,150
    - Softwareanforderungen,151
    - Transportschichtsicherheit,1454
    - Unterschiede zum Personal Server,151
    - unterstützte Kommunikationsprotokolle,103
  - Netzwerkserver, Monitor
    - Syntax,981
    - verwenden,877
  - Netzwerktreiber
    - Datenbankdateien,213
  - Netzwerkverbindungen
    - Befehlszeilenooptionen,388
    - Fehlersuche,1113
    - Optionen,103
  - Neu aufbauen
    - Datenbanken unter Windows Mobile,447
    - Windows Mobile-Datenbanken,447
  - Neu starten
    - SNMP-Dienst,1221
    - SQL Anywhere SNMP-Erweiterungsagent,1221
  - Neuerstellung
    - authentifizierte Datenbanken,200
  - NewPassword, Verbindungsparameter
    - Kennwortablauf einrichten,1411
  - NewPassword-Verbindungsparameter
    - Beschreibung,372
  - NEWPWD, Verbindungsparameter
    - Kennwortablauf einrichten,1411
  - NEWPWD-Verbindungsparameter
    - Beschreibung,350,372,375
  - NextScheduleTime, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
  - Nicht eingesandte Fehlerberichte
    - anzeigen,1108
  - Nicht festgeschriebene Transaktionen
    - mit der Befehlszeile wiederherstellen,1048
    - mit Sybase Central wiederherstellen,1048
  - Nicht geplante Anforderungen
    - Info,175
  - Nicht geplante Aufgaben
    - Info,175
  - Nicht unterstützte Funktionen
    - SQL Anywhere-Einschränkungen unter Windows Mobile,423
  - Nicht verkettet, Modus
    - chained-Option,587
  - Nicht-englische Datenbanken
    - erstellen,522
  - Nie-Schreiben-Modus
    - Datenbankserver,257
  - NIST
    - FIPS-Zertifizierung,1445
  - NodeAddress-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - non\_keywords, Option
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
    - Transact-SQL-Kompatibilität,560
  - non\_keywords-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - non\_keywords-Option
    - Beschreibung,641
  - NOTIFY TRACE EVENT-Systemprivileg
    - Beschreibung,1309
  - NULL
    - für Export definieren,867
    - in Spalten zulassen,122
    - nulls-Option,865
    - Transact-SQL,580
  - nulls, Option
    - Einstellungen von Interactive SQL,851
  - nulls-Option
    - Info,865
  - Number-Eigenschaft
    - Verbindungs-ID abrufen,31
    - Verbindungseigenschaft, Beschreibung,711
  - NumLocalTempTables-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - NumLogicalProcessors, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - NumLogicalProcessors-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
  - NumLogicalProcessorsUsed, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - NumLogicalProcessorsUsed-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
  - Nummerische Gesamtstellenzahl

- Datenbankoption,653
- NumPhysicalProcessors, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- NumPhysicalProcessors-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- NumPhysicalProcessorsUsed, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- NumPhysicalProcessorsUsed-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- Nur-Checkpoint-Modus
  - Datenbankserver,257
- Nutzungsinformationen
  - anzeigen,216

**O**

- Obere Codepage
  - Info,499
- ObjectType-Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- Objekte
  - in Sybase Central suchen,799
- Objektprivilegien
  - Info,1305
  - Liste,1305
- ODBC
  - Administrator,41
  - Client-APIs und Zeichensatzkonvertierung,505
  - Datenquellen,38
  - Datenquellen unter Windows Mobile benutzen,48
  - Datenquellen-Verbindungsparameter,911
  - Delphi,642
  - eingeschränkte Funktionalität unter Windows Mobile,423
  - Fehlerbehandlung,955
  - Initialisierungsdatei für Unix,49
  - mit dem Dienstprogramm dbdsn erstellen,43
  - mit dem ODBC-Datenquellen-Administrator erstellen,41
  - mithilfe des Fensters Verbinden erstellen,39
  - odbc\_describe\_binary\_as\_varbinary-Option,642
  - odbc\_distinguish\_char\_and\_varchar-Option,642
  - Speicherort des Treibers,80
  - Unix-Unterstützung,49

- Verbindungen,50
- Verbindungsparameter,337
- ODBC INI-Dateien
  - Info,49
- ODBC Sample
  - verwenden,464
- ODBC, Datenquellen
  - generieren,39
  - mit dbdsn erstellen,905
- ODBC, Verbindungsparameter
  - Delphi,911
  - DescribeCursor,911
  - Description,911
  - Driver,911
  - GetTypeInfoChar,911
  - InitString,911
  - IsolationLevel,911
  - KeysInSQLStatistics,911
  - LazyAutocommit,911
  - PreFetchOnOpen,911
  - PreventNotCapable,911
  - SuppressWarnings,911
  - TranslationDLL,911
  - TranslationName,911
  - TranslationOption,911
- ODBC-Datenquelle
  - bearbeiten,42
  - Datei erstellen,47
  - unter Mac OS X erstellen,44
- ODBC-Datenquellen
  - Datenbankverbindungen,19
  - Datenbankverbindungen (dbisql),20
  - erstellen mit Als ODBC-Datenquelle speichern,39
  - für Windows Mobile erstellen,435
  - Info,38
  - konfigurieren,41
  - mit dem ODBC-Datenquellen-Administrator erstellen,41
  - Unix,49
  - unter Mac OS X erstellen,45
- ODBC-Datenquellen-Administrator
  - Datei erstellen,47
  - verwenden,41
- ODBC-Treiber
  - einrichten,45
- odbc.ini
  - Info,49
- odbc\_describe\_binary\_as\_varbinary, Option

---

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 odbc\_describe\_binary\_as\_varbinary-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 odbc\_describe\_binary\_as\_varbinary-Option  
   Beschreibung,642  
 odbc\_distinguish\_char\_and\_varchar, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 odbc\_distinguish\_char\_and\_varchar-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 odbc\_distinguish\_char\_and\_varchar-Option  
   Beschreibung,642  
 ODBC\_INI, Umgebungsvariable  
   Beschreibung,471  
   die Systeminformationsdatei lokalisieren,49  
 ODBCHOME, Umgebungsvariable  
   Beschreibung,470  
 ODBCINI, Umgebungsvariable  
   Beschreibung,471  
   die Systeminformationsdatei lokalisieren,49  
 OEM Edition  
   Info,194  
 OEM-Codepages  
   Info,500  
 oem\_string, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 oem\_string-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 oem\_string-Option  
   Beschreibung,643  
 Öffentliche Schlüssel, Verschlüsselung  
   Info,1444  
 Offline-Sicherungen  
   Info,1029  
 Offline-Transaktionslogs  
   Sicherungen,1079  
 OIDs  
   Datenbankeigenschaften,1248  
   Datenbankoptionen,1253  
   Datenbankstatistiken,1244  
   Definition,1217  
   Info,1217  
   RDBMS MIB,1263  
   Servereigenschaften,1237  
   Serverstatistiken,1234  
   SQL Anywhere MIB-Datenbank,1230  
 OLAP  
   optimization\_workload-Option,649  
 OLE DB  
   Client-APIs und Zeichensatzkonvertierung,505  
 OmniConnect, Unterstützung  
   Info,1570  
 OmniIdentifier, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 OmniIdentifier-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 ON EXCEPTION RESUME-Klausel  
   on\_tsql\_error-Option,646  
 on\_charset\_conversion\_failure, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 on\_charset\_conversion\_failure-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 on\_charset\_conversion\_failure-Option  
   Beschreibung,645  
 on\_error-Option  
   Info,865  
 on\_tsql\_error, Option  
   ASE-Kompatibilität,559  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
   Transact-SQL-Kompatibilität,560  
 on\_tsql\_error-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 on\_tsql\_error-Option  
   Beschreibung,646  
   Sybase Open Client,1571  
 Online-Sicherungen  
   Info,1029  
   Sicherungsdienstprogramm (dbbackup),886  
 Operatoren  
   Monitor-Benutzer,1175  
 Optimieren  
   Multiprogramming-Stufe, dynamisch,176  
   Multiprogramming-Stufe, manuell,179  
 Optimierer  
   Aufwand zur Lokalisation von Zugriffsplänen  
   steuern,648  
   Bypass,649  
   jüngsten Plan erfassen,316  
 optimization\_goal, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253

- optimization\_goal-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- optimization\_goal-Option
  - Beschreibung,647
- optimization\_level, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- optimization\_level-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- optimization\_level-Option
  - Beschreibung,648
- optimization\_workload-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- optimization\_workload-Option
  - Beschreibung,649
- option-Schlüsselwort
  - kann nicht deaktiviert werden ,641
- Optionen
  - alphabetische Liste der Datenbankoptionen,544
  - ansi\_update\_constraints,579
  - ANSINULL,580
  - ASE, Kompatibilitätsoptionen,559
  - Bereich und Dauer von Datenbankoptionen,564
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - chained,587
  - Command Sequence-Kommunikationsprotokoll,572
  - Datenbankoptionen einstellen,566
  - Datenbankoptionen in SQL Anywhere MIB,1253
  - Datenbankserver (Datenbank),203
  - Datenquelle, Dienstprogramm (dbdsn),905
  - Dienstprogramm dbisqlc,915
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Anzeigen von Zertifikaten (viewcert),903
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Erstellen von Zertifikaten (createcert),894
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Einstellungen beim Start,1572
  - Einstellungen löschen,567
  - Einstellungen überwachen,569
  - für SQL Anywhere MobiLink-Clients setzen,562
  - Groß-/Kleinschreibung,567
  - Histogramm, Dienstprogramm (dbhist),924
  - Info,544
  - Informationsdienstprogramm (dbinfo),926
  - Initialisierung, Dienstprogramm (dbinit),927
  - Interactive SQL (dbisql), Dienstprogramm,939
  - isql\_allow\_read\_client\_file,858
  - isql\_print\_result\_set,863
  - Klassifizierung,559
  - Kollationsanpassung,523
  - Linux, Dienstprogramm für Dienste (dbsvc),968
  - Löschen-Dienstprogramm (dberase),916
  - Optionen für Interactive SQL,851
  - Ping-Dienstprogramm (dbping),953
  - PUBLIC-Option,565
  - Serverauflistung, Dienstprogramm (dblocate),961
  - Serverstart im Hintergrund (dbspawn), Dienstprogramm,983
  - Serverstopp-Dienstprogramm (dbstop),984
  - Sicherungsdienstprogramm (dbbackup),886
  - Sprachauswahl-Dienstprogramm (dblang),946
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
  - SQL Anywhere-Skriptausführung, Dienstprogramm (dbrunsql),959
  - SQL Remote-Replikationsoptionen,563
  - sr\_date\_format,673
  - Sybase Open Client,1571
  - TDS-Kommunikationsprotokoll,572
  - temporär einstellen,565
  - Transact-SQL, Kompatibilitätsoptionen,560
  - Transaktionslog-Dienstprogramm (dblog),998
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Werte finden,567
  - Windows, Dienstprogramm für Dienste (dbsvc),974
- Optionen Fenster
  - Interactive SQL,817
- options-Schlüsselwort
  - kann nicht deaktiviert werden ,641
- OptionWatchAction, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- OptionWatchAction-Eigenschaft
  - Info,569
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- OptionWatchList, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767

---

OptionWatchList-Eigenschaft  
     Info,569  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1248  
 Oracle-Treiber  
     Datenquellen erstellen,906  
 Ordnerliste  
     Sybase Central,796  
 Organisation  
     certificate\_company-Protokolloption,392  
 Organisationseinheit  
     certificate\_unit, Protokolloption,394  
     in MobiLink-Transportschichtsicherheit  
     überprüfen,1462  
 os\_charset, Alias  
     Info,501  
 OSUser-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 Outbound Enabler  
     Ausführung als Linux-Dienst,968  
     Ausführung als Windows-Dienst,974  
     hohe Verfügbarkeit und Scale-Out-Lösungen,1540  
 output\_format, Option  
     Einstellungen von Interactive SQL,851  
 output\_format-Option  
     Info,866  
 output\_length, Option  
     Einstellungen von Interactive SQL,851  
 output\_length-Option  
     Info,867  
 output\_nulls, Option  
     Einstellungen von Interactive SQL,851  
 output\_nulls-Option  
     Info,867  
 Override-Magic  
     user\_estimates-Option,702

**P**

PacketSize, Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 PacketsReceived, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     Verbindungseigenschaft, Beschreibung,711  
 PacketsReceived-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 PacketsReceived-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1234,1244  
 PacketsReceivedUncomp, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     Verbindungseigenschaft, Beschreibung,711  
 PacketsReceivedUncomp-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 PacketsReceivedUncomp-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1234,1244  
 PacketsSent, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     Verbindungseigenschaft, Beschreibung,711  
 PacketsSent-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 PacketsSent-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1234,1244  
 PacketsSentUncomp, Eigenschaft  
     Servereigenschaft, Beschreibung,745  
     Verbindungseigenschaft, Beschreibung,711  
 PacketsSentUncomp-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 PacketsSentUncomp-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1234,1244  
 page, Modus  
     Datenbankspiegelung,1478  
 PageRelocations, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 PageRelocations-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1244  
 PageSize, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
     Servereigenschaft, Beschreibung,745  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1248  
 PageSize-Eigenschaft  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1237  
 Paketgröße  
     -p, Datenbankserveroption,271  
     -pt dbsrv16-Serveroption,273  
     CommBufferSize-Verbindungsparameter  
     (CBSIZE),343  
 Parallelausführung  
     Prozessoren,251

- Parallele Sicherungen
  - dbbackup-Dienstprogramm,886
  - Info,1080
  - unter Windows Mobile nicht unterstützt,423
- Parallelität
  - max\_query\_tasks-Option,633
- Parameter
  - Broadcast Repeater-Dienstprogramm (dbns16),892
  - Datenbankserver (Datenbank),203
  - Datenquelle, Dienstprogramm (dbdsn),905
  - Dienstprogramm dbisqlc,915
  - Dienstprogramm für Supportanfragen (dbsupport),987
  - Dienstprogramm zum Anzeigen von Zertifikaten(viewcert),903
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Dienstprogramm zur Serverlizenzierung (dblic),964
  - Erstellen von Zertifikaten (createcert),894
  - Histogramm, Dienstprogramm (dbhist),924
  - Informationsdienstprogramm (dbinfo),926
  - Initialisierungsdienstprogramm (dbinit),927
  - Interactive SQL (dbisql), Dienstprogramm,939
  - Linux, Dienstprogramm für Dienste (dbsvc),968
  - Löschen, Dienstprogramm (dberase),916
  - Ping-Dienstprogramm (dbping),953
  - Serverauflistung, Dienstprogramm (dblocate),961
  - Serverstart im Hintergrund (dbspawn), Dienstprogramm,983
  - Serverstopp-Dienstprogramm (dbstop),984
  - Sprachauswahl-Dienstprogramm (dblang),946
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
  - SQL Anywhere-Skriptausführung, Dienstprogramm (dbrunsql),959
  - Transaktionslog-Dienstprogramm (dblog),998
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Windows, Dienstprogramm für Dienste (dbsvc),974
- Partnerserver
  - für Datenbankspiegelung festlegen,1480
  - in Kopieknotten konvertieren,1554
  - Info,1467
- PartnerState, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- PartnerState-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- password, Parameter
  - LDAP,110
- Password, Verbindungsparameter
  - Beschreibung,378
- PATH, Umgebungsvariable
  - Beschreibung,471
- PBUF, Verbindungsparameter
  - Beschreibung,379
- PeakCacheSize, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- PeakCacheSize-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- PEM-kodierte PKI-Objekte
  - anzeigen,903
- Performance
  - Auswirkungen der Tabellenverschlüsselung,1438
  - Cachegröße,167
  - Datenbankspiegelung,1476
  - Embedded SQL-Verbindungen testen,96
  - Ergebnismengen,647
  - Festplattenfragmentierung,132,133
  - Komprimierung,112
  - Meldungen in Meldungslogdatei des Datenbankservers,1110
  - OLAP queries,649
  - Prefetch,653
  - Primärschlüssel,138
  - Prioritäten einstellen,656
  - Serveroptionen,167
  - Sybase PowerBuilder DataWindow,647
  - Transaktionslog-Größe,138
  - Transaktionslog-Spiegel,138
  - verschlüsselte Datenbanken,1433
  - Vorteile des Transaktionslogs,135
  - Warnungen in Meldungslogdatei des Datenbankservers,1110
- Performance verbessern
  - adäquate Hardware verwenden,794
- Performance-Statistiken
  - Sammlung deaktivieren,259
- Performancedaten
  - an das Softwareentwicklungsteam senden,1108
- Performancestatistik, Dienstprogramm (dbstats)
  - Beendigungscodes,954

---

Syntax,953

Performancestatistiken

Überwachung unter Unix,953

Performancewarnungen

Info,1110

Perl

Client-APIs und Zeichensatzkonvertierung,505

Perseat, Lizenzierung

info,964

Personal Server

Einstellungen der Multiprogramming-Stufe,177

Info,150

unter Windows Mobile nicht unterstützt,423

Unterschiede zum Netzwerkserver,151

unterstützte Kommunikationsprotokolle,103

PHP

Client-APIs und Zeichensatzkonvertierung,505

Physische Einschränkungen

SQL Anywhere,791

PID-Dateien

Linux-Dienste,972

Ping-Dienstprogramm (dbping)

Beendigungscodes,958

Syntax,955

verwenden,95

pingen

Server,955

pinned\_cursor\_percent\_of\_cache, Option

SQL Anywhere SNMP-Erweiterungsagent,

OID,1253

pinned\_cursor\_percent\_of\_cache-Eigenschaft

Verbindungseigenschaft, Beschreibung,711

pinned\_cursor\_percent\_of\_cache-Option

Beschreibung,650

PKI, Objekte

anzeigen,903

Plananzeige

Dateierweiterung,839

Info,839

Navigation,839

Pläne

aktuellsten aufzeichnen,316

grafische Pläne anpassen,840

max\_plans\_cached-Option,632

Optimierer-Verwendung steuern,648

Planung

Datenbanken,121

Datenbanken, Hinweise,121

Sicherung und Wiederherstellung,1061

Sicherungen,1063

Planungsmodus

Info,808

Platform, Eigenschaft

Verbindungseigenschaft, Beschreibung,745

Platform-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,

OID,1237

PlatformVer, Eigenschaft

Verbindungseigenschaft, Beschreibung,745

PlatformVer-Eigenschaft

SQL Anywhere SNMP-Erweiterungsagent,

OID,1237

Plattenspiegelung

Transaktionslogs,139

Plug-In registrieren

Info,807

Plug-In-Assistenten registrieren

verwenden,807

Plug-Ins

Plug-In-Architektur von Sybase Central,806

Registrierungseinstellungen,490

SQL Anywhere,808

Pooling

ConnectionPool-Verbindungsparameter

(CPOOL),350

port, Parameter

LDAP,110

port-Protokolloption

Beschreibung,416

Portnummer

Datenbankserver,416

Schnelllader,876

ServerPort-Protokolloption (PORT),416

Ports

Standardwert,416

post\_login\_procedure, Option

Beschreibung,651

Kennwortablauf implementieren,1411

SQL Anywhere SNMP-Erweiterungsagent,

OID,1253

post\_login\_procedure-Eigenschaft

Verbindungseigenschaft, Beschreibung,711

Praktische Einführung

Rollen und Privilegien erteilen (SQL),1378

Rollen und Privilegien erteilen (Sybase

Central),1371

- Verbindung mit der Beispieldatenbank herstellen,1
- Windows Mobile,461
- Praktische Einführungen
  - Datenbankspiegelung,1509
  - Datenbankspiegelung bei mehreren Datenbanken,1516
  - ein Server als Kopieknoten und Arbiter,1561
  - Erstellen einer Datenbank,114
  - Monitor,1200
  - Partnerserver in Kopieknoten konvertieren,1563
  - Scale-Out mit Schreibschutz,1556
  - Spiegelungssysteme zu Scale-Out-Systemen mit Schreibschutz hinzufügen,1565
  - Windows Mobile-Datenbanken mit Interactive SQL verwalten,457
  - Windows Mobile-Datenbanken über Sybase Central ausführen,452
- precision, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- precision-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- precision-Option
  - Beschreibung,653
- prefetch, Option
  - DisableMultiRowFetch-Verbindungsparameter,357
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- prefetch-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- prefetch-Option
  - Beschreibung,653
- PrefetchBuffer, Verbindungsparameter
  - Beschreibung,379
- PrefetchOnOpen, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- PrefetchOnOpen-Verbindungsparameter
  - Beschreibung,380
- PrefetchRows, Verbindungsparameter
  - Beschreibung,381
- Prepares, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- Prepares-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- PrepStmt, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- PrepStmt-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- PrepStmt-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- preserve\_source\_format, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- preserve\_source\_format-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- preserve\_source\_format-Option
  - Beschreibung,655
- prevent\_article\_pkey\_update, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- prevent\_article\_pkey\_update-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- prevent\_article\_pkey\_update-Option
  - Beschreibung,655
- PreventNotCapable, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- Primärschlüssel
  - Transaktionslog,138
- Primärserver
  - bestimmen,1483
  - Datenbankspiegelung, Übersicht,1467
  - Failover erzwingen,1488
  - Löschen von Servern aus einem Scale-Out-System,1552
  - nach einem Ausfall wiederherstellen,1499
  - Spiegelserver löschen,1490
  - stoppen,1490
  - Unterschiede zu Kopieknoten,1539
- Priorität
  - Prozess,238
- priority, Option
  - Beschreibung,656
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- priority-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Private Schlüssel
  - anzeigen,903
- Privilegien
  - Ansichten für zusätzliche Sicherheit einsetzen,1403
  - Anweisungen zur Dateiverwaltung,255
  - aus Berechtigungen migrieren,1389

---

Daten entladen,242  
 Daten laden,242  
 Datenbanken starten,240  
 Datenbanken stoppen,240  
 Datenbankserver stoppen,242  
 DBSpaces,1305  
 deaktivierte Objekte,1349  
 einzeln,1340  
 entziehen (SQL),1338  
 erteilen (SQL),1332,1335  
 explizit einem Benutzer oder einer Gruppe (Rolle)  
 erteilt,1348  
 für Ansichten erteilen,1305  
 für Prozeduren festlegen,1305  
 in Sybase Central entziehen,1336  
 in Sybase Central erteilen,1331,1333  
 Info,1305  
 Liste,1309  
 mit integriertem Login,52  
 negative Privilegien nicht unterstützt,1348  
 Optionen,170  
 praktische Einführung (SQL),1378  
 praktische Einführung, Sybase Central,1371  
 Privilegien eines Benutzers anzeigen (SQL),1344  
 Privilegien eines Benutzers anzeigen (Sybase  
 Central),1343  
 Prozeduren,1305  
 Schema,1409  
 Sequenzgeneratoren,1305  
 Sicherheitsfunktionen,1409  
 System,1309  
 Tabellen,1305  
 Vererbung,1349  
 Privilegien auf Objektebene  
 entziehen (SQL),1340  
 in Sybase Central entziehen,1339  
 praktische Einführung (SQL),1378  
 praktische Einführung, Sybase Central,1371  
 ProcedurePages, Eigenschaft  
 Datenbankeigenschaft, Beschreibung,767  
 ProcedurePages-Statistik  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1244  
 ProcedureProfiling, Eigenschaft  
 Datenbankeigenschaft, Beschreibung,767  
 ProcedureProfiling-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1248  
 ProcessCPU, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProcessCPU-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProcessCPUSystem, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProcessCPUSystem-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProcessCPUUser, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProcessCPUUser-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProcessID-Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 processor\_affinity  
 gesicherte Funktion,1413  
 processor\_affinity-Funktion  
 -sf, Serveroption,280  
 ProcessorAffinity-Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProcessorArchitecture, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProcessorArchitecture-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProductName, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProductName-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 ProductVersion, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProductVersion-Eigenschaft  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1237  
 PROFILE-Berechtigung (nicht mehr empfohlen)  
 konvertiert in SYS\_AUTH\_PROFILE\_ROLE-  
 Kompatibilitätsrolle,1275  
 ProfileFilterConn, Eigenschaft  
 Servereigenschaft, Beschreibung,745  
 ProfileFilterConn-Eigenschaft

- SQL Anywhere SNMP-Erweiterungsagent,
  - OID,1237
- ProfileFilterUser, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- ProfileFilterUser-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1237
- Programmdateien
  - bedingte syntaktische Analyse in
    - Konfigurationsdateien verwenden,883
    - Konfigurationsdateien verwenden,882
    - Speicherort,482
- Programmdateiname
  - Dienstprogramm zur Serverlizenzierung
    - (dblic),964
- Programmierschnittstellen
  - Verbindungen,50
- Progress-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- progress\_messages-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- progress\_messages-Option
  - Beschreibung,657
  - SQL Anywhere SNMP-Erweiterungsagent,
    - OID,1253
- promotion\_time-Option
  - verwenden,1553
- Protokolle
  - Angabe für Datenbankserver,306
  - auswählen,103
  - Fehlerbehandlung,1113
  - Info,102
  - Optionen,103
  - TCP/IP verwenden, Datenbankserver,389
  - unterstützte,102
- Protokollieren
  - Anweisungen in Interactive SQL,826
  - Datenbankserver-Aktionen,163
  - Datenbankserver-Meldungen,268
  - HTTP-Logformat,408
  - HTTP-Serveranforderungen,408
  - Transaktionslog,135
- Protokollierung
  - HTTP-Clientinformationen,315
- Protokolloptionen
  - alphabetische Liste,388
  - Boolesche Werte,388
  - Groß-/Kleinschreibung nicht berücksichtigen,388
- HTTP verwenden, Datenbankserver,389
- HTTPS verwenden, Datenbankserver,389
- Liste,389
- TLS verwenden, Datenbankserver,389
- PROWS, Verbindungsparameter
  - Beschreibung,381
- Proxy-Ports
  - für Windows Mobile-Geräte erstellen,437
- Prozeduren
  - alphabetische Liste der Systemprivilegien,1309
  - Datenbankdokumentation erstellen,814
  - EXECUTE-Privileg,1305
  - in Interactive SQL nachschlagen,828
  - max\_plans\_cached-Option,632
  - Sicherheit,1403,1405
- Prozessor, Lizenzierung
  - Info,964
- Prozessoren
  - mehrere,169
  - Parallelität,253
  - verwendete,252
  - verwendete Anzahl,251
- Prüfsummen
  - wc, Datenbankoption,334
  - wc, Datenbankserveroption,304
  - aktiviert bei Windows Mobile-Datenbanken,441
  - automatisch,1085
  - automatisch aktiviert bei Windows Mobile-Datenbanken,1086
  - Info,1084
  - Initialisierung, Dienstprogramm (dbinit),927
  - Validierungs-Dienstprogramm (dbvalid),1021
- Prüfsummen validieren
  - Info,1086
- Public Key Infrastructure, Objekte
  - anzeigen,903
- PUBLIC, Option
  - Info,565
- PUBLIC-Optionen
  - SET ANY PUBLIC OPTION-Systemprivileg
    - erforderlich,565
- PUBLIC-Systemrolle
  - Info,1272
- Publikationseigentümer
  - db\_publisher-Option,602
- PUBLISH-Privileg
  - Info,1305
- Punkt zu Punkt, Verschlüsselung

---

createkey, Dienstprogramm,945  
Punkt zu Punkt-Verschlüsselung  
MobiLink, Info,1459  
PWD, Verbindungsparameter  
Beschreibung,378  
Python  
Client-APIs und Zeichensatzkonvertierung,505

## Q

qualify\_owners-Option  
SQL Remote, Beschreibung,658  
SQL Remote-Replikationsoption,563  
Quaternär, Berücksichtigung von Satzzeichen  
Datenbanken mit Berücksichtigung von Groß- und  
Kleinschreibung und Akzenten,938  
query\_mem\_timeout-Eigenschaft  
Verbindungseigenschaft, Beschreibung,711  
query\_mem\_timeout-Option  
Beschreibung,659  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253  
query\_plan\_on\_open, Option  
Transact-SQL-Kompatibilität,560  
QueryBypassed, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryBypassedCosted, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryBypassedHeuristic, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryBypassedOptimized, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryCachedPlans, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryCachePages, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryCachePages-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1244  
QueryDescribedBypass, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryDescribedOptimizer, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryHeapPages, Eigenschaft  
Servereigenschaft, Beschreibung,745  
Verbindungseigenschaft, Beschreibung,711  
QueryHeapPages-Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
QueryHeapPages-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234,1244  
QueryJHToJNLOptUsed, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryLowMemoryStrategy, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Verbindungseigenschaft, Beschreibung,711  
QueryLowMemoryStrategy-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1244  
QueryMemActiveCurr, Eigenschaft  
Verbindungseigenschaft, Beschreibung,711  
QueryMemActiveCurr-Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
Servereigenschaft, Beschreibung,745  
QueryMemActiveCurr-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234,1244  
QueryMemActiveEst, Eigenschaft  
Servereigenschaft, Beschreibung,745  
QueryMemActiveEst-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234  
QueryMemActiveMax, Eigenschaft  
Servereigenschaft, Beschreibung,745  
QueryMemActiveMax-Eigenschaft  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237  
QueryMemExtraAvail-Eigenschaft  
Servereigenschaft, Beschreibung,745  
QueryMemExtraAvail-Statistik  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1234  
QueryMemGrantBase, Eigenschaft  
Servereigenschaft, Beschreibung,745  
QueryMemGrantBase-Eigenschaft  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237

- QueryMemGrantBaseMI, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantBaseMI-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- QueryMemGrantExtra, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantExtra-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- QueryMemGrantFailed, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryMemGrantFailed-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantFailed-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- QueryMemGrantGranted, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryMemGrantGranted-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantGranted-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- QueryMemGrantRequested-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- QueryMemGrantRequested-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- QueryMemGrantWaited, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryMemGrantWaited-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantWaited-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- QueryMemGrantWaiting, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryMemGrantWaiting-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Servereigenschaft, Beschreibung,745
- QueryMemGrantWaiting-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244
- QueryMemPages, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- QueryMemPages-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- QueryMemPercentOfCache, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- QueryMemPercentOfCache-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- QueryOpened, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- QueryOptimized, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryOptimized-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- QueryReused, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryReused-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- QueryRowsFetched-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- QueryRowsMaterialized, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- QueryRowsMaterialized-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- QueryRowsMaterialized-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- QuittingTime, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- QuittingTime-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- Quorum
  - Datenbankspiegelung,1469
- quote\_all\_identifiers-Option
  - SQL Remote, Beschreibung,659
  - SQL Remote-Replikationsoption,563
- quoted\_identifier, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- quoted\_identifier-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244

---

Verbindungseigenschaft, Beschreibung,711  
quoted\_identifizier-Option  
Beschreibung,660  
Sybase Open Client,1571

## R

RAISERROR, Anweisung  
continue\_after\_raisererror-Option,594  
on\_tsq\_error-Option,646  
RAISERROR, Systemereignis  
Beschreibung,1092  
RAS  
DFÜ-Netzwerk,109  
Rate-Eigenschaften  
Info,789  
Räumliche Daten  
st\_geometry\_asbinary\_format-Option,679  
st\_geometry\_astext\_format-Option,680  
st\_geometry\_asxml\_format-Option,681  
st\_geometry\_describe\_type-Option,682  
st\_geometry\_interpolation-Option,683  
st\_geometry\_on\_invalid-Option,684  
Raw-Eigenschaften  
Info,789  
RAW-Verschlüsselung  
Info,1436  
RCVBUFSZ, Protokolloption  
Beschreibung,415  
RDBMS MIB  
Tabellenliste,1263  
RDBMS MIB-Datenbank  
Info,1220  
RDBMS-MIB.mib  
Info,1220  
Speicherort,1263  
SQL Anywhere SNMP-Erweiterungsagent,1216  
rdbmsDbInfoTable  
Beschreibung,1263  
rdbmsDbLimitedResourceTable  
Beschreibung,1265  
rdbmsDbParamTable  
Beschreibung,1264  
rdbmsDbTable  
Beschreibung,1263  
rdbmsSrvInfoTable  
Beschreibung,1266  
rdbmsSrvLimitedResourceTable

Beschreibung,1268  
rdbmsSrvParamTable  
Beschreibung,1267  
rdbmsSrvTable  
Beschreibung,1266  
READ CLIENT FILE-Systemprivileg  
Beschreibung,1309  
READ FILE-Systemprivileg  
Beschreibung,1309  
read\_authdn, Parameter  
LDAP,110  
read\_password, Parameter  
LDAP,110  
read\_past\_deleted, Option  
Beschreibung,661  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253  
read\_past\_deleted-Eigenschaft  
Verbindungseigenschaft, Beschreibung,711  
READCLIENTFILE-Berechtigung (nicht mehr  
empfohlen)  
konvertiert in  
SYS\_AUTH\_READCLIENTFILE\_ROLE-  
Kompatibilitätsrolle,1275  
READFILE-Berechtigung (nicht mehr empfohlen)  
konvertiert in SYS\_AUTH\_READFILE\_ROLE-  
Kompatibilitätsrolle,1275  
ReadOnly, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
ReadOnly-Eigenschaft  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248  
ReceiveBufferSize, Protokolloption  
Beschreibung,415  
ReceivingTracingFrom, Eigenschaft  
Datenbankeigenschaft, Beschreibung,767  
ReceivingTracingFrom-Eigenschaft  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1248  
recovery\_time, Option  
SQL Anywhere SNMP-Erweiterungsagent,  
OID,1253  
verwenden,1077  
recovery\_time-Eigenschaft  
Verbindungseigenschaft, Beschreibung,711  
recovery\_time-Option  
Beschreibung,661  
RecoveryUrgency, Eigenschaft

- Datenbankeigenschaft, Beschreibung,767
- RecoveryUrgency-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- RecursiveIterations, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- RecursiveIterationsHash, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- RecursiveIterationsNested, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- RecursiveJNLMisses, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- RecursiveJNLProbes, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- REFERENCES-Privileg
  - Info,1305
- Registrierung
  - ändern,467
  - Info,487
  - Sprachauswahl-Dienstprogramm (dblang),946
  - SQLREMOTE-Umgebungsvariable setzen,480
  - Standort-Einstellung,490
  - Sybase Central,490
  - Toolstandort-Einstellung,490
  - Umgebungsvariablen,467
  - Windows Mobile,491
  - Windows-Dienste,488
- Registrierungseinstellungen
  - Sprache,490
- Rekursive Abfragen
  - max\_recursive\_iterations-Option,634
- Relay Server
  - hohe Verfügbarkeit und Scale-Out-Lösungen,1540
  - überwachen,1115
- Relay Server-Farm
  - überwachen,1115
- Relay Server-Farmen
  - überwachen,1135
- Relay Server-Status-Manager
  - Ausführung als Linux-Dienst,968
  - Ausführung als Windows-Dienst,974
- RelocatableHeapPages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- RelocatableHeapPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- RememberLastPlan, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- RememberLastPlan-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- RememberLastStatement, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- RememberLastStatement-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- REMOTE DBA-Berechtigung (nicht mehr empfohlen)
  - stattdessen GRANT ROLE SYS\_RUN\_REPLICATION\_ROLE verwenden,1400
- remote\_idle\_timeout-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- remote\_idle\_timeout-Option
  - Beschreibung,662
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- RemoteCapability, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- RemoteCapability-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- RemoteputWait, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- RemoteputWait-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- RemoteTrunc, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- RemoteTrunc-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- REMOVE JAVA-Anweisung
  - unter Windows Mobile nicht unterstützt,425
- REORGANIZE ANY OBJECT-Systemprivileg
  - Beschreibung,1309
- REORGANIZE TABLE-Anweisung
  - unter Windows Mobile nicht unterstützt,425
- Reparieren
  - Monitor-Ressourcen,1147
- replicate\_all, Option

---

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 replicate\_all-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 replication\_error-Option  
   SQL Remote, Beschreibung,663  
   SQL Remote-Replikationsoption,563  
 replication\_error\_piece-Option  
   SQL Remote, Beschreibung,663  
 Replikation  
   Sicherungsprozeduren,1069  
   SQL Remote-Optionen,563  
   Systemrollen,1273  
   Transaktionslogverwaltung,1069  
   Trigger-Aktionen,612  
   verschlüsselte Datenbanken neu aufbauen,1017  
 Replikationsoptionen  
   Klassifizierung,559  
   SQL Remote blob\_threshold,585  
   SQL Remote delete\_old\_logs,607  
   SQL Remote external\_remote\_options,611  
   SQL Remote qualify\_owners,658  
   SQL Remote quote\_all\_identifiers,659  
   SQL Remote replication\_error,663  
   SQL Remote replication\_error\_piece,663  
   SQL Remote save\_remote\_passwords,668  
   SQL Remote sr\_date\_format,673  
   SQL Remote sr\_time\_format,675  
   SQL Remote sr\_timestamp\_format,676  
   SQL Remote  
   sr\_timestamp\_with\_time\_zone\_format,677  
   SQL Remote subscribe\_by\_remote,686  
   SQL Remote verify\_all\_columns,704  
   SQL Remote verify\_threshold,707  
   SQL Remote-Komprimierung,592  
   SQL Remote-Liste,563  
 Req, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 Req-Statistik  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1234  
 ReqCountActive-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountBlockContention-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountBlockIO-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountBlockIO-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountBlockLock, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountBlockLock-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
 ReqCountUnscheduled, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqCountUnscheduled-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
 ReqStatus, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqTimeActive, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqTimeActive-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
 ReqTimeBlockContention, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqTimeBlockContention-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248  
 ReqTimeBlockIO, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 ReqTimeBlockIO-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237,1248

- ReqTimeBlockLock, Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- ReqTimeBlockLock-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - Servereigenschaft, Beschreibung, 745
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237, 1248
- ReqTimeUnscheduled, Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- ReqTimeUnscheduled-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - Servereigenschaft, Beschreibung, 745
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237, 1248
- ReqType, Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- request\_timeout-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- request\_timeout-Option
  - Beschreibung, 664
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- RequestFilterConn, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestFilterConn-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestFilterDB, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestFilterDB-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestLogFile, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestLogFile-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestLogging, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestLogging-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestLogMaxSize, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestLogMaxSize-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestLogNumFiles, Eigenschaft
  - Servereigenschaft, Beschreibung, 745
- RequestLogNumFiles-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- RequestsReceived-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - Servereigenschaft, Beschreibung, 745
  - Verbindungseigenschaft, Beschreibung, 711
- RequestsReceived-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1234, 1244
- RequestTiming-Eigenschaft
  - Servereigenschaft, Beschreibung, 745
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
- reserved\_keywords-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- reserved\_keywords-Option
  - Beschreibung, 665
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
  - Transact-SQL-Kompatibilität, 560
- RESOURCE-Berechtigung (nicht mehr empfohlen)
  - konvertiert in SYS\_AUTH\_RESOURCE\_ROLE-Kompatibilitätsrolle, 1275
- Ressourcen
  - Datenbanken überwachen, 1132
  - entfernen, 1148
  - Monitor, reparieren, 1147
  - Monitor, Ressourcen importieren, 1138
  - Monitor, Verbindungen löschen, 1130
  - Überwachung stoppen, 1146
- Ressourcenwächter
  - Anweisungen, 635
  - Cursor, 631
- RetryConnectionTimeout-Verbindungsparameter
  - Beschreibung, 382
  - mit gespiegelten Datenbanken verbinden, 1472
- RetryConnTO, Verbindungsparameter
  - Beschreibung, 382
  - mit gespiegelten Datenbanken verbinden, 1472
- return\_date\_time\_as\_string-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- return\_date\_time\_as\_string-Option
  - Beschreibung, 666
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- REVOKE GROUP-Anweisung

---

Syntax (nicht mehr empfohlen),1397  
 REVOKE MEMBERSHIP IN GROUP-Anweisung  
     Syntax (nicht mehr empfohlen),1397  
 REVOKE-Anweisung  
     Änderungen in Version 16.0,1396  
     Vergleich der Syntax für Berechtigungen und Rollen,1396  
 Richtlinien  
     SQL Anywhere-Login,535  
     Unterstützung für SELinux,1403  
 Richtlinienoptionen  
     Info,535  
 Rlbk-Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
     Servereigenschaft, Beschreibung,745  
     Verbindungseigenschaft, Beschreibung,711  
 Rlbk-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1234,1244  
 ROLLBACK-Anweisung  
     Log,1079  
     WITH HOLD-Cursor,576  
 Rollback-Log  
     Datenbankgröße erhöhen,1107  
     Info,1079  
 rollback\_on\_deadlock, Option  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253  
 rollback\_on\_deadlock-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 rollback\_on\_deadlock-Option  
     Beschreibung,666  
 RollbackLogPages, Eigenschaft  
     Datenbankeigenschaft, Beschreibung,767  
 RollbackLogPages-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 RollbackLogPages-Statistik  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1244  
 Rollen  
     Benutzer in benutzererweiterte Rollen konvertieren (SQL),1290  
     Benutzer in benutzererweiterte Rollen konvertieren (Sybase Central),1289  
     benutzererweiterte Rollen in Benutzer zurückkonvertieren (Sybase Central),1291  
     Datenbankoptionen ändern,570  
     Datenbankspiegelung,1487  
     entziehen (SQL),1302  
     erteilen (SQL),1299  
     in Sybase Central entziehen,1301  
     in Sybase Central erstellen,1285  
     in Sybase Central erteilen,1298  
     in Sybase Central konfigurieren,1296  
     in Sybase Central löschen,1303  
     in Sybase Central migrieren,1277  
     Info,1271  
     Kompatibilitätsrollen,1275  
     Kompatibilitätsrollen erteilen (SQL),1281  
     Kompatibilitätsrollen in Sybase Central erteilen,1280  
     konfigurieren (SQL),1297  
     löschen (SQL),1304  
     migrieren (SQL),1278  
     min\_role\_admins-Option,638  
     mindestens erforderliche Anzahl von Administratoren,638  
     Möglichkeit zum Verwalten mit MANAGE ROLES gewährleisten,1294  
     praktische Einführung (SQL),1378  
     praktische Einführung, Sybase Central,1371  
     Privilegien erteilen,1331  
     Privilegkonflikte,1331  
     Rollen eines Benutzers anzeigen (SQL),1344  
     Rollen eines Benutzers anzeigen (Sybase Central),1343  
     Rollen in Benutzer ändern (SQL),1292  
     Vererbungsverhalten von Berechtigungen,1400  
 Rollenadministratoren  
     Info,1293  
 Rollenbasierte Sicherheit  
     implementieren,1364  
     Info,1271  
     planen,1364  
 Rollenwechsel  
     Datenbankspiegelung,1487  
 Root-Login-Richtlinie  
     ändern,541  
     Info,535  
     Standardwerte,536  
 Router  
     zum Rundsenden verwenden,398  
 row\_counts, Option  
     SQL Anywhere SNMP-Erweiterungsagent, OID,1253  
 row\_counts-Eigenschaft

- Verbindungseigenschaft, Beschreibung,711
- row\_counts-Option
  - Beschreibung,667
- rs\_systabgroup-Systemrolle
  - Info,1272
- RSA
  - Unterstützung,1445
- RSA-Option
  - ec, Datenbankserveroption,230
- RSA-Zertifikate
  - anzeigen,903
  - erstellen,894
- Ruby
  - Client-APIs und Zeichensatzkonvertierung,505
- Rückgabecodes
  - Datenquellendienstprogramm (dbdsn),909
  - Dienstprogramm für den Serverstart im Hintergrund (dbspawn),984
  - Dienstprogramm zum Entladen (dbunload),1014
  - Dienstprogramm zum Upgrade (dbupgrad),1020
  - Dienstprogramm zur Logkonvertierung (dbtran),953
  - Dienstprogramm zur Serverlizenzierung (dblic),967
  - Histogramm-Dienstprogramm (dbhist),925
  - Informationsdienstprogramm (dbinfo),927
  - Initialisierungsdienstprogramm (dbinit),938
  - Interactive SQL (dbisql), Dienstprogramm,944
  - Löschen-Dienstprogramm (dberase),918
  - Performancestatistik-Dienstprogramm (dbstats),954
  - Ping-Dienstprogramm (dbping),958
  - Serverauflistung, Dienstprogramm (dblocate),963
  - Serverstopp-Dienstprogramm (dbstop),986
  - Sicherungen [dbbackup], Dienstprogramm,891
  - Sprache, Dienstprogramm (dblang),947
  - Transaktionslog-Dienstprogramm (dblog),1000
  - Validierung, Dienstprogramm [dbvalid],1024
  - Windows, Dienstprogramm für Dienste (dbsvc),980
- Ruhezustand
  - Windows Mobile,430
- Runden
  - scale-Option,668
- S**
- sa\_config.csh
  - als Source nehmen,468
- sa\_config.sh
  - als Source nehmen,468
- sa\_conn\_properties, Systemprozedur
  - anwenden,567
- sa\_conn\_properties-Systemprozedur
  - alphabetische Liste der Verbindungseigenschaften,711
- sa\_db\_properties-Systemprozedur
  - alphabetische Liste der Datenbankeigenschaften,767
- SA\_DEBUG-Systemrolle
  - Info,1272
- sa\_eng\_properties-Systemprozedur
  - alphabetische Liste der Datenbankserveigenschaften,745
- sa\_monitor\_connection\_failed\_event, Ereignis
  - Monitor,1193
- sa\_monitor\_connection\_failure, Tabelle
  - Monitor,1193
- sa\_monitor\_count\_unsubmitted\_crash\_reports, Funktion
  - Monitor,1193
- sa\_monitor\_user
  - Info,1193
- sa\_server\_option-Systemprozedur
  - Datenbankeinstellungen überwachen,569
- SACA
  - Einbyte-Zeichensätze,516
  - Info,515
  - Mehrbyte-Zeichensätze,516
  - UTF-8-Zeichensätze,516
- SACHARSET, Umgebungsvariable
  - Zeichensätze angeben,472
- SACHARSET-Umgebungsvariable
  - festlegen,514
- SADatabase, Agent
  - konfigurieren,1532
  - testen,1535
- saDbOptMetaDataTable
  - SQL Anywhere MIB-Datenbank,1233
- saDbPropMetaDataTable
  - SQL Anywhere MIB-Datenbank,1233
- saDbStatMetaDataTable
  - SQL Anywhere MIB-Datenbank,1232
- SADIAGDIR, Umgebungsvariable
  - Speicherort von Diagnoseinformationen angeben,473

---

SALANG, Umgebungsvariable  
     Sprachen angeben,473  
 SALANG-Umgebungsvariable  
     festlegen,514  
 saldap.ini  
     Info,109  
 SALOGDIR, Umgebungsvariable  
     Beschreibung,474  
 samonitor.bat  
     Monitor-Dienst starten,1120  
     Monitor-Dienst stoppen,1121  
 samonitor.sh  
     Monitor-Dienst starten,1120  
     Monitor-Dienst stoppen,1121  
 sample\_config.csh  
     als Source nehmen,468  
 sample\_config.sh  
     als Source nehmen,468  
 Sandboxing  
     -sbx, Datenbankoption ,330  
     -sbx, Datenbankserveroption,279  
     -sf, Serveroption,280  
     gesicherte Funktion,1413  
     Info,1411  
     Sicherheitstipp,1408  
 SANs  
     Datenbankdateien speichern,136  
 SAP HANA  
     Interactive SQL,814  
 SAPLAN-Dateien  
     Dateierweiterung für die Plananzeige,839  
 SAServer, Agent  
     konfigurieren,1528  
 SAServer-Agent  
     testen,1531  
 sasnmp.ini  
     für SQL Anywhere SNMP-Erweiterungsagenten  
     erforderlich,1222  
     Info,1216  
 sasrv.ini  
     CommLinks-Verbindungsparameter,90  
     Fehlerbehandlung beim Serverstart,95  
     Host-Verbindungsparameter,87  
     Serverdaten,94  
 saSrvPropMetaDataTable  
     SQL Anywhere MIB-Datenbank,1232  
 saSrvStatMetaDataTable  
     SQL Anywhere MIB-Datenbank,1231  
 SATMP-Umgebungsvariable  
     Beschreibung,475  
     Speicherplatz,1110  
     Unix,481  
     Unix, Shared Memory-Verbindungen sichern,1407  
 save\_remote\_passwords, Option  
     SQL Remote-Option,668  
 scale, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 scale-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 scale-Option  
     Beschreibung,668  
 Scale-Out  
     -xp, Option,335  
     Kopieknoten,1536  
     Login-Richtlinien verwalten,543  
     mit Datenbankspiegelung verwenden,1538  
     mit Verbindungspooling verwenden,78  
     mit Webdiensten verwenden,1540  
     praktische Einführung,1556  
     Server ändern,1552  
     SQL Anywhere,1536  
     übergeordnete Knoten automatisch zuweisen,1550  
     übergeordneten Knoten eines Kopieknotens  
     ermitteln,1551  
     Verbindungsparameter NodeType (NODE),375  
     Verlust von Verbindungen zu übergeordneten  
     Knoten,1553  
 Scale-Out mit Schreibschutz  
     -xp, Option,335  
     Info,1536  
     Kopieknoten definieren,1548  
     mit Datenbankspiegelung verwenden,1538  
     mit Verbindungspooling verwenden,78  
     praktische Einführung,1556  
     Server löschen,1552  
     Spiegelung hinzufügen,1555  
     Unterschiede zwischen Personal Server und  
     Netzwerkserver,151  
     Verbindungsparameter NodeType (NODE),375  
 Schätzungen  
     user\_estimates-Option,702  
     Wiederherstellungszeit,661  
     Zeilenanzahl,667  
 Schemata  
     Definitionen entladen,1001

- vergleichen,809
- vergleichen und angleichen,810
- Schließen von Verbindungen
  - Monitor,1130
- Schlüsselpaargenerator, Dienstprogramm (createkey)
  - Syntax,945
- Schlüsselwörter
  - aktivieren,665
  - ausschalten,641
  - non\_keywords-Option,641,665
- Schnelllader
  - Info,876
  - konfigurieren,876
  - Portnummer einstellen,876
- Schnellstart
  - Transportschichtsicherheit,1446
- Schnittstellenbezeichner
  - IPv6-Adressen,107
  - unter Linux erforderlich,107
- Schnittstellenbibliotheken
  - ermitteln,80
  - Verbindungen,5
- Schnittstellennamen
  - IPv6-Adressen,107
- Schrägstriche
  - nicht zulässig in Datenbankservernamen,267
- Schreib-Prüfsummen
  - wc, Datenbankserveroption,304
  - automatisch,1085
  - I/O-Vorgänge,1085
  - Info,1084
- Schreibgeschützt
  - sm option,331
  - Datenbanken,170
  - Zugriff auf Spiegeldatenbanken,1473
- Schreibgeschützte Datenbank
  - r, Datenbankoption,329
- Schreibgeschützte Datenbanken
  - r, Datenbankserveroption,277
  - Datenbankspiegelung,543
  - Scale-Out,543
- Schreibvorgang, Prüfsummen
  - Validierungs-Dienstprogramm (dbvalid),1021
- Schriftarten
  - Einstellungen für den Code-Editor,800
- Schritt für Schritt
  - Interactive SQL,819
- Schwedisch
  - UCA-Kollation,523
- Schwerwiegende Fehler
  - uf, Serveroption,298
  - ufd, Serveroption,299
  - berichten,1108
- scjview
  - Info,5
- scjview.exe
  - Schnelllader-Option,876
- search\_timeout-Parameter
  - LDAP,110
- secure\_feature\_key, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- secure\_feature\_key-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- secure\_feature\_key-Option
  - Beschreibung,669
- SecureFeatures-Eigenschaft
  - sf, Serveroption,280
- Seiten
  - Belegung in Datenbankdatei anzeigen,925
  - Schreib-Prüfsummen,1085
  - Transaktionslog,136
- Seitengrößen
  - auswählen,927
  - Datenbanken,927
  - Optionen,160
  - zulässiges Maximum,249
- Seitennutzung
  - Informationsdienstprogramm (dbinfo),926
- Selbstsignierte Zertifikate
  - erstellen, für Transportschichtsicherheit,1448
  - Transportschichtsicherheit,1447
- Selbstsignierte Zertifikate einrichten
  - Transportschichtsicherheit,1448
- SELECT ANY TABLE-Systemprivileg
  - Beschreibung,1309
- SELECT-Privileg
  - Info,1305
- Selektivitätsschätzungen
  - user\_estimates-Option,702
- SELinux, Richtlinien
  - SQL Anywhere-Richtlinie verwenden,1403
- Semikola
  - in Verbindungszeichenfolgen verwenden,31
- SEND EMAIL-Systemprivileg
  - Beschreibung,1309

- 
- SendBufferSize, Protokolloption
    - Beschreibung, 416
  - Senden
    - Perfomancedaten, 1108
  - SendFail-Eigenschaft
    - Serveireigenschaft, Beschreibung, 745
  - SendFail-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent, OID, 1234
  - SendingTracingTo, Eigenschaft
    - Datenbankeigenschaft, Beschreibung, 767
  - SendingTracingTo-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248
  - Sequenzen
    - entziehen, REVOKE USAGE ON SEQUENCE (nicht mehr empfohlen), 1397
    - erteilen, GRANT USAGE ON SEQUENCE (nicht mehr empfohlen), 1393
  - Sequenzgeneratoren
    - Privilegien, 1305
  - Server
    - alternative Namen angeben, 332
    - automatisch starten, 83
    - Datenbank ohne Verbindung starten, 157
    - Datenbank stoppen, 158, 159
    - Datenbankfunktionen sichern, 1415
    - Eigenschaften, 745
    - Fehlerbehandlung beim Serverstart, 1109
    - hohe Verfügbarkeit bei Datenbankspiegelung, 1467
    - mit Transportschichtssicherheit starten, 1454
    - Namen-Kürzungslänge, 267
    - Namenseinschränkungen, 267
    - schreibgeschützter Zugriff, Datenbankspiegelung, 331
    - suchen, 960
    - Verbindungen begrenzen, 244
    - verwalten, 974
    - von Batchdateien starten, 983
    - zum Stoppen erforderliche Privilegien, 242
  - SERVER OPERATOR-Systemprivileg
    - Beschreibung, 1309
  - Server überprüfen
    - SQL Anywhere-Transportschichtssicherheit, 1455
  - Server, Multiprogramming-Stufe
    - automatische Optimierung, 175
  - server, Parameter
    - LDAP, 110
  - Server-Startoptionen, Optionen
    - unter Linux verwenden, 302
  - Server-StartoptionenFenster
    - unter Windows Mobile verwenden, 452
  - Server-Verbindungsparameter
    - Info, 383
  - Serverauflistung, Dienstprogramm (dblocate)
    - Beendigungscodes, 963
    - Syntax, 960
  - Serverauthentifizierung
    - MobiLink-Transportschichtssicherheit, 1461
    - SQL Anywhere-Transportschichtssicherheit, 1455
  - Serverdaten
    - sasrv.ini, 94
  - ServerEdition, Eigenschaft
    - Serveireigenschaft, Beschreibung, 745
  - ServerEdition-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent, OID, 1237
  - Serveireigenschaften
    - alphabetische Liste, 745
    - Berichte, 955
    - Groß-/Kleinschreibung, 744
    - mit dem SQL Anywhere SNMP-Erweiterungsagenten abfragen, 1225
    - mit dem SQL Anywhere SNMP-Erweiterungsagenten setzen, 1226
    - OIDs für den SQL Anywhere SNMP-Erweiterungsagenten, 1237
  - ServerIdle, Systemereignis
    - Beispiel, 1094
    - Beschreibung, 1093
  - Serverlizenzierung, Dienstprogramm (dblic)
    - Beendigungscodes, 967
    - Syntax, 964
  - Servermeldungen
    - Anzeige auf Mac OS X, 300
    - anzeigen, 275
    - auf Mac OS X anzeigen, 300
    - Ausgabe in Datei, 268
    - Ausgabe in eine Datei und Kürzen der Datei, 271
    - Cache-Vorwärmung, 227
    - Größe der Logdatei begrenzen, 270
    - Linux im Shell-Modus, 297
    - Linux-Anzeige von Servermeldungen, Fenster, 302
    - Linux-Anzeige von Servermeldungen-Fenstern und Datenbank starten, 300
    - Logdatei umbenennen und neu starten, 269
-

- Startfehler protokollieren,269
  - unter Solaris anzeigen,297
- Servermeldungen und ausgeführte SQL,  
Fensterausschnitt
  - Info,164
- Servername
  - Groß-/Kleinschreibung berücksichtigen,162
  - Serverauflistung, Dienstprogramm (dblocate),961
  - Stopp (dbstop), Syntax,984
- ServerName, Eigenschaft
  - Servereigenschaft, Beschreibung,745
- ServerName, Verbindungsparameter
  - mit gespiegelten Datenbanken verbinden,1472
  - Zeichensätze,36
- ServerName-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent,  
OID,1237
- ServerName-Verbindungsparameter
  - eingebettete Datenbanken,28
  - Info,383
  - Zeichensätze,36
- Servernamen
  - Option -n,266
- ServerNodeAddress, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ServerNodeAddress-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Serveroptionen
  - bei Windows Mobile-Datenbanken angeben,1442
  - Datenbank,321
  - Datenbankserver (Datenbank),203
  - nicht unterstützte Option unter Windows  
Mobile,426
  - Wiederherstellung,234
- ServerPort, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- ServerPort-Protokolloption
  - Beschreibung,416
- Serverseitig
  - ec, Serveroption,230
  - ek, Serveroption,326
  - ep, Serveroption,233
  - es, Serveroption,234
  - parallele Sicherungen,1080
  - Sicherungen,1036
  - Sicherungen, Kurzeinführung,1027
- serverseitig
  - Sicherungen mit dem Dienstprogramm  
dbbackup,1040
  - serverseitige Sicherungen
    - dbbackup, Dienstprogramm,1040
  - Serverstart im Hintergrund (dbspawn),  
Dienstprogramm
    - Beendigungscode,984
    - Syntax,983
  - Serverstatistiken
    - mit dem SQL Anywhere SNMP-  
Erweiterungsagenten abfragen,1225
    - OIDs für den SQL Anywhere SNMP-  
Erweiterungsagenten,1234
  - Serverstopp [dbstop], Dienstprogramm  
verwenden,154
  - Serverstopp-Dienstprogramm (dbstop)
    - Beendigungscode,986
    - mit SQLCONNECT verwenden,986
    - Privilegien,242
    - Syntax,984
  - Serververbindungsparameter
    - mit gespiegelten Datenbanken verbinden,1472
  - Serverzertifikate
    - globale Zertifikate für Transportschichtssicherheit  
verwenden,1452
  - SessionCreateTime, Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - SessionID, Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - SessionLastTime, Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - SessionTimeout-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - SET ANY PUBLIC OPTION-Systemprivileg
    - Beschreibung,1309
  - SET ANY SECURITY OPTION-Systemprivileg
    - Beschreibung,1309
  - SET ANY SYSTEM OPTION-Systemprivileg
    - Beschreibung,1309
  - SET ANY USER DEFINED OPTION-Systemprivileg
    - Beschreibung,1309
  - SET OPTION, Anweisung
    - verwenden,566
  - SET OPTION-Anweisung
    - Interactive SQL-Optionen,851
  - SET TEMPORARY OPTION, Anweisung
    - verwenden,566
  - SET USER-Systemprivileg

- 
- andere Benutzer impersonieren,1358
  - Beschreibung,1309
  - erneut erteilen, um Einstellungen anzuhängen oder zu ersetzen,1358
  - erteilen,1358
  - Info,1358
  - set-Schlüsselwort
    - kann nicht deaktiviert werden ,641
  - SetupVSPackage.exe
    - erweiterte Privilegien eventuell unter Windows 7 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Server 2008 erforderlich,202
    - erweiterte Privilegien eventuell unter Windows Vista und später erforderlich,202
  - Setzen
    - temporäre Optionen,565
  - Shared Memory
    - CommLinks-Verbindungsparameter,345
    - Serverkonfiguration,305
    - Terminalsdiene,104
    - Verbindungen unter Unix sichern,1407
  - Shell-Modus
    - Datenbankservermeldungen anzeigen,297
  - SHLIB\_PATH, Umgebungsvariable
    - Beschreibung,477
  - Sichere Funktionen
    - secure\_feature\_key-Option,669
  - Sichere Socket-Ebenen
    - Info,1444
  - Sicherheit
    - ec, Serveroption,230
    - ek, Serveroption,326
    - ep, Serveroption,233
    - es, Serveroption,234
    - AES-Verschlüsselung,1425
    - Ansichten,1403
    - Auditing,1416
    - Auditing-Abruf,1420
    - auditing-Option,582
    - Beispiel für ein Ereignis,1094
    - DatabaseKey-Verbindungsparameter (DBKEY),353
    - Dateizugriff,242
    - Daten entladen,1408
    - Daten laden,1408
    - Datenbankdateien kopieren,76
    - Datenbankdateien verschlüsseln,1424
    - Datenbanken erstellen,1408
    - Datenbanken löschen,1408
    - Datenbankfunktionen sichern,1415
    - Datenbankserver,1408
    - Dienste,187
    - Dienstprogramm zum Verschleiern von Dateien (dbfhide),922
    - Dienstprogramm Datenbank,255
    - einfache Verschlüsselung Initialisierungsdateien hinzufügen,922
    - FIPS,1445
    - Info,1402
    - integrierte Logins,1409
    - Kennwörter,1410
    - minimale Kennwortlänge,637
    - Prozeduren,1403,1405
    - Rollen,1271
    - rollenbasierte Zugriffssteuerung,1271
    - SQL Anywhere unter Vista betreiben,202
    - SQL Anywhere unter Windows 7 ausführen,202
    - SQL Anywhere unter Windows Server 2008 ausführen,202
    - Systemfunktionen,1406
    - Systemprivilegien,1271
    - temporäre Dateien,475
    - Tipps,1406
    - Transportschichtssicherheit, Info,1444
    - Überblick,1402
    - Verbindungsparameter Encryption (ENC),359
    - Windows Mobile,1442
  - Sichern und Wiederherstellen
    - Überblick,1027
  - Sicherungen
    - Abfolgeplanung,1063
    - Archiv,1034
    - Archivsicherungen mit SQL erstellen,1038
    - Archivsicherungen mit Sybase Central erstellen,1041
    - auf Bandlaufwerken mit SQL,1038
    - auf Bandlaufwerken mit Sybase Central,1041
    - automatische,1063
    - bei aktivem Sandboxing erstellen,1412
    - clientseitig, Kurzeinführung,1028
    - Datenbankdokumentation erstellen,814
    - Datenbanken außerhalb von Replikationssystemen,1078
    - Datenbanken mit Interactive SQL aus Archiven wiederherstellen,1051

- Datenbanken mit Sybase Central aus Archiven wiederherstellen,1050
- Datenbanken über Live-Sicherungen neu starten,1052
- Datenbankspiegelung,1487
- dbmlsync,1068
- dbremote,1068
- Einführung,1027
- Einschränkungen,1036
- entfernte Datenbanken,1069
- Format wählen,1033
- in Datei mit SQL,1038
- in Datei mit Sybase Central,1041
- Info,1027
- inkrementelle,1031
- interne Abläufe,1075
- Komponenten,1076
- Kurzeinführung,1027
- laufende Datenbank,1027
- live,1032
- Live-Sicherungen erstellen,1044
- mit MobiLink konsolidierte Datenbanken,1078
- MobiLink, entfernte SQL Anywhere-Datenbanken,1068
- Monitor ,1191
- nicht abgeschlossen,141
- nur Datenbank,886
- offline,1027
- online,1027
- Optionen,886
- parallele,1080
- planen,1063
- serverseitig, Kurzeinführung,1027
- serverseitige Sicherungen mit dem Dienstprogramm dbbackup erstellen,1040
- Sicherungen, Dienstprogramm (dbbackup),886
- Sicherungs-Transaktionslog umbenennen,1073,1074
- Sicherungskopien mit SQL erstellen,1039
- Sicherungskopien mit Sybase Central erstellen,1041
- SQL Remote,1068
- Transaktionslogs mit dem Dienstprogramm dbbackup umbenennen,1072
- Transaktionslogs mit der Befehlszeile kürzen,1072
- Transaktionslogs mit SQL kürzen,1071
- Transaktionslogs mit SQL umbenennen,1071
- Transaktionslogs mit Sybase Central kürzen,1070
- Transaktionslogs mit Sybase Central umbenennen,1070
- Typen vergleichen,1029
- umbenennen und neues Transaktionslog starten,886
- unter Windows Mobile durchführen,449
- validieren,1045,1080
- vollständig,1030
- Wiederherstellungspläne implementieren,1062
- Windows Mobile-Datenbank,449
- Sicherungen, automatische Info,1063
- Sicherungen, Dienstprogramm (dbbackup) Syntax,886
- Sicherungsabbild erstellen mit dem Sicherungsdienstprogramm (dbbackup),886
- Sicherungsdienstprogramm (dbbackup) Beendigungscode,891
- Fehlermeldungen,886
- Live-Sicherungen,1044
- Sicherungsdienstprogramm [dbbackup] clientseitige Sicherungen,1043
- Sicherungsformate Typen,1033
- Sicherungskopien BACKUP-Anweisung,1039
- dbbackup, Dienstprogramm,1040
- Definition,1033
- Fehlermeldungen von dbbackup,886
- Info,1035
- mit Sicherungsprogramm (dbbackup) ausführen,886
- parallele,1080
- Sybase Central,1041
- ursprüngliche Transaktionslog umbenennen,1073,1074
- wiederherstellen,1049
- Sicherungskopien erstellen, Assistent verwenden,1041
- Sicherungspläne Datenbank dokumentieren,814
- Info,1061
- Sicherungsverzeichnis Sicherungsdienstprogramm (dbbackup),886
- Signaturen für authentifizierte Anwendungen beziehen,195
- Signieren

- 
- ausführbare Dateien für Windows 7,203
  - ausführbare Dateien für Windows Server 2008,203
  - ausführbare Programme für Vista,203
  - RSA-Zertifikate,894
  - Signierte Zertifikate
    - Transportschichtsicherheit,1451
  - Signierte Zertifikate erstellen
    - Transportschichtsicherheit,1451
  - Sitzungen
    - für die Ereignisprotokollierung erstellen,1103
    - für die Ereignisprotokollierung starten,1104
    - für die Ereignisprotokollierung stoppen,1104
  - Skriptausführung, Dienstprogramm (dbrunsql)
    - Syntax,959
  - Skripten-Verzeichnis
    - Info,483
  - Smartphone
    - Einschränkungen für SQL Anywhere Server,431
  - SMP
    - gt, Datenbankserveroption,251
    - Anzahl von Prozessoren,169
  - Snapshot-Isolation
    - isolation\_level-Datenbankoption,619
    - updatable\_statement\_isolation-Option,700
  - SnapshotCount, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - SnapshotCount-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - SnapshotCount-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1244
  - SnapshotIsolationState, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - SnapshotIsolationState-Eigenschaft
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1248
  - Snapshots
    - Point-in-time,1042
  - SNDBUFSZ, Protokolloption
    - Beschreibung,416
  - SNMP
    - Agenten,1217
    - dynamische Traps,1228
    - Info,1217
    - installieren,1221
    - Manager,1217
    - SQL Anywhere SNMP-Erweiterungsagent verwenden,1216
    - Traps,1217
    - Traps senden,1227
    - Traps verwenden,1227
  - SNMP-Dienst
    - neu starten,1221
  - SNMPv2-SMI.mib
    - Info,1216
  - SNMPv2-TC.mib
    - Info,1216
  - Software
    - aktualisieren,879
    - Datenbankserver lizenzieren,964
    - Version,303,1024
  - Software-Updates
    - abrufen,879
  - Softwarelizenzen
    - Server lizenzieren,964
  - Softwareversion
    - Datenbankserver,303
  - Solaris
    - IPv6-Unterstützung,106
    - LD\_LIBRARY\_PATH-Umgebungsvariable,469
    - Servermeldungen im Shell-Modus anzeigen,297
    - Verbindung mit der Beispieldatenbank herstellen,7
  - Sommerzeit
    - geplante Ereignisse,1097
  - sort\_collation-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - sort\_collation-Option
    - Beschreibung,670
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1253
  - Sortieren
    - Ergebnismengen,830
  - Sortierreihenfolge
    - Info,497
  - Sortierreihenfolgen
    - Kollationen,493
  - SortMergePasses, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
    - Verbindungseigenschaft, Beschreibung,711
  - SortRowsMaterialized, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
    - Verbindungseigenschaft, Beschreibung,711
  - SortRunsWritten, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
    - Verbindungseigenschaft, Beschreibung,711
  - SortSortedRuns, Eigenschaft

- Datenbankeigenschaft, Beschreibung,767
- Verbindungseigenschaft, Beschreibung,711
- SortWorkTables, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- sp\_login\_environment-Systemprozedur
  - mit der Option login\_procedure verwenden,625
- Spalte kopieren
  - in Interactive SQL,834
- Spalten
  - benennen,122
  - Datentyp wählen,122
  - Einschränkungen,791
  - in Interactive SQL nachschlagen,828
  - Integritätsregeln,125
  - Komprimierung,124
  - NULL zulassen,122
  - Privilegien,1305
  - Verschlüsselung,1435
  - Verschlüsselung (RAW),1436
- Spaltenkomprimierung
  - Info,124
- Spaltennamen
  - internationale Aspekte,505
- Spaltenprivilegien
  - festlegen,1305
- Spaltenstatistiken
  - collect\_statistics\_on\_dml\_updates-Option,591
- Speicher
  - anfängliche Cachegröße festlegen,217
  - anfängliche statische Cachegröße festlegen,219
  - Anforderungen,794
  - maximale Cachegröße festlegen,221
  - minimale Cachegröße festlegen,224
- Speicherkarten
  - Windows Mobile,430
- Speicherplatz
  - Dateisystem voll, Callback-Funktion,235
- Speicherplatz auf der Festplatte
  - mit dbinfo die Größe einer Tabelle auf der Festplatte ermitteln,926
- Sperren
  - Spiegeldatenbanken,1473
- Sperrenkonflikte
  - blocking-Option,585
  - blocking\_timeout-Option,587
- Spiegeldatenbanken
  - abfragen,1473
  - schreibgeschützter Zugriff,1473
- Spiegeln
  - sm, Option,331
- Spiegelserver
  - Datenbankspiegelung, Übersicht,1467
  - löschen,1490
  - schreibgeschützter Datenbankzugriff,1473
  - stoppen,1490
  - Unterschiede zu Kopieknoten,1539
- Spiegelung
  - Asynchron-Ganzseiten-Modus,1478
  - asynchroner Modus,1478
  - Clientverbindungen,1472
  - Datenbankserver stoppen,1490
  - den Primärserver bestimmen,1483
  - Einschränkungen,1475
  - Info,1467
  - konfigurieren,1480
  - mit Webdiensten verwenden,1540
  - MobiLink,1470
  - nach einem Primärserver-Ausfall wiederherstellen,1499
  - Option -sn,332
  - Option -xa,306
  - Option -xf,308
  - Option -xp,335
  - Performance,1476
  - Praktische Einführung,1509
  - praktische Einführung mit gemeinsamem Arbiterserver,1516
  - Rolle des Arbiterservers,1468
  - Sicherungen,1487
  - Statusinformationsdateien,1498
  - Synchroner Modus,1478
  - Synchronisationsmodi,1477
  - Synchronisationsstatus,1480
  - synchronize\_mirror\_on\_commit-Option setzen,688
  - Systemereignisse,1093
  - Szenarien,1501,1504
  - Transaktionslog,138
  - Trap des SQL Anywhere SNMP-Erweiterungsagenten,1227
  - zu Scale-Out mit Schreibschutz hinzufügen,1555
- Spiegelungssysteme
  - Info,1467
- Sprachauswahl-Dienstprogramm (dblang)
  - Beendigungscodes,947
  - Syntax,946

- 
- Sprachcodes
    - Sprache, Dienstprogramm (dblang),946
  - Sprache
    - DLL-Registrierungseinstellungen,946
  - Spracheinstellungen
    - Zeichensatzkonvertierungen,502
  - Sprachen
    - angeben,473
    - Datenbanken erstellen,522
    - Groß-/Kleinschreibung,505
    - in der Client/Server-Umgebung,498
    - lokalisierte Versionen von SQL Anywhere,493
    - nicht englische Datenbanken,493
    - Registrierungseinstellungen,490
    - Software und Dokumentation,494
    - Sprachauswahl-Dienstprogramm (dblang),946
    - Sprachumgebung,510
    - Türkisch,532
    - vom Datenbankserver verwendete Sprache bestimmen,512
    - von der CHAR-Kollation unterstützte Sprachen bestimmen,512
  - Sprachen-DLL
    - Position ermitteln,484
  - Sprachen-Labels
    - Liste der Werte,510
  - Sprachen-Ressourcebibliothek
    - Nachrichtendatei,498
    - Registrierungseinstellungen,946
  - Sprachumgebungen
    - Definition,509
    - ermitteln,512
    - festlegen,514
    - Info,509
    - Sprache,510
    - Zeichensätze,512
  - Sprachunterstützung
    - Info,493
    - Mehrbyte-Zeichensätze,514
  - SQL
    - unter Windows Mobile nicht unterstützte Anweisungen,425
  - SQL Anweisungen
    - Dienstprogrammdatenbank,145
  - SQL Anywhere
    - als Open Server einrichten,1570
    - authentifizierte Anwendungen,194
    - Clientanwendungen für die Verwendung der Transportschichtssicherheit konfigurieren,1455
    - Datenbanken für Windows Mobile konfigurieren,439
    - Datenbankserver für die Verwendung der Transportschichtssicherheit konfigurieren,1454
    - Fehlerbehandlung,1107
    - internationale Funktionen,491
    - lokalisierte Versionen,493
    - Software-Updates,879
    - SQL Anywhere installieren,430
    - SQL Anywhere verwenden,423
    - über Datenquellen verbinden,19
    - über Verwendung von Datenquellen verbinden (Dienstprogramm dbisql),20
    - unter Vista betreiben,202
    - unter Windows 7 ausführen,202
    - unter Windows Mobile nicht unterstützte Funktionen,423
    - unter Windows Mobile verwenden,423
    - Webserver für die Verwendung der Transportschichtssicherheit konfigurieren,1458
  - SQL Anywhere 16-Plug-In
    - Anwendungsprofil-Modus,808
    - Debug-Modus,808
    - Planungsmodus ,808
    - Überblicks-Registerkarte,812
    - verwenden,808
  - SQL Anywhere JDBC-Treiber
    - nicht unterstützt,423
  - SQL Anywhere MIB
    - Agent-Tabelle,1230
    - Datenbankeigenschaften,1248
    - Datenbankoptionen,1253
    - Datenbankstatistiken,1244
    - saDbPropMetaDataTable,1233
    - saDbStatMetaDataTable,1232
    - saMetaData tables,1231
    - saSrvPropMetaDataTable,1232
    - saSrvStatMetaDataTable,1231
    - Serveereigenschaften,1237
    - Serverstatistiken,1234
    - Tabellenliste,1230
  - SQL Anywhere MIB, Referenzhandbuch
    - Übersicht,1230
  - SQL Anywhere MIB-Datenbank
    - Info,1217
    - saDbOptMetaDataTable,1233

- SQL Anywhere ODBC-Treiber
  - Info,38
- SQL Anywhere OEM Edition
  - Anwendung entwickeln,194
  - Anwendungsauthentifizierung,197
  - Authentifizierungssignaturen,195
  - connection\_authentication-Option,593
  - database\_authentication-Option,597
  - Datenbankauthentifizierung,195
  - Info,194
  - Upgrade von Datenbanken,200
  - Verbindungen authentifizieren,198
- SQL Anywhere SNMP, Erweiterungsagent
  - gespeicherte Prozeduren ausführen,1226
  - Info,1216
  - unterstützte Plattformen,1216
- SQL Anywhere SNMP-Erweiterungsagent
  - dynamische Traps,1228
  - Funktionen ausführen,1226
  - konfigurieren,1221
  - neu starten,1221
  - sasnm.ini file,1222
  - unterstützte MIB-Datenbanken,1217
- SQL Anywhere VSS-Schreibprogramm
  - dbvss16.exe,1042
- SQL Anywhere, Transportschichtsicherheit
  - Info,1444
- SQL Anywhere-Kollationsalgorithmus (SACA)
  - Info,515
- SQL Anywhere-Konsolendienstprogramm (dbconsole)
  - Benutzer trennen,102
  - Fenster konfigurieren,878
  - Mac OS X, Hardwareanforderungen,877
  - Software-Updates,879
  - Syntax,981
  - verwenden,877
- SQL Anywhere-ODBC-Treiber
  - Versionen mit oder ohne Threading,45
- SQL Anywhere-Oracle-ODBC-Treiber
  - Datenquellen erstellen,906
- SQL Anywhere-Supportanfragen (dbsupport), Dienstprogramm
  - SADIAGDIR-Umgebungsvariable,473
- SQL Anywhere-Umgebungsvariablen
  - als Source unter Unix nehmen,467
  - Info,467
  - setzen,467
- Unix,467
  - unter Mac OS X setzen,468
  - unter Windows einrichten,467
- SQL Anywhere-Volumeschattenkopie-Dienst (VSS)
  - Typen der Sicherung,1042
- SQL Anywhere-VSS-Schreibprogramm
  - vss, Datenbankserveroption,303
- SQL Flagger
  - sql\_flagger\_error\_level-Option,671
  - sql\_flagger\_warning\_level-Option,672
- SQL Remote
  - SQL Remote-Replikationsoptionen,563
  - Transaktionslog automatisch umbenennen,1070
  - unter Windows Mobile nicht unterstützte Funktionen,429
- SQL, Befehlsdateien
  - in Interactive SQL öffnen,817
- SQL, Dateiformat
  - Interactive SQL, Ausgabe,866
- SQL-Abfragen
  - mit dem Abfrage-Editor erstellen,837
- SQL-Anweisungen
  - ausführen,819
  - Client/Server,503
  - Datenbankoptionen,565
  - Einzelschritt,819
  - Favoriten bearbeiten,825
  - in Interactive ausführen,819
  - in Interactive protokollieren,826
  - in Interactive SQL protokollieren,826
  - Interactive SQL,821
  - nicht unterstützte Anweisungen unter Windows Mobile,425
  - protokollieren,164
  - Protokollierung in Sybase Central,164
  - Symbolleistenschaltfläche zum Ausführen von Anweisungen,819
  - zu Favoriten hinzufügen,824
  - zuletzt vorbereitete Anweisungen abfangen,313
- SQL-Anweisungen ausführen
  - Interactive SQL,819
- SQL-Anweisungen, Fensterausschnitt
  - Info,817
- SQL-Dateiformat
  - Dateien sichern,821
  - Interactive SQL, Standardeditor,817
- SQL-Kompatibilität
  - Datenbankoptionen,559

---

SQL-Skriptdateien  
     Favoriten bearbeiten,825  
     Interactive SQL als Standardeditor festlegen,821  
     zu Favoriten hinzufügen,824  
 SQL-Standards  
     Transact-SQL, Kompatibilitätsoptionen,560  
     UPDATE-Anweisung,948  
 SQL/2008-Konformität  
     Aktualisierungen,579  
     SQL\_FLAGGER\_ERROR-Option,671  
 sql\_flagger\_error\_level, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
     Transact-SQL-Kompatibilität,560  
 sql\_flagger\_error\_level-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 sql\_flagger\_error\_level-Option  
     Beschreibung,671  
 sql\_flagger\_warning\_level, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
     Transact-SQL-Kompatibilität,560  
 sql\_flagger\_warning\_level-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 sql\_flagger\_warning\_level-Option  
     Beschreibung,672  
 SQLANY16-Umgebungsvariable  
     Beschreibung,477  
 SQLANYSAM16-Umgebungsvariable  
     Beschreibung,478  
 SQLCONNECT, Umgebungsvariable  
     Verbindungen,30  
 SQLCONNECT-Umgebungsvariable  
     Info,479  
     mit dem dbstop-Dienstprogramm verwenden,986  
 SQLDA  
     ansi\_blanks-Option,575  
 SQLPATH, Umgebungsvariable  
     Beschreibung,480  
 SQLREMOTE, Umgebungsvariable  
     Beschreibung,480  
 SQLTables  
     MatView-Verbindungsparameter,374  
 sr\_date\_format, Option  
     SQL Remote-Option,673  
 sr\_time\_format, Option  
     SQL Remote-Option,675  
 sr\_timestamp\_format, Option  
     SQL Remote-Option,676  
 sr\_timestamp\_with\_time\_zone\_format-Option  
     SQL Remote-Option,677  
 SSPI  
     Kerberos-Logins unter Windows,72  
     von SQL Anywhere-Clients unterstützt,64  
     von SQL Anywhere-Server nicht unterstützt,64  
 st\_geometry\_asbinary\_format-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_asbinary\_format-Option  
     Beschreibung,679  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 st\_geometry\_astype\_format-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_astype\_format-Option  
     Beschreibung,680  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 st\_geometry\_asxml\_format-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_asxml\_format-Option  
     Beschreibung,681  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 st\_geometry\_describe\_type-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_describe\_type-Option  
     Beschreibung,682  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 st\_geometry\_interpolation option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 st\_geometry\_interpolation-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_interpolation-Option  
     Beschreibung,683  
 st\_geometry\_on\_invalid-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
 st\_geometry\_on\_invalid-Option  
     Beschreibung,684  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 Stack-Überlauf  
     Fehler,250  
 Stackgröße  
     externe Funktionen,241

- Maximum,250
- Stammzertifikate
  - Transportschichtssicherheit,1447
  - Transportschichtssicherheit, Client-Verifizierung,1453
- Standarddatenbankserver
  - Inf,266
- Standardeinstellung
  - Verbindungsparameter,35
- Standardkollationseigenschaft
  - abfragen,527
- Standardwerte
  - Kollation,526
  - Ports,416
- Standardzeichensatz
  - Info,512
  - Unix,512
  - Windows,512
- Starke Tabellenverschlüsselung
  - Initialisierungsdienstprogramm (dbinit),927
- Starke Verschlüsselung
  - ec, Serveroption,230
  - ek, Datenbankoption,326
  - ep, Serveroption,233
  - AES-Algorithmus,1425
  - DatabaseKey-Verbindungsparameter (DBKEY),353
  - Datenbankdateien,1424
  - Dienstprogramm zum Entladen (dbunload),1001
  - Info,1444
  - Initialisierungsdienstprogramm (dbinit),927
  - Rijndael,1425
  - SQL Anywhere-Datenbanken unter Windows Mobile,1443
  - stark verschlüsselte Datenbank erstellen,1426
- START JAVA-Anweisung
  - unter Windows Mobile nicht unterstützt,425
- START, Verbindungsparameter
  - Beschreibung,385
  - eingebettete Datenbanken,29
- StartDBPermission, Eigenschaft
  - Serveireigenschaft, Beschreibung,745
- StartDBPermission-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- Starten
  - Windows-Dienste mit Sybase Central,189
- Starten nicht möglich, Fehler
  - Ursache diagnostizieren,98
- Starten von Datenbanken
  - verbinden,28
- StartLine, Verbindungsparameter
  - Beschreibung,385
  - eingebettete Datenbanken,29
- StartTime, Eigenschaft
  - Serveireigenschaft, Beschreibung,745
- StartTime-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- StatementDescribes, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- StatementPostAnnotates, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- StatementPostAnnotatesSimple, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- StatementPostAnnotatesSkipped, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - Verbindungseigenschaft, Beschreibung,711
- Statistiken
  - Datenbankstatistiken in SQL Anywhere MIB,1244
  - dynamische Cachedimensionierung,227
  - Serverstatistiken-OIDs für den SQL Anywhere SNMP-Erweiterungsagenten,1234
  - Überblick-Register,812
- Statistikwächter
  - mit update\_statistics-Option aktivieren,701
  - mit update\_statistics-Option deaktivieren,701
- Statusinformationsdateien
  - Datenbankspiegelung,1498
  - Rolle bei Bestimmung des Primärservers,1483
- Steuerung des Thread-Verhaltens
  - Info,174
- STOP JAVA-Anweisung
  - unter Windows Mobile nicht unterstützt,425
- Stoppen
  - Datenbanken,984
  - Datenbanken (ASTOP),342
  - Windows-Dienste mit Sybase Central,189
- Storage Area Networks (SANs)
  - Datenbankdateien speichern,136
- StreamsUsed-Eigenschaft
  - Serveireigenschaft, Beschreibung,745
- string\_truncation, Option

---

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 Transact-SQL-Kompatibilität,560  
 string\_truncation-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 string\_truncation-Option  
   Beschreibung,685  
 subscribe\_by\_remote, Option  
   Replikationsoption,686  
 subscribe\_by\_remote-Option  
   SQL Remote-Replikationsoption,563  
 subsume\_row\_locks, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 subsume\_row\_locks-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 subsume\_row\_locks-Option  
   Beschreibung,686  
 Suchbedingungen  
   user\_estimates-Option,702  
 Suchen  
   in Datenbanken,799  
   Sybase Central,799  
 Suchfunktion für Updates  
   dbconsole, Dienstprogramm,881  
   Info,879  
   Interactive SQL,880  
   Sybase Central,880  
 Superuser  
   aus DBA-Berechtigung migrieren,1390  
   Info,1295  
   Tipp: Kennwörter sicher speichern,1406  
   Tipp: Superuser sparsam einsetzen,1406  
 suppress\_tds\_debugging, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 suppress\_tds\_debugging-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 suppress\_tds\_debugging-Option  
   Beschreibung,687  
 SuppressInfoForDataTypes-Verbindungsparameter  
   ODBC-Verbindungsparameter, Beschreibung,911  
 SuppressWarnings, Verbindungsparameter  
   ODBC-Verbindungsparameter, Beschreibung,911  
 SVGs  
   in Interactive SQL anzeigen,841  
 Sybase Central  
   Auditing,1418,1419  
   Code-Editor,800  
   Datenbanken löschen,149  
   Datenbankobjekte kopieren,795  
   Hardwareanforderungen für Mac OS X,5  
   Hauptfenster aktualisieren,795  
   Info,795  
   Interactive SQL starten,815  
   Log-Viewer,805  
   navigieren,796  
   Plug-In-Architektur,806  
   Registrierungseinstellungen,490  
   Schnellader konfigurieren,876  
   Software-Updates,879  
   Spalten im rechten Fensterausschnitt anpassen,798  
   SQL Anywhere 16-Plug-In,808  
   starten (Linux),5  
   starten (Mac OS X),5  
   starten (Unix),5  
   starten (Windows),5  
   Statusleiste,798  
   suchen,799  
   Suchfunktion für Updates konfigurieren,880  
   Tastenkürzel,799  
   Textvervollständigung,873  
   Transaktionslogs kürzen,1070  
   unter Windows Mobile nicht unterstützte  
   Assistenten,428  
   Verbindungsprofile,10  
   Windows Mobile, praktische Einführung,452  
 Sybase Open Client  
   ASE-Kompatibilitätsoptionen,559  
   Client-APIs und Zeichensatzkonvertierung,505  
   Kerberos-Authentifizierung,69  
   Kompatibilitäts-Datenbankoptionen,559  
   Optionen,1571  
   Schnittstelle,1569  
   unter Windows Mobile nicht unterstützt,423  
 Sybase Open Server  
   Architektur,1569  
   starten,1571  
   Systemanforderungen,1570  
 Sybase PowerBuilder DataWindow  
   Abfrageperformance,647  
 SYBASE, Umgebungsvariable  
   Beschreibung,480  
 SYBASE-MIB.mib  
   Info,1216  
 sybinit, Dienstprogramm

- Info, 1571
- Symbole
  - Fehlerbehandlung bei unerwarteten Symbolen in den Ergebnissen, 504
  - um Dienste auszuführen, 187
- Symbolleisten
  - Interactive SQL, Schaltfläche zum Ausführen von Anweisungen, 819
- Symbolleistenschaltfläche zum Ausführen von Anweisungen
  - konfigurieren, 819
- Synchron, Modus
  - Datenbankspiegelung, 1478
- Synchroner Modus
  - Fehlerbehandlung, 1499
- Synchronisation
  - Datenbankoptionen, 562
  - Datenbankspiegelung, 1477
  - default\_timestamp\_increment einstellen, 605
  - Hochverfügbarkeit, 1470
  - Sicherungen, 1068
  - SQL Remote delete\_old\_logs-Option, 607
  - Transportschichtssicherheit, 1444
  - truncate\_timestamp\_values einstellen, 698
  - verschlüsselte Datenbanken neu aufbauen, 1017
- Synchronisationsmodi
  - Datenbankspiegelung, 1477
- Synchronisationsstatus
  - Datenbankspiegelung, 1480
- SynchronizationSchemaChangeActive-Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248
- synchronize\_mirror\_on\_commit, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1253
- synchronize\_mirror\_on\_commit-Eigenschaft
  - Verbindungseigenschaft, Beschreibung, 711
- synchronize\_mirror\_on\_commit-Option
  - Beschreibung, 688
- SyncTrunc, Eigenschaft
  - Datenbankeigenschaft, Beschreibung, 767
- SyncTrunc-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID, 1248
- Syntax
  - dbbackup-Dienstprogramm, 886
  - dbconsole, Dienstprogramm, 981
  - dbdsn-Dienstprogramm, 905
  - dberase, Dienstprogramm, 916
  - dbfhide, Dienstprogramm, 922
  - dbhist, Dienstprogramm, 923
  - dbinfo, Dienstprogramm, 925
  - dbinit, Dienstprogramm, 927
  - dbisql, Dienstprogramm, 939
  - dbisqlc-Dienstprogramm, 915
  - dblang, Dienstprogramm, 946
  - dblic, Dienstprogramm, 964
  - dblocate, Dienstprogramm, 960
  - dblog, Dienstprogramm, 998
  - dbns16, Dienstprogramm, 891
  - dbping, Dienstprogramm, 955
  - dbrunsql, Dienstprogramm, 959
  - dbspawn, Dienstprogramm, 983
  - dbstats, Dienstprogramm, 953
  - dbstop, Dienstprogramm, 984
  - dbsupport, Dienstprogramm, 987
  - dbsvc, Dienstprogramm (Linux), 968
  - dbsvc, Dienstprogramm (Windows), 974
  - dbtran, Dienstprogramm, 948
  - dbunload, Dienstprogramm, 1000
  - dbupgrad, Dienstprogramm, 1017
  - dbvalid, Dienstprogramm, 1020
  - Erstellen von Zertifikaten (createcert), 894
  - Schlüsselpaargenerator-Dienstprogramm (createkey), 945
  - Verbindungsparameter, 36
  - viewcert-Dienstprogramm, 903
  - Zugriff auf Datenbankeigenschaften, 766
  - Zugriff auf Datenbankserveigenschaften, 744
  - Zugriff auf Verbindungseigenschaften, 710
- Syntaxfehler
  - Joins, 610
- SYS-Systemrolle
  - Info, 1272
- SYS\_AUTH\_BACKUP\_ROLE-Kompatibilitätsrolle
  - Info, 1275
  - Wiederherstellen (SQL), 1284
  - wiederherstellen (Sybase Central), 1283
- SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle
  - Info, 1275
  - Wiederherstellen (SQL), 1284
  - wiederherstellen (Sybase Central), 1283
- SYS\_AUTH\_PROFILE\_ROLE-Kompatibilitätsrolle
  - Info, 1275
  - Wiederherstellen (SQL), 1284

---

wiederherstellen (Sybase Central),1283	SYS_SAMONITOR_ADMIN_ROLE-Systemrolle
SYS_AUTH_READCLIENTFILE_ROLE-	Info,1272
Kompatibilitätsrolle	SYS_SPATIAL_ADMIN_ROLE-Systemrolle
Info,1275	Info,1272
Wiederherstellen (SQL),1284	Syslog
wiederherstellen (Sybase Central),1283	-Benutzer-ID,278
SYS_AUTH_READFILE_ROLE-	system, DBSpace
Kompatibilitätsrolle	Info,127
Info,1275	System-Trace-Ereignisse
Wiederherstellen (SQL),1284	Info,1101
wiederherstellen (Sybase Central),1283	Systemanforderungen
SYS_AUTH_RESOURCE_ROLE-	Veritas Cluster Server-Agenten,1527
Kompatibilitätsrolle	Systemausfall
Info,1275	Info,1067
Wiederherstellen (SQL),1284	Wiederherstellung,1067
wiederherstellen (Sybase Central),1283	Systemausfälle
SYS_AUTH_SA_ROLE-Kompatibilitätsrolle	Wiederherstellung,1027
Info,1275	Systemereignisse
Wiederherstellen (SQL),1284	BackupEnd,1091
wiederherstellen (Sybase Central),1283	Connect,1091
SYS_AUTH_SSO_ROLE-Kompatibilitätsrolle	ConnectFailed,1091
Info,1275	DatabaseStart,1091
Wiederherstellen (SQL),1284	Datenbankspiegelung,1093
wiederherstellen (Sybase Central),1283	DBDiskSpace,1092
SYS_AUTH_VALIDATE_ROLE-	Deadlock,1091
Kompatibilitätsrolle	Definition,1087
Info,1275	Disconnect,1092
Wiederherstellen (SQL),1284	Ereignisprotokollierung,1106
wiederherstellen (Sybase Central),1283	GlobalAutoIncrement,1092
SYS_AUTH_WRITECLIENTFILE_ROLE-	GrowDB,1092
Kompatibilitätsrolle	GrowLog,1092
Info,1275	GrowTemp,1092
Wiederherstellen (SQL),1284	Info,1091
wiederherstellen (Sybase Central),1283	Interna,1096
SYS_AUTH_WRITEFILE_ROLE-	LogDiskSpace,1092
Kompatibilitätsrolle	MirrorFailover,1093
Info,1275	MirrorServerDisconnect,1093
Wiederherstellen (SQL),1284	RAISERROR,1092
wiederherstellen (Sybase Central),1283	ServerIdle,1093
SYS_REPLICATION_ADMIN_ROLE-Systemrolle	TempDiskSpace,1092
Info,1273	Systeminformationsdatei
verwaltet durch MANAGE REPLICATION-	Datenquellen unter Mac OS X erstellen,45
Systemprivileg,1272	im Verbindungsparameter DSN angeben,356
SYS_RUN_REPLICATION_ROLE-Systemrolle	Info,49
Info,1273	Kennwörter speichern,378
verwaltet durch	mit Datenquellen-Dienstprogramm (dbdsn)
SYS_REPLICATION_ADMIN_ROLE-	verwenden,908
Systemrolle,1272	verschlüsselte Kennwörter speichern,358

- Systemobjekte
  - entladen,1013
- Systemprivilegien
  - alphabetische Liste,1309
  - Info,1305
  - Liste,1309
  - praktische Einführung (SQL),1378
  - praktische Einführung, Sybase Central,1371
- Systemrollen
  - Info,1272
  - Liste,1272
- Systemschlüssel für gesicherte Funktionen
  - Info,1413
  - mit -sk angeben,288
- Systemtabellen
  - preserve\_source\_format,655
  - prevent\_article\_pkey\_update,655
  - Quellspalte,655
- Szenarien
  - Failover in einem Datenbankspiegelungssystem,1501,1504

## T

- Tabellen
  - aus Sybase Central validieren,1086
  - belegten Speicherplatz auf der Festplatte ermitteln,926
  - benennen,122
  - Eigentümer,1348
  - Einschränkungen,791
  - entschlüsseln,1437
  - in Interactive SQL nachschlagen,828
  - Integritätsregeln,125
  - Tabellenverschlüsselung aktivieren (dbinit),1440
  - Tabellenverschlüsselung aktivieren (SQL),1438
  - verschlüsseln,1437
- Tabellengröße
  - Anzahl der Zeilen,791
  - Grenze,791
- Tabellennamen
  - internationale Aspekte,505
- Tabellenprivilegien
  - festlegen,1305
- Tabellenverschlüsselung
  - Info,1437
  - Initialisierungsdienstprogramm (dbinit),927
- Tabellenwerte
  - in Interactive SQL bearbeiten,831
- Tabular Data Stream (TDS), Kommunikationsprotokoll
  - Sybase Open Server,1569
- Task-Liste
  - anzeigen,796
- Tastaturzuordnung
  - Info,497
- Tastenbelegung
  - Sybase Central,799
- Tastenkürzel
  - Code-Editor,801
  - Interactive SQL,845
  - Sybase Central,799
  - Textvervollständigung,875
- TCP/IP
  - x, Datenbankserveroption,305
  - Abhängigkeiten von Diensten einstellen,976
  - bei Datenbankspiegelung erforderlich,1475
  - BroadcastListener-Protokolloption (BLISTENER),391
  - ClientPort-Protokolloption (CPORT),395
  - Firewalls und LDAP-Server,109
  - Host-Protokolloption (IP),399
  - Info,105
  - IPv6-Unterstützung,106
  - kennzeichnende Ports,416
  - LDAP, Protokolloption,406
  - MobiLink TLS für SQL Anywhere-Clients,1463
  - MobiLink-TLS für UltraLite-Clients,1464
  - Portnummer,418
  - Protokolloptionen,389
  - Server über Firewalls auffinden,963
  - Serverkonfiguration,388
  - ServerPort-Protokolloption (PORT),416
  - starten,103
  - über Firewalls verbinden,107
  - unterstützte Protokolle,102
  - verbinden,25
  - Verschlüsseln der Client/Server-Kommunikation,106
  - Windows,106
- TcpIpAddresses, Eigenschaft
  - Serveereigenschaft, Beschreibung,745
- TcpIpAddresses-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- TDI

- 
- Abhängigkeiten von Diensten einstellen,976
  - TDS
    - Info,1569
  - TDS, Protokolloption
    - Beschreibung,419
  - tds\_empty\_string\_is\_null, Option
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1253
  - tds\_empty\_string\_is\_null-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - tds\_empty\_string\_is\_null-Option
    - Beschreibung,689
  - Technischer Kundendienst
    - Datenbanken für den technischen Kundendienst verschlüsseln,1109
    - Verschlüsseln von Datenbanken,1431
  - temp, DBSpace
    - Info,127
  - TEMP, Umgebungsvariable
    - Beschreibung,481
    - Festplattenspeicher,1110
    - Windows Mobile,491
  - temp\_space\_limit\_check, Option
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1253
  - temp\_space\_limit\_check-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - temp\_space\_limit\_check-Option
    - Beschreibung,689
  - TempDir-Eigenschaft
    - Servereigenschaft, Beschreibung,745
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1237
  - TempDiskSpace, Systemereignis
    - Beschreibung,1092
  - TempFileName, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1248
  - TempFilePages-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - Temporäre Dateien
    - begrenzen,791
    - maximaler Speicher von Verbindungen,689
    - Sicherheit,475
    - Speicherort mit SATMP -Umgebungsvariable festlegen,475
    - Speicherort mit TEMP-Umgebungsvariable festlegen,481
    - Speicherort mit TMP-Umgebungsvariable festlegen,481
    - Speicherort mit TMPDIR-Umgebungsvariable festlegen,481
    - Speicherort unter Windows Mobile,491
    - Standort mit Serveroption -dt angeben,228
    - temp\_space\_limit\_check-Option,689
    - Unix-Verbindungen über gemeinsam genutzten Speicher,476
  - Temporäre Optionen
    - Bereich und Dauer,565
    - einstellen,566
    - integriertes Login, Sicherheit,76
    - Kerberos-Login, Sicherheit,76
  - Temporäre Tabellen
    - Einschränkungen,791
  - Temporäre Verbindungen
    - Info,78
  - Temporärer DBSpace
    - Privilegien,129
  - Temporärer Speicher
    - begrenzen,636
  - temporary DBSpace
    - Info,127
  - TempTablePages, Eigenschaft
    - Datenbankeigenschaft, Beschreibung,767
  - TempTablePages-Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - TempTablePages-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent,OID,1244
  - Terminaldienste
    - Verbindungen über gemeinsam genutzten Speicher,104
  - Text, Dateiformat
    - Interactive SQL, Eingabe,857
    - Interactive SQL-Ausgabe,866
  - Textpläne
    - UltraLite-Plananzeige,839
  - Textvervollständigung
    - konfigurieren,873
    - Tastenkürzel,875
    - verwenden,873
  - Thread-Deadlock
    - Beziehung zur Multiprogramming-Stufe,179
  - ThreadDeadlocksAvoided-Eigenschaft

- Servereigenschaft, Beschreibung,745
- ThreadDeadlocksAvoided-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- ThreadDeadlocksReported-Eigenschaft
  - Servereigenschaft, Beschreibung,745
- ThreadDeadlocksReported-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- Threading
  - Info,171
- Threads
  - gn dbsrv16-Serveroption,244
  - gna dbsrv16-Serveroption,245
  - gnh dbsrv16-Serveroption,246
  - gnl dbsrv16-Serveroption,247
  - in SQL Anywhere,172
  - Linux,173
  - mehrere Prozessoren,251
  - Unix-Verhalten,173
  - Verhalten steuern,174
  - Windows,173
- Threads in SQL Anywhere
  - Info,171
- Ticket-erteilende Tickets
  - Kerberos,67
- time\_format, Option
  - ASE-Kompatibilität,559
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- time\_format-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- time\_format-Option
  - Beschreibung,690
  - Sybase Open Client,1571
- time\_zone\_adjustment, Option
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- time\_zone\_adjustment-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- time\_zone\_adjustment-Option
  - Beschreibung,691
- Timeout
  - Fehlerbehandlung,1114
- Timeout-Protokolloption
  - Beschreibung,420
- Timeouts
  - request\_timeout-Option,664
- TIMESTAMP, Datentyp
  - default\_timestamp\_increment-Option,605
- TIMESTAMP-Datentyp
  - Dezimalstellen in Vergleichen,605
- timestamp\_format, Option
  - ASE-Kompatibilität,559
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
  - Transact-SQL-Kompatibilität,560
- timestamp\_format-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- timestamp\_format-Option
  - Beschreibung,692
  - Sybase Open Client,1571
- timestamp\_with\_time\_zone\_format-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- timestamp\_with\_time\_zone\_format-Option
  - Beschreibung,694
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- TimeZoneAdjustment, Eigenschaft
  - Servereigenschaft, Beschreibung,745
  - Verbindungseigenschaft, Beschreibung,711
- TimeZoneAdjustment-Eigenschaft
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1237
- TLS
  - Info,1444
  - MobiLink mit Punkt zu Punkt-Verschlüsselung,1459
  - MobiLink-Clients (SQL Anywhere),1463
  - MobiLink-Clients (UltraLite),1464
  - Monitor,1197
  - Protokolloptionen,389
  - unter Windows Mobile nicht unterstützt,426
  - Unterstützung,1445
- TLS, Synchronisation
  - Info,1444
- TLS, Unterstützung
  - Info,1445
- TMP, Umgebungsvariable
  - Beschreibung,481
  - Windows Mobile,491
- TMPDIR, Umgebungsvariable
  - Beschreibung,481
  - Windows Mobile,491
- TO, Protokolloption

- 
- Beschreibung,420
  - TotalBuffers, Eigenschaft
    - Servereigenschaft, Beschreibung,745
  - TotalBuffers-Statistik
    - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
  - Trace-Ereignisse
    - Info,1101
    - Sitzungen erstellen,1103
    - Sitzungen über die Befehlszeile einstellen,294
  - Trace-Sitzungen
    - Info,1101
  - trace\_system\_event
    - gesicherte Funktion,1413
  - trace\_system\_event-Funktion
    - sf, Serveroption,280
  - tracetime.pl
    - Analysieren von Dateien des Anforderungsprotokolls,631
  - Transact-SQL
    - allow\_nulls\_by\_default-Option,572
    - im Abfrage-Editor nicht unterstützt,837
    - Kompatibilitäts-Datenbankoptionen,559
    - Kompatibilitätsoptionen,560
    - NULL-Verhalten,580
    - Privilegien aktualisieren,577
    - Privilegien löschen,577
    - quoted\_identifizier-Option,660
    - Spalten-NULL-Kompatibilität,660
  - TransactionStartTime, Eigenschaft
    - Verbindungseigenschaft, Beschreibung,711
  - Transaktionen
    - Cursor schließen,590
    - Datenbankspiegelung,1477
    - Event-Handler-Verhalten,1098
    - nicht festgeschriebene mit der Befehlszeile,1048
    - nicht festgeschriebene mit Sybase Central,1048
    - wiederherstellen, wenn Transaktionen sich über mehrere Transaktionslogs erstrecken,1053
  - Transaktionslog
    - a, Datenbankoption,321
    - ad, Datenbankoption ,322
    - ar, Datenbankoption,323
    - as, Datenbankoption,324
    - f, Wiederherstellungsoption,234
    - m, Datenbankoption,327
    - m, Serveroption,265
    - altes löschen,998
    - Betrieb ohne (Option -n),927
    - Dateinamen des Transaktionslogs spiegels setzen,998
    - Datenbankspiegelung,1484
    - Datenbankspiegelung, Einschränkungen,1475
    - Dienstprogramm zur Logkonvertierung (dbtran),948
    - einrichten,1067
    - empfohlener Speicherort,136
    - Festplattenspeicher zuweisen für,132,133
    - für Sicherungen verwalten,1078
    - Größe,138
    - Größe begrenzen,1093
    - Info,135,138
    - Initialisierungsdienstprogramm (dbinit),927
    - Konvertierungs-Dienstprogramme,948
    - Live-Sicherung,1032
    - mit dberase löschen,916
    - nach Checkpoint löschen,265
    - nach Datenträgerfehler wiederherstellen,1059
    - nach einem Checkpoint kürzen,327
    - nicht festgeschriebene Änderungen mit der Befehlszeile,1048
    - nicht festgeschriebene Änderungen mit Sybase Central,1048
    - Optionen,170
    - Position,213
    - Primärschlüssel,138
    - Serveroption -ds,325
    - Sicherung mit umbenannten Transaktionslog,1073,1074
    - Sicherungsdienstprogramm (dbbackup),886
    - Sicherungskopie umbenennen,1073,1074
    - Speicherort ändern,136,137
    - Speicherort für die Wiederherstellung mit Serveroption -ds angeben,325
    - SQL Remote delete\_old\_logs-Option,607
    - SQL Remote verwalten,607
    - SQL Remote, automatisch umbenennen,1070
    - Standort bei Wiederherstellung angeben,322
    - Standort bei Wiederherstellung von Datenbank beziehen,323
    - starten,234
    - Transaktionslog-Dienstprogramm (dblog),998
    - Transaktionslog-Spiegel erstellen,125,126
    - Transaktionslog-Spiegeldatei für eine vorhandene Datenbank starten,140
    - Transaktionslogs validieren,1075

- Unvollständige Transaktionen suchen,141
- von einem Scale-Out-Server verarbeiteter Umfang,1553
- während der Wiederherstellung anwenden,321
- Warnung bei Betrieb ohne (Option -n),927
- Wiederherstellen aus mehreren Transaktionslogs,1053
- Windows Mobile,440
- Zeitstempel,136
- Transaktionslog validieren
  - Info,1075
- Transaktionslog-Dienstprogramm (dblog)
  - Auditing,1418
  - Beendigungs-codes,1000
  - Syntax,998
- Transaktionslog-Spiegel
  - empfohlener Speicherort,139
  - erstellen,125,126
- Transaktionslog-Spiegeldatei
  - starten,140
  - Zweck,139
- Transaktionslogdateien
  - Transaktionslog-Dienstprogramm (dblog),998
- Transaktionslogs
  - Datenträgerfehler,1060
  - für Sicherungen umbenennen mit dem Dienstprogramm dbbackup,1072
  - für Sicherungen umbenennen mit SQL,1071
  - für Sicherungen umbenennen mit Sybase Central,1070
  - mit der Befehlszeile kürzen,1072
  - mit SQL kürzen,1071
  - mit Sybase Central kürzen,1070
- Transaktionslogspiegel
  - Initialisierung, Dienstprogramm (dbinit),927
  - Unterschiede zu Live-Sicherungen,1033
- Transaktionsmodi
  - verkettet/nicht verkettet,587
- Transaktionssicherheit
  - bei Datenbankspiegelung gewährleisten,1478
  - Datenbankspiegelung,1477
- TranslationDLL, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- TranslationName, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- TranslationOption, Verbindungsparameter
  - ODBC-Verbindungsparameter, Beschreibung,911
- translog, DBSpace
  - Info,127
- translogmirror, DBSpace
  - Info,127
- Transport Data Interface
  - Abhängigkeiten von Diensten einstellen,976
- Transportschichtssicherheit
  - Einführung,1444
  - einrichten,1446
  - Info,1444
  - unterstützte Plattformen,1445
  - von SSL unterstützte Version,1458
  - Wirkungsgrad,1444
- Transportschichtssicherheit über HTTPS
  - MobiLink,1463
- Transportschichtssicherheit über TCP/IP
  - MobiLink,1463
- Traps
  - an einen Computer senden,1227
  - dynamische Traps,1228
  - Info,1217
  - mit SQL Anywhere SNMP-Erweiterungsagent verwenden,1227
- Treiber
  - SQL Anywhere ODBC-Treiber,38
- Trennen
  - andere Benutzer mithilfe von Sybase Central,100
  - andere Benutzer von einer Datenbank (dbconsole),102
  - andere Benutzer von einer Datenbank (SQL),101
  - Datenbank stoppen,158,159
- Trigger
  - Datenbankdokumentation erstellen,814
  - deaktivieren,241
  - Privilegien,1305
  - und Replikation,612
- Triggerbedingungen
  - Definition,1091
- TriggerPages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- TriggerPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- TRUNCATE ANY TABLE-Systemprivileg
  - Beschreibung,1309
- truncate\_timestamp\_values, Option
  - in MobiLink-Synchronisation verwenden,698
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253

truncate\_timestamp\_values-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

truncate\_timestamp\_values-Option  
 Beschreibung,697

truncation\_length, Option  
 Einstellungen von Interactive SQL,851

truncation\_length-Option  
 Info,868

trusted\_certificates-Protokolloption  
 Beschreibung,421  
 MobiLink-Transportschichtssicherheit,1462

trusted\_certificates\_file-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

trusted\_certificates\_file-Option  
 Beschreibung,696  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253

tsql\_outer\_joins, Option  
 ASE-Kompatibilität,559  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 Transact-SQL-Kompatibilität,560

tsql\_outer\_joins-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

tsql\_outer\_joins-Option  
 Beschreibung,699

tsql\_variables, Option  
 ASE-Kompatibilität,559  
 SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 Transact-SQL-Kompatibilität,560

tsql\_variables-Eigenschaft  
 Verbindungseigenschaft, Beschreibung,711

tsql\_variables-Option  
 Beschreibung,699  
 Sybase Open Client,1571

Türkische Datenbanken  
 benutzerdefinierte Objekte referenzieren,532  
 Groß-/Kleinschreibung berücksichtigen,532  
 Groß-/Kleinschreibung nicht berücksichtigen,534  
 Systemobjekte referenzieren,532

Type 2 JDBC  
 Client-APIs und Zeichensatzkonvertierung,505

Typfilter  
 konfigurieren,797

## U

UAC, Benutzerkontensteuerung  
 SQL Anywhere unter Vista ausführen,202  
 SQL Anywhere unter Windows 2008 Server  
 ausführen,202  
 SQL Anywhere unter Windows 7 ausführen,202

Überblick, Registerkarte  
 SQL Anywhere,812

Überprüfen, Zertifikatsfelder  
 MobiLink-Transportschichtssicherheit,1461

Übersetzen einer Logdatei, Assistent  
 verwenden,1048

Überwachen  
 Datenbanken,1133  
 Datenbankoptionseinstellungen,569  
 MobiLink-Server,1115,1135  
 MobiLink-Serverfarmen,1137  
 Monitor,1115  
 Performance mit Histogramms,923  
 Relay Server-Farmen,1135  
 wer ist eingeloggt,981

Überwachungsliste  
 Datenbankoptionen,569

Überwachungsliste für Optionen  
 Info,569

UCA  
 bei Einbyte-Zeichensätzen verwenden,516  
 Info,516

UCA-Kollation  
 Hiragana,523  
 Katakana,523  
 schwedische Sprachumgebung,523  
 Standards der Schwedischen Akademie,523

UDP  
 Info,105

UID, Verbindungsparameter  
 Beschreibung,387

ulcond16, Dienstprogramm  
 erweiterte Privilegien eventuell unter Windows 7  
 erforderlich ,202  
 erweiterte Privilegien eventuell unter Windows  
 Server 2008 erforderlich ,202  
 erweiterte Privilegien eventuell unter Windows  
 Vista und später erforderlich,202

UltraLite  
 MobiLink-Transportschichtssicherheit,1464

UltraLite, Clients

- TLS,1464
- UltraLite-Clients konfigurieren, für
- Transportschichtssicherheit
  - Info,1464
- Umbenennen
  - Transaktionslog,1073,1074
- Umgebungsvariable
  - @data-Option,882
  - einrichten,467
  - ERRORLEVEL,939
  - LD\_LIBRARY\_PATH,469
  - LIBPATH,470
  - ODBC\_INI,471
  - ODBCHOME,470
  - ODBCINI,471
  - PATH,471
  - SACHARSET,472
  - SADIAGDIR,473
  - SALANG,473
  - SALOGDIR,474
  - SHLIB\_PATH,477
  - SQLANY16,477
  - SQLANY16,SAMP16,478
  - SQLCONNECT,479
  - SQLPATH,480
  - SQLREMOTE,480
  - SYBASE,480
  - TEMP,481
  - TEMP-Verzeichnis unter Windows Mobile setzen,491
  - TMP,481
  - Verbindung mit Datenbankdienstprogramm herstellen,30
- Umgebungsvariablen
  - als Source unter Unix nehmen,467
  - DYLD\_LIBRARY\_PATH,469
  - Info,467
  - SATMP,475
  - TMPDIR,481
  - Unix,467
  - unter Mac OS X setzen,468
  - unter Windows einrichten,467
- Umgekehrte Schrägstriche
  - nicht zulässig in Datenbankservernamen,267
- UNC, Verbindungsparameter
  - Beschreibung,386
- UncommitOp-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Unconditional, Verbindungsparameter
  - Beschreibung,386
- Undo-Log
  - Info,1079
- Unicode-Kollationsalgorithmus (UCA)
  - Info,516
- Unicode-Zeichensätze
  - Info,514
- UniqueClientAddresses, Eigenschaft
  - Verbindungseigenschaft, Beschreibung,745
- UniqueClientAddresses-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1234
- Unix
  - Berechtigungen für temporäre Dateien,476
  - Cachegröße,217
  - Dateien als Source nehmen,468
  - Dateisuche,486
  - Datenbankserver starten,153
  - Dienstprogramm dbconsole starten,877
  - Interactive SQL starten,815
  - IPv6-Unterstützung,106
  - Kollation wählen,531
  - LD\_LIBRARY\_PATH-Umgebungsvariable,469
  - Lizenzierungsprogramme,967
  - ODBC-Unterstützung,49
  - ODBC\_INI-Umgebungsvariable,471
  - ODBCHOME-Umgebungsvariable,470
  - ODBCINI-Umgebungsvariable,471
  - Performancestatistiken überwachen,953
  - Ping-Dienstprogramm mit einer Verbindungsbibliothek mit Threads verwenden,955
  - SATMP-Umgebungsvariable,481
  - Shared Memory-Verbindungen sichern,1407
  - Standardzeichensatz,512
  - Sybase Central starten,5
  - Systeminformationsdatei,49
  - temporäre Dateien,476
  - Thread-Verhalten,173
  - Umgebungsvariablen setzen,467
  - Verbindung mit der Beispieldatenbank herstellen,7
- UNLOAD TABLE-Anweisung
  - Sicherheit,1408
- UNLOAD-Anweisung
  - Sicherheit,1408
- unprocessed.sql
  - Info,1016
- UnschReq, Eigenschaft

---

Servedeigenschaft, Beschreibung,745  
 UnschReq-Statistik  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1234  
 Unterbrochene Verbindungen  
   Trap des SQL Anywhere SNMP-  
   Erweiterungsagenten,1227  
 Untere Codepage  
   Info,499  
 Unternehmens-Stammzertifikate  
   erstellen,901  
 Unternehmensstammzertifikate  
   Transportschichtsicherheit,1451  
   Zertifikatketten,1449  
 Unternehmensstammzertifikate erstellen  
   Transportschichtsicherheit,1451  
 Unterschiede  
   Kopieknoten und Spiegelknoten,1539  
 Unterschiede zwischen Live-Sicherungen und  
 Transaktionslog-Spiegeldateien  
   Info,1033  
 Unterstützte Funktionen  
   Windows Mobile,423  
 Unterstützte Plattformen  
   Kerberos,64  
   SQL Anywhere SNMP-Erweiterungsagent,1216  
 Unterverzeichnisse  
   Windows Mobile,430  
 updatable\_statement\_isolation, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 updatable\_statement\_isolation-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 updatable\_statement\_isolation-Option  
   Beschreibung,700  
 UPDATE ANY TABLE-Systemprivileg  
   Beschreibung,1309  
 UPDATE, Anweisung  
   in Interactive SQL generieren,829  
   kürzen von Zeichenfolgen,685  
 UPDATE-Privileg  
   Info,1305  
 update\_statistics, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 update\_statistics-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 update\_statistics-Option  
   Beschreibung,701  
 update\_timeout-Parameter  
   LDAP,110  
 Upgrade  
   authentifizierte Datenbanken,200  
   Datenbanken,1017  
 UPGRADE ROLE-Systemprivileg  
   Beschreibung,1309  
 upgrade\_database\_capability, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 upgrade\_database\_capability-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 USAGE ON SEQUENCE  
   GRANT-Anweisung, Syntax (nicht mehr  
   empfohlen),1393  
   REVOKE-Anweisung, Syntax (nicht mehr  
   empfohlen),1397  
 USAGE-Privileg  
   Info,1305  
 USE ANY SEQUENCE-Systemprivileg  
   Beschreibung,1309  
 user\_estimates, Option  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253  
 user\_estimates-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 user\_estimates-Option  
   Beschreibung,702  
 UserAppInfo, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRate01  
   Info,789  
 UserDefinedCounterRate01-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servedeigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRate02  
   Info,789  
 UserDefinedCounterRate02-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servedeigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRate03  
   Info,789  
 UserDefinedCounterRate03-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servedeigenschaft, Beschreibung,745

Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRate04  
   Info,789  
 UserDefinedCounterRate04-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
 UserDefinedCounterRate05  
   Info,789  
 UserDefinedCounterRate05-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRaw01  
   Info,789  
 UserDefinedCounterRaw01-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRaw02  
   Info,789  
 UserDefinedCounterRaw02-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRaw03  
   Info,789  
 UserDefinedCounterRaw03-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRaw04  
   Info,789  
 UserDefinedCounterRaw04-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Servereigenschaft, Beschreibung,745  
   Verbindungseigenschaft, Beschreibung,711  
 UserDefinedCounterRaw05  
   Info,789  
 UserDefinedCounterRaw05-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767  
   Verbindungseigenschaft, Beschreibung,711  
 UserID, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 Userid, Verbindungsparameter  
   Beschreibung,387  
 UTCTimestampCatalog-Eigenschaft  
   Datenbankeigenschaft, Beschreibung,767

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1248  
 UTF-8  
   bei Datenbanken verwenden,927  
 util\_db.ini  
   Info,146  
 UtilCmdsPermitted, Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 utility\_db  
   Name für Dienstprogrammdatenbank  
   reserviert,145  
   Privilegien zur Ausführung von Anweisungen  
   steuern,255  
   Verbindung,147  
 uuid\_has\_hyphens-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 uuid\_has\_hyphens-Option  
   Beschreibung,703  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1253

## V

VALIDATE ANY OBJECT-Systemprivileg  
   Beschreibung,1309  
 VALIDATE-Berechtigung (nicht mehr empfohlen)  
   konvertiert in SYS\_AUTH\_VALIDATE\_ROLE-  
   Kompatibilitätsrolle,1275  
 Validieren  
   Datenbanken,1080  
   dbvalid, Dienstprogramm,1020  
   Sicherungen,1045  
   Tabellen aus Sybase Central,1086  
   Transaktionslog,1075  
 Validierung  
   Datenbanken,1080  
   Datenbanken aus Sybase Central,1081  
   Spalten-Integritätsregeln,125  
 Validierungs-Dienstprogramm (dbvalid)  
   Beendigungscodes,1024  
   Syntax,1020  
 VCS, Agenten  
   SADatabase,1532  
   SAServer,1528  
 Verarbeitung von Ereignissen  
   Info,1087  
 Verarbeitungsfortschritt, Meldungen  
   für Sicherungen aktivieren,886

- 
- Verarbeitungsfortschritts-Meldungen
    - Einstellung,657
  - Verbinden
    - Beispieldatenbank (Dienstprogramm dbisql),7
    - Beispieldatenbank (Sybase Central),5
    - Datenbank ohne Verbindung starten,157
    - Datenbankserver automatisch starten,83
    - Datenquellen mit Verbindungszeichenfolgen verwenden,22
    - Datenquellen verwenden,19
    - Datenquellen verwenden (Dienstprogramm dbisql),20
    - dblocate und LDAP,963
    - Dienstprogrammdatenbank,147
    - Fehlerbehandlung,79
    - Firewalls,107
    - integrierte Logins,1409
    - lokale Datenbank starten (Dienstprogramm dbisql),18
    - lokale Datenbanken,17
    - lokale Datenbanken starten,16
    - lokale Datenbankserver starten,16
    - lokalen Server starten (Dienstprogramm dbisql),18
    - mit Datenbanken,5
    - mit einer lokalen Datenbank (Dienstprogramm dbisql),18
    - mit LDAP,109
    - Netzwerkdatenbanken,23
    - Netzwerkdatenbanken (Dienstprogramm dbisql),24
    - RAS,109
    - Speicherort eines Datenbankservers ermitteln,83
    - TCP/IP,25
    - Verbinden-Fenster, Überblick (Dienstprogramm dbconsole),15
    - Verbinden-Fenster, Überblick (Interactive SQL),15
    - Verbinden-Fenster, Überblick (Sybase Central),14
    - Verbindungsprofile verwenden,12
    - vom SQL Anywhere-Konsolendienstprogramm,15
    - von Interactive SQL,15
    - Windows Mobile,434
    - Windows Mobile und ODBC-Datenquellen,48
    - Windows Mobile-Datenbanken und Desktop-Anwendungen,37
    - Windows Mobile-Geräte,434
    - Zeichensätze,503
  - Verbinden-Fenster
    - Öffnen (Dienstprogramm dbconsole),15
    - öffnen (Interactive SQL),15
    - öffnen (Sybase Central),14
    - Überblick (Dienstprogramm dbconsole),15
    - Überblick (Interactive SQL),15
    - Überblick (Sybase Central),14
  - Verbindung herstellen
    - BroadcastListener-Protokolloption (BLISTENER),391
    - ClientPort-Protokolloption (CPORT),395
    - Datenbankverbindungsszenarien,30
    - Host-Protokolloption (IP),399
    - IPv6-Adressen,106
    - LDAP, Protokolloption,406
    - ServerPort-Protokolloption (PORT),416
    - von Sybase Central,14
  - Verbindung mit Datenbanken
    - Info,5
  - Verbindung trennen
    - Datenbanken (dbconsole),102
    - Datenbanken (SQL),101
  - Verbindungen
    - alphabetische Liste der Eigenschaften,711
    - Auditing,1417
    - Authentifizierung,593
    - begrenzen,244
    - Beispiele für das Starten von Datenbankservern,153
    - benennen,349
    - Datenbanken automatisch starten,28
    - Datenbankfunktionen aktivieren,669
    - Datenbankspiegelung,1472
    - dedicated\_task-Option,603
    - Definition,5
    - Eigenschaften,711
    - eingebettete Datenbanken,28
    - erforderliche Verbindungsparameter,32
    - Favoriten bearbeiten,825
    - Fehlerbehandlung,79
    - Fehlerbehandlung mit dblocate,960
    - Fehlerbehandlung mit dbping,955
    - Funktionen sichern,1406
    - für die SQL Anywhere OEM Edition authentifizieren,198
    - Info,5
    - IPv6-Adressen,106
    - Kopieknotten,1545
    - Login-Richtlinien,535
    - maximale Anzahl mit login\_procedure-Option einstellen,626

- maximaler Speicher für temporäre Dateien,689
- mehrere in Interactive SQL,844
- mit Serveroption -tdsl trennen,290
- mit Serveroption -ti trennen,291
- Performance,94
- Performance von Embedded SQL testen,96
- Pooling,77
- Probleme,79
- Programmierschnittstellen,50
- Protokolloptionen,388
- Scale-Out mit Schreibschutz,1545
- Speicher für temporäre Dateien limitieren,689
- Speicherort eines Datenbankservers ermitteln,83
- Standardparameter,35
- temporär,78
- temporären Speicher limitieren,636
- Überblick,5
- Verfügbarkeit,292
- Verlust in Scale-Out-Systemen,1553
- von Dienstprogrammen,30
- Windows Mobile,434
- zu Favoriten hinzufügen,824
- Verbindungs-IDs
  - Info,30
- Verbindungsbeispiele
  - Überblick,30
- Verbindungseigenschaften
  - alphabetische Liste,711
  - Berichte,955
  - Groß-/Kleinschreibung,710
- Verbindungsfehler
  - Fehlerbehandlung,79
- Verbindungsparameter
  - alphabetische Liste,337
  - Beschreibung,911
  - Boolesche Werte,338
  - Datenquelle, Dienstprogramm (dbdsn),905
  - Datenquellen,38
  - Delphi,911
  - DescribeCursor,911
  - Dienstprogramm dbisqlc,915
  - Dienstprogramm zum Entladen (dbunload),1001
  - Dienstprogramm zum Upgrade (dbupgrad),1018
  - Dienstprogramm zur Logkonvertierung (dbtran),948
  - Einstellungen,31
  - Escape,911
  - GetTypeInfoChar,911
  - Groß-/Kleinschreibung berücksichtigen,337
  - Groß-/Kleinschreibung nicht berücksichtigen,338
  - Info,337
  - Informationsdienstprogramm (dbinfo),926
  - InitString,911
  - Interactive SQL (dbisql), Dienstprogramm,939
  - IsolationLevel,911
  - KeysInSQLStatistics,911
  - LazyAutocommit,911
  - leere Werte,37
  - ODBC-Datenquellen,911
  - Ping-Dienstprogramm (dbping),955
  - PrefetchOnOpen,911
  - PreventNotCapable,911
  - Priorität,36
  - Regeln,36
  - Sicherungsdienstprogramm (dbbackup),886
  - Speicherort,81
  - SQL Anywhere,337
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),982
  - SQL Anywhere-Skriptausführung, Dienstprogramm (dbrunsql),959
  - Standardparameter verwenden,35
  - Stopp-Dienstprogramm (dbstop),984
  - SuppressWarnings,911
  - Syntax,36
  - Szenarien,32
  - TranslationDLL,911
  - TranslationName,911
  - TranslationOption,911
  - Treiber,911
  - Validierungs-Dienstprogramm (dbvalid),1021
  - Verbindungen einrichten,50
  - Verbindungszeichenfolgen,31
  - Vorrang,37
- Verbindungsparameter Elevate
  - Beschreibung,358
- Verbindungspooling
  - ADO.NET Sample verwenden,461
  - ConnectionPool-Verbindungsparameter (CPOOL),350
  - mit Scale-Out mit Schreibschutz verwenden,78
  - SQL Anywhere,77
  - unter Windows Mobile nicht unterstützt,423
  - Verbindungen in SQL Anywhere,77
- Verbindungsprofile
  - bearbeiten,12

---

- erstellen,10
- exportieren,13
- importieren,13
- Info,10
- verbinden,12
- Verbindungsumleitung
  - Administrationstools,25
- Verbindungszeichenfolgen
  - alphabetische Liste der Verbindungsparameter,337
  - Darstellung,31
  - Einführung,31
  - Info,31
  - leere Verbindungsparameter,37
  - Leerstellen in,36
  - Priorität bei doppelten Parametern,36
  - Verbindungsparameter verwenden,31
  - Zeichensätze,503
- Verbundene Benutzer
  - verwalten,99
- Vereinigungen
  - im Abfrage-Editor nicht unterstützt,837
- Vererbung
  - Rollen und Privilegien,1348
- Verfügbarkeit
  - Datenbankserver,180
  - hohe,1032
  - Verbindungen,292
- Vergleiche
  - Sicherungsarten,1029
  - TIMESTAMP,605
- Vergleichen
  - Datenbankschemata,810
- VERIFY, Protokolloption
  - Beschreibung,422
- verify\_all\_columns, Option
  - Replikationsoption,704
- verify\_all\_columns-Option
  - SQL Remote-Replikationsoption,563
- verify\_password\_function, Option
  - Kennwörter authentifizieren,1411
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1253
- verify\_password\_function-Eigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- verify\_password\_function-Option
  - Beschreibung,704
- verify\_threshold, Option
  - Beschreibung,707
- verify\_threshold-Option
  - SQL Remote-Replikationsoption,563
- VerifyServerName, Protokolloption
  - Beschreibung,422
- Veritas Cluster Server
  - mit SQL Anywhere verwenden,1527
- Veritas Cluster Server, Agenten
  - Info,1527
- Verkettet, Transaktionsmodus
  - chained-Option,587
- Verschlüsseln
  - Datenbanken,1426
  - Datenbanken für den technischen Kundendienst,1109
  - Spalten,1435
- Verschlüsselung
  - ec, Serveroption,230
  - ek, Serveroption,326
  - ep, Serveroption,233
  - es, Serveroption,234
  - AES-Algorithmus,1425
  - certificate\_company-Protokolloption,392
  - certificate\_name-Protokolloption,393
  - certificate\_unit-Protokolloption,394
  - Client/Server-Kommunikation unter Windows Mobile,1443
  - Datenbank entschlüsseln,1431
  - Datenbankdateien,1424
  - Datenbankdateien, nach ihrer Erstellung,1430
  - Datenbanken mit dbinit erstellen,927
  - Dienstprogramm zum Verschleiern von Dateien (dbfhide),922
  - einfache,1424
  - FIPS,1445
  - Info,1424
  - INI-Dateien,922
  - Kommunikationen,1444
  - MobiLink,1458
  - öffentlicher Schlüssel,1444
  - Performance verschlüsselter Datenbanken,1433
  - Punkt zu Punkt,1459
  - RAW-Verschlüsselung,1436
  - Spalten,1435
  - SQL Anywhere-Datenbanken unter Windows Mobile,1443
  - starke,1425
  - Tabellen,1437,1440
  - Tabellenverschlüsselung aktivieren (dbinit),1440

- Tabellenverschlüsselung aktivieren (SQL),1438
- TDS-Protokolloption,419
- trusted\_certificates-Protokolloption,421
- Verbindungsparameter Encryption (ENC),359
- Vergleich der Anweisungen CREATE ENCRYPTED FILE und CREATE ENCRYPTED DATABASE,1427
- Windows Mobile,441
- Verschlüsselung, stark
  - Verbindungsparameter Encryption (ENC),359
- Verschlüsselung:
  - EncryptedPassword (ENP)-Verbindungsparameter,358
- Verschlüsselungsalgorithmen
  - AES,1425
  - Rijndael,1425
- Verschlüsselungseigenschaft
  - Verbindungseigenschaft, Beschreibung,711
- Verschlüsselungsschlüssel
  - angeben,927
  - starten verschlüsselte Datenbanken,353
  - verwenden,1424
- Version
  - Datenbankserver,303
  - ermitteln,1024
- Versionenkonflikt
  - Dateipositionen,483
- Versionsdiagnose (dbversion)
  - Syntax,1024
- VersionStorePages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- VersionStorePages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Versionsverwaltung
  - Check-In von Dateien von Interactive SQL,871
  - Check-Out von Dateien von Interactive SQL,871
  - in Interactive SQL konfigurieren,869
  - Integration mit Interactive SQL,868
  - mit Projekten,871
  - von Interactive SQL aus verfügbare Aktionen,873
- Verteilte Transaktionen
  - Aufnahme-Timeout,294
  - Wiederherstellung mit der Option -tmf,293
- Verwaltungsinformations-Datenbanken
  - Info,1217
- Verzeichnisstruktur
  - SQL Anywhere,482
- Verzeichniszugriffsserver
  - unter Windows Mobile nicht unterstützt,423
- viewcert, Dienstprogramm
  - Syntax,903
  - Verwendung,1447
- ViewPages, Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- ViewPages-Statistik
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1244
- Vista
  - Benutzerkontensteuerung,202
  - Datenbankserver mit Dienstprogramm dbconsole überwachen,203
  - dbelevat16.exe,203
  - Dienste interagieren nicht mit dem Desktop,203
  - Hinweise zum Deployment,203
  - signierte ausführbare Dateien,203
  - SQL Anywhere ausführen,202
  - SQL Anywhere, Agent für Vorgänge mit erweiterten Berechtigungen,202
  - Verbindungsparameter DisableMultiRowFetch ,358
- Vollständige Sicherungen
  - Info,1030
- Vorbereitete Anweisungen
  - max\_statement\_count-Option,635
  - vom Server unterstütztes Maximum,791
- Vordefinierte DBSpaces
  - Info,127
- Voreinstellungen
  - SQL Anywhere-Konsolendienstprogramm (dbconsole),878
- Vorrang
  - Verbindungsparameter,37
- Vorwärts-Log
  - Info,135
- VSS
  - Datenbankserver,303
  - SQL Anywhere Volume-Schattenkopie-Dienst,1042
- VSS-Dienstverfasser
  - dbvss16.exe,1042
- W**
  - wait\_for\_commit, Option

---

SQL Anywhere SNMP-Erweiterungsagent,  
 OID,1253  
 wait\_for\_commit-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 wait\_for\_commit-Option  
   Beschreibung,708  
 WaitStartTime-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 WaitType-Eigenschaft  
   Verbindungseigenschaft, Beschreibung,711  
 Warnungen  
   Datenbankserver-Performance,1110  
 Wartungsplan erstellen, Assistent  
   verwenden,1064  
 Wartungspläne  
   Berichte anzeigen,1065  
   erstellen,1064  
   Info,1064  
   löschen,1066  
 WebClientLogFile, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 WebClientLogFile-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 WebClientLogging, Eigenschaft  
   Servereigenschaft, Beschreibung,745  
 WebClientLogging-Eigenschaft  
   SQL Anywhere SNMP-Erweiterungsagent,  
   OID,1237  
 Webdienst-Clientlogdatei  
   Namen einstellen,315  
 Webdienst-Clients  
   certificate\_company-Protokolloption,393  
   certificate\_name-Protokolloption,394  
   certificate\_unit-Protokolloption,395  
   Protokollierung,315  
   trusted\_certificates-Protokolloption,421  
 Webdienste  
   Datenbankserver-Konfiguration,310  
   mit Transportschichtssicherheit starten,1458  
   standardmäßig ausgeführte Login-Prozeduren,626  
   webservice\_namespace\_host-Option,708  
   webservice\_sessionid\_name-Option,709  
 Webserver  
   Größe der Logdatei,410  
   in Spiegelungssystemen verwenden,1476  
   Logdatei-Nachrichtenformat,408  
   mit Transportschichtssicherheit starten,1458  
   webservice\_namespace\_host, Option  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
   webservice\_namespace\_host-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
   webservice\_namespace\_host-Option  
     Beschreibung,708  
   webservice\_sessionid\_name-Eigenschaft  
     Verbindungseigenschaft, Beschreibung,711  
   webservice\_sessionid\_name-Option  
     Beschreibung,709  
     SQL Anywhere SNMP-Erweiterungsagent,  
     OID,1253  
 Werte  
   in Interactive SQL bearbeiten,831  
 Widgets  
   hinzufügen,1128  
   Monitor,1127  
   verwalten,1128  
 Wiederherstellen  
   Datenbankdatei,1057  
   Datenbanken mit mehreren Transaktionslogs  
   (Serveroption -a),1055  
   Kompatibilitätsrollen (SQL),1284  
   Kompatibilitätsrollen (Sybase Central),1283  
   Monitor-Datenbanken,1192  
   nicht gespiegelte Transaktionslogs,1060  
   SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle  
   (SQL),1284  
   SYS\_AUTH\_DBA\_ROLE-Kompatibilitätsrolle  
   (Sybase Central),1283  
   SYS\_AUTH\_SA\_ROLE-Kompatibilitätsrolle  
   (SQL),1284  
   SYS\_AUTH\_SA\_ROLE-Kompatibilitätsrolle  
   (Sybase Central),1283  
   SYS\_AUTH\_SSO\_ROLE-Kompatibilitätsrolle  
   (SQL),1284  
   SYS\_AUTH\_SSO\_ROLE-Kompatibilitätsrolle  
   (Sybase Central),1283  
   Transaktionslogspiegel,1059  
 Wiederherstellen, Log  
   Info,135  
 Wiederherstellung  
   automatisch,1027  
   Datenbanken,1047  
   Datenbanken mit mehreren Transaktionslogs  
   (Serveroption -ad),1054  
   Datenträgerfehler,1056

- Dringlichkeit,1077
- Einschränkungen,1036
- Info,1027
- interne Vorgänge,1075
- Maximalzeit,249
- nach einem Primärserver-Ausfall,1499
- nicht festgeschriebene Änderungen mit der Befehlszeile,1048
- nicht festgeschriebene Änderungen mit Sybase Central,1048
- Option für verteilte Transaktionen,293
- Optionen,170
- schnell,1032
- Serveroptionen,234
- Sicherungspläne implementieren,1062
- Speicherort von Transaktionslog angeben,325
- Strategien für Windows Mobile,449
- Systemausfall,1067
- Transaktionslog-Spiegel,138
- Windows
  - Cachegröße,217
  - Codepages,500
  - Dateisuche,484
  - Datenbankserver starten,153
  - Dienste,181
  - Dienstprogramm dbconsole starten,877
  - Ereignisprotokoll,167
  - Installations-Registrierungseinstellungen,490
  - integrierte Logins,52
  - Interactive SQL starten,815
  - IPv6-Unterstützung,106
  - Kollation wählen,530
  - Minimale Cachegröße,224
  - SNMP installieren,1221
  - Standardzeichensatz,512
  - Sybase Central starten,5
  - TCP/IP,106
  - Thread-Verhalten,173
  - Zeichensätze,500
- Windows 2003
  - SNMP installieren,1221
- Windows 7
  - Benutzerkontensteuerung,202
  - Datenbankserver mit Dienstprogramm dbconsole überwachen,203
  - dbelevat16.exe,203
  - Dienste interagieren nicht mit dem Desktop,203
  - Hinweise zum Deployment,203
  - signierte ausführbare Dateien,203
  - SQL Anywhere ausführen,202
  - SQL Anywhere, Agent für Vorgänge mit erweiterten Berechtigungen,202
- Windows CE
  - IPv6-Adressen nicht unterstützt,106
- Windows MIT, Kerberos-Client
  - Keytab-Dateien,64
- Windows Mobile
  - Gerätesicherheit,1442
  - @data-Option nicht unterstützt,426
  - ADO.NET Sample verwenden,461
  - Anforderungen einer SQL Anywhere-Installation,430
  - Auditing,1442
  - Beispiele,432
  - beschränkte Unterstützung der Kollationsanpassung,439
  - das .NET Compact Framework verwenden,431
  - Dateistandorte,430
  - Dateisuche,485
  - Datenbanken auf Ihr Gerät kopieren,446
  - Datenbanken erstellen,441
  - Datenbanken konfigurieren,439
  - Datenbanken löschen (Geräte-Benutzeroberfläche),450
  - Datenbanken löschen (Windows-Explorer),450
  - Datenbanken mit dem Dienstprogramm dbinit erstellen,444
  - Datenbanken mit Interactive SQL erstellen,445
  - Datenbanken neu aufbauen,447
  - Datenbanken sichern,449
  - Datenbankserver,451
  - Datenbankserver starten,434
  - Datenbankserveroptionen,1442
  - Datenbankspiegelung nicht unterstützt,423
  - Datenbankverschlüsselung,1443
  - dbxtract nicht unterstützt,429
  - eingeschränkte jConnect-Funktionalität,423
  - eingeschränkte ODBC-Funktionalität,423
  - Einschränkungen bei
    - Anwendungsprofilerstellung,423
    - Einschränkungen unter Windows Mobile 5.0 für Smartphones,431
  - ESQL Sample,463
  - externe gespeicherte Prozeduren nicht unterstützt,423
  - externe Umgebungen nicht unterstützt,423

- 
- Extraktionsdienstprogramm nicht unterstützt,429
  - Ferndatenzugriff nicht unterstützt,423
  - ICU,430
  - Installation,430
  - Interactive SQL, praktische Einführung,457
  - IP-Adresse ermitteln,438
  - jConnect,440
  - Kerberos nicht unterstützt,423
  - Kommunikationsverschlüsselung,1443
  - LDAP nicht unterstützt,423
  - nicht unterstützte Administrationstools,423
  - nicht unterstützte Datenbankserveroptionen,426
  - nicht unterstützte SQL Anywhere-Funktionen,423
  - nicht unterstützte SQL Remote-Funktionen,429
  - nicht unterstützte SQL-Anweisungen,425
  - nicht unterstützte Sybase Central-Assistenten,428
  - ODBC Sample,464
  - ODBC-Datenquellen erstellen,435
  - ODBC-Datenquellen verwenden,48
  - parallele Sicherungen nicht unterstützt,423
  - Personal Server nicht unterstützt,423
  - praktische Einführung,461
  - Proxy-Ports,437
  - Prüfsummen standardmäßig aktiviert,1086
  - Server-StartoptionenFenster,452
  - Sicherheit,1442
  - Speicherkarten,430
  - SQL Anywhere installieren,432
  - SQL Anywhere JDBC-Treiber nicht unterstützt,423
  - SQL Anywhere verwenden,423
  - Sybase Central, praktische Einführung,452
  - Sybase Open Client nicht unterstützt,423
  - TEMP-Datei setzen,491
  - Transaktionslog,440
  - unterstützte Funktionen,423
  - Unterverzeichnisse,430
  - Verbindungspooling nicht unterstützt,423
  - Verschlüsselung ,441
  - Verzeichniszugriffsserver nicht unterstützt,423
  - vom Desktop verbinden,37
  - von einem PC verbinden,434
  - Windows Mobile 5.0
    - Einschränkungen für Smartphones,431
  - Windows Mobile Proxy-Ports, Fenster verwenden,437
  - Windows Mobile-Beispielanwendung
    - starten,432
  - Windows Mobile-Gerätecenter
    - erforderliche Version,430
  - Windows Server 2008
    - Benutzerkontensteuerung,202
    - Datenbankserver mit Dienstprogramm dbconsole überwachen,203
    - dbelevate16.exe,203
    - Dienste interagieren nicht mit dem Desktop,203
    - Hinweise zum Deployment,203
    - signierte ausführbare Dateien,203
    - SQL Anywhere, Agent für Vorgänge mit erweiterten Berechtigungen,202
  - Windows Systemmonitor
    - gemeinsam genutzten Speicher erstellen,264
  - Windows Vista
    - SNMP installieren,1221
    - Verbindungsparameter
      - DisableMultiRowFetch ,358
  - Windows XP
    - integrierte Logins,52
    - SNMP installieren,1221
  - Windows-Benutzergruppen
    - integrierte Logins,58
  - Windows-Dienste
    - Abhängigkeiten,191
    - aktualisieren,189
    - Datenbankserver,180
    - Erläuterung,181
    - erstellen,182,183
    - Gruppen,190
    - konfigurieren,185
    - Konto-Optionen,187
    - löschen,184,185
    - mehrere,191
    - nutzbare Programme,181
    - Optionen,186
    - Parameter,185
    - Programmdatei,187
    - Registrierungseinstellungen,488
    - starten,189
    - Startoptionen,186
    - Startreihenfolge,191
    - stoppen,189
    - Symbol auf dem Desktop,187
    - Windows-Dienste-Manager ,190
  - Windows-Dienste, Manager
    - Info,190
  - Windows-Systemmonitor

- Steuerung der Anzahl von überwachten Datenbanken,264
- Steuerung der Anzahl von überwachten Verbindungen,264
- Winsock
  - TCP/IP mit Windows verwenden,106
- Worker
  - Threads in SQL Anywhere,172
  - Unix-Verhalten,173
- Worker-Threads
  - Linux-Verhalten,173
  - Stackgröße,250
  - Windows-Verhalten,173
- WRITE CLIENT FILE-Systemprivileg
  - Beschreibung,1309
- WRITE FILE-Systemprivileg
  - Beschreibung,1309
- WriteChecksum-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
  - SQL Anywhere SNMP-Erweiterungsagent, OID,1248
- WRITECLIENTFILE-Berechtigung (nicht mehr empfohlen)
  - konvertiert in
  - SYS\_AUTH\_WRITECLIENTFILE\_ROLE-Kompatibilitätsrolle,1275
- WRITEFILE-Berechtigung (nicht mehr empfohlen)
  - konvertiert in SYS\_AUTH\_WRITEFILE\_ROLE-Kompatibilitätsrolle,1275

## X

- X Window-Server
  - Benutzeroberfläche unter Linux anzeigen,302
- X.509-Zertifikate
  - anzeigen,903
  - erstellen,894
- XML
  - in Interactive SQL anzeigen,843
- XML, Dateiformat
  - Interactive SQL, Ausgabe,866
- xp\_cmdshell, Systemprozedur
  - Sicherheitsfunktionen,1406
- xp\_sendmail, Systemprozedur
  - Sicherheitsfunktionen,1406
- xp\_srvmon\_count\_unsubmitted\_crash\_reports, Prozedur
  - Monitor,1193

- xp\_startmail, Systemprozedur
  - Sicherheitsfunktionen,1406
- xp\_startsmtp, Systemprozedur
  - Sicherheitsfunktionen,1406
- xp\_stopmail, Systemprozedur
  - Sicherheitsfunktionen,1406
- xp\_stopsmtp, Systemprozedur
  - Sicherheitsfunktionen,1406
- XPathCompiles-Eigenschaft
  - Datenbankeigenschaft, Beschreibung,767
- xs, Option
  - Kommunikationen sichern,1458

## Z

- Zahlenzeichen
  - in Konfigurationsdateien verwenden,882
- Zeichen
  - mit Kollationen sortieren,514
- Zeichen V und W
  - in der schwedischen UCA-Kollation festlegen,523
- Zeichenersetzung
  - on\_charset\_conversion\_failure-Option,645
- Zeichenfolgen
  - maximale Größe,791
  - und Hostvariable,575
- Zeichenkodierung
  - Info,497
- Zeichensätze
  - alternative Zeichensätze,501
  - angeben,472
  - Anwendung,512
  - ASE-Labels,501
  - Daten entladen,343
  - den CHAR-Zeichensatz bestimmen,512
  - den NCHAR-Zeichensatz bestimmen,512
  - ermitteln, ob ein Zeichensatz unterstützt wird,501
  - für Mac OS X empfohlen,530
  - für Unix-Plattformen empfohlene,531
  - für Windows-Plattformen empfohlene,530
  - IANA-Labels,501
  - IANA-Labels, Liste,530
  - ICU-Labels,501
  - in SQL Anywhere,500
  - Info,497
  - Initialisierung, Dienstprogramm (dbinit),927
  - JAVA-Labels,501
  - kodieren,493

---

- Konvertierung,502
- Labels,530
- Liste der gelieferten CHAR-Zeichensätze,501
- Mehrbyte,500
- Mehrbyte-Kollationen,514
- MIME-Labels,501
- mit fester Weite,500
- mit variabler Weite,500
- Server,512
- Single-Byte,499
- türkische Datenbanken,532
- Unicode,514
- Unix-Standard,512
- Verbindungsparameter,343
- Windows,500
- Windows-Standard,512
- Zeichensätze mit fester Weite
  - Info,500
- Zeichensätze mit variabler Weite
  - Info,500
- Zeichensatzkonvertierung
  - Client-APIs,505
  - Client/Server,503
  - ICU,502
  - Info,502
  - SQL-Anweisungen,503
- Zeilen
  - in Interactive SQL bearbeiten,831
  - in Interactive SQL einfügen,832
  - in Interactive SQL kopieren,834
  - löschen mit Interactive SQL,833
- Zeilenanzahl
  - aktivieren,667
- Zeilennummern
  - SQL-Anweisungen, Fensterausschnitt,817
- Zeitplan erstellen, Assistent
  - Vorgehensweise,1090
- Zeitpläne
  - für Ereignisse definieren,1090
- Zeitstempel
  - Datenbankdateien,136
  - Transaktionslog,136
- Zeitzone
  - anpassen,691
  - SQL Remote, TIMESTAMP WITH TIME ZONE-  
Anzeigeformat,677
  - TIMESTAMP WITH TIME ZONE-  
Anzeigeformat,694
- Zelle kopieren
  - in Interactive SQL,834
- Zertifikat-Dienstprogramme
  - Transportschichtsicherheit,1466
- Zertifikatanforderungen
  - anzeigen,903
- Zertifikate
  - certificate\_company-Protokolloption,392
  - certificate\_name-Protokolloption,393
  - certificate\_unit-Protokolloption,394
  - digitale Zertifikate für  
Transportschichtsicherheit,1447
  - Erstellen von RSA-Zertifikaten,894
  - Info,1447
  - trusted\_certificates-Protokolloption,421
  - X.509 anzeigen,903
- Zertifikatketten
  - Transportschichtsicherheit,1449
- Zertifikatsfelder überprüfen
  - SQL Anywhere-Transportschichtsicherheit,1456
- Zertifikatsperrliste
  - anzeigen,903
- Zertifizierungsstellen
  - Transportschichtsicherheit,1453
- Ziffern
  - maximale Anzahl,653
- Zugriffspläne
  - Optimierer-Verwendung steuern,648
- Zustand
  - Wartungspläne,1064
- Zustandsüberwachung und Statistik
  - Monitor,1115

