Insight Security (SecurityAdmin-Tool)

OnCommand Insight

NetApp
October 24, 2024

Inhalt

Sicherheitstool

OnCommand Insight bietet Funktionen, mit denen Insight Umgebungen sicherer betrieben werden können. Diese Funktionen umfassen Verschlüsselung, Passwort-Hashing und die Möglichkeit, interne Benutzerpasswörter und Schlüsselpaare zu ändern, die Kennwörter verschlüsseln und entschlüsseln. Sie können diese Funktionen auf allen Servern in der Insight-Umgebung mit dem **SecurityAdmin Tool** verwalten.

Was ist das SecurityAdmin-Tool?

Das Sicherheits-Admin-Tool unterstützt Änderungen am Inhalt der Vaults sowie koordinierte Änderungen an der OnCommand Insight-Installation.

Die primären Verwendungszwecke für das SecurityAdmin-Tool sind **Backup** und **Restore** der Sicherheitskonfiguration (d.h. Tresor) und Passwörter. Sie können beispielsweise den Tresor auf einer lokalen Erfassungseinheit sichern und auf einer Remote-Erfassungseinheit wiederherstellen, um die Passwortkoordination in Ihrer gesamten Umgebung sicherzustellen. Oder wenn Sie mehrere OnCommand Insight-Server in Ihrer Umgebung haben, möchten Sie möglicherweise ein Backup des Server-Tresors erstellen und diese auf anderen Servern wiederherstellen, um die Passwörter unverändert zu halten. Dies sind nur zwei Beispiele für die Art und Weise, wie SecurityAdmin verwendet werden kann, um die Kohäsion in Ihren Umgebungen zu gewährleisten.

Es wird dringend empfohlen, den Vault * zu sichern, wenn Sie eine OnCommand Insight-Datenbank sichern. Andernfalls kann der Zugriff verloren gehen.

Das Tool bietet sowohl **Interactive** als auch **command line** Modi.

Viele Operationen des SecurityAdmin Tools ändern den Inhalt des Tresors und nehmen auch Änderungen an der Installation vor, um sicherzustellen, dass der Tresor und die Installation synchron bleiben.

Beispiel:

- Wenn Sie ein Insight-Benutzerpasswort ändern, wird der Benutzereintrag in der Tabelle SANscreen.Users mit dem neuen Hash aktualisiert.
- Wenn Sie das Passwort eines MySQL-Benutzers ändern, wird die entsprechende SQL-Anweisung ausgeführt, um das Kennwort des Benutzers in der MySQL-Instanz zu aktualisieren.

In einigen Situationen werden mehrere Änderungen an der Installation vorgenommen:

- Wenn Sie den dwh MySQL-Benutzer ändern, werden neben der Aktualisierung des Passworts in der MySQL-Datenbank auch mehrere Registrierungseinträge für ODBC aktualisiert.

In den folgenden Abschnitten wird der Begriff "koordinierte Änderungen" verwendet, um diese Änderungen zu beschreiben.

Ausführungsmodi

- Normaler/Standardbetrieb – der SANscreen-Serverdienst muss ausgeführt werden

  Für den Standardausführungsmodus erfordert das SecurityAdmin-Tool, dass der **SANscreen-Serverdienst** ausgeführt wird. Der Server wird für die Authentifizierung verwendet, und viele koordinierte

Änderungen an der Installation werden durch Aufrufen des Servers vorgenommen.

- Direkter Betrieb – der SANscreen-Serverdienst wird möglicherweise ausgeführt oder angehalten.

  Bei Ausführung auf einem OCI-Server oder einer DWH-Installation kann das Tool auch im „direkten“ Modus ausgeführt werden. In diesem Modus werden Authentifizierung und koordinierte Änderungen über die Datenbank durchgeführt. Der Serverdienst wird nicht verwendet.

  Der Betrieb ist mit dem normalen Modus identisch, mit den folgenden Ausnahmen:

- Die Authentifizierung wird nur für Benutzer unterstützt, die keine Domäne haben. (Benutzer, deren Passwort und Rollen sich in der Datenbank befinden, nicht LDAP).
- Der Vorgang „Schlüssel ersetzen“ wird nicht unterstützt.
- Der Schritt zur erneuten Verschlüsselung der Vault-Wiederherstellung wird übersprungen.
- Wiederherstellungsmodus das Tool kann auch dann ausgeführt werden, wenn der Zugriff auf den Server und die Datenbank nicht möglich ist (z. B. weil das Root-Passwort im Tresor falsch ist).

  Bei Ausführung in diesem Modus ist keine Authentifizierung möglich und daher kann kein Vorgang mit koordinierter Änderung der Installation durchgeführt werden.

  Der Wiederherstellungsmodus kann verwendet werden, um:

- Bestimmen Sie, welche Vault-Einträge falsch sind (mit dem Verifizierungs-Vorgang).
- Ersetzen Sie das falsche Root-Passwort durch den richtigen Wert. (Das Passwort wird dadurch nicht geändert. Der Benutzer muss das aktuelle Passwort eingeben.)

> ⓘ Wenn das Root-Passwort im Tresor falsch ist und das Passwort nicht bekannt ist und es keine Sicherung des Tresors mit dem korrekten Root-Passwort gibt, kann die Installation nicht mit dem SecurityAdmin-Tool wiederhergestellt werden. Die einzige Möglichkeit, die Installation wiederherzustellen, ist das Zurücksetzen des Passworts der MySQL-Instanz nach dem unter dokumentierten Verfahren https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Verwenden Sie nach dem Zurücksetzen den Vorgang Correct-stored-password, um das neue Passwort in den Tresor einzugeben.

Befehle

Unbeschränkte Befehle

Unbeschränkte Befehle nehmen alle koordinierten Änderungen an der Installation vor (außer Vertrauensstellungen). Unbeschränkte Befehle können ohne Benutzerauthentifizierung ausgeführt werden.

Befehl	Beschreibung

Backup-Vault	Erstellen Sie eine ZIP-Datei mit dem Tresor. Der relative Pfad zu den Vault-Dateien stimmt mit dem Pfad der Vaults relativ zum Installationsroot überein. • wildfly/Standalone/Configuration/Vault/* • acq/conf/Vault/* Beachten Sie, dass es dringend empfohlen wird, den Tresor zu sichern, wenn Sie eine OnCommand Insight-Datenbank sichern.
Nach Standardschlüsseln suchen	Überprüfen Sie, ob die Schlüssel des Tresors mit denen des Standard-Tresors übereinstimmen, der in Instanzen vor 7.3.16 verwendet wird.
Korrekt gespeichertes Passwort	Ersetzen Sie ein (falsches) Kennwort, das im Tresor gespeichert ist, durch das korrekte Kennwort, das dem Benutzer bekannt ist. Dies kann verwendet werden, wenn der Tresor und die Installation nicht konsistent sind. **Beachten Sie, dass es das eigentliche Passwort in der Installation nicht ändert.**
	Change-Trust-Store-password Ändern Sie das für einen Trust-Store verwendete Passwort und speichern Sie das neue Passwort im Tresor. Das aktuelle Kennwort des Vertrauenshauses muss „bekannt“ sein.
Verify-keystore	Prüfen Sie, ob die Werte im Tresor korrekt sind: • Stimmt der Hash des Passworts für OCI-Benutzer mit dem Wert in der Datenbank überein • Für MySQL-Benutzer kann eine Datenbankverbindung hergestellt werden • Für Schlüsselspeicher kann der Schlüsselspeicher geladen und seine Schlüssel (falls vorhanden) gelesen werden
Listentasten	Einträge im Tresor auflisten (ohne Anzeige des gespeicherten Wertes)

Eingeschränkte Befehle

Für alle nicht verborgenen Befehle, die koordinierte Änderungen an der Installation vornehmen, ist eine Authentifizierung erforderlich:

Befehl	Beschreibung

Restore-Vault-Backup	Ersetzt den aktuellen Tresor durch den Tresor, der in der angegebenen Vault-Sicherungsdatei enthalten ist. Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Kennwörtern im wiederhergestellten Tresor entspricht: • Aktualisieren Sie die Benutzerpasswörter für die OCI-Kommunikation • Aktualisieren Sie die MySQL-Benutzerpasswörter, einschließlich Root • Wenn das Schlüsselspeicher-Passwort „bekannt“ ist, aktualisieren Sie den Schlüsselspeicher mit den Kennwörtern aus dem wiederhergestellten Tresor. Bei der Ausführung im normalen Modus werden auch alle verschlüsselten Werte von der Instanz gelesen, mit dem Verschlüsselungsdienst des aktuellen Tresors entschlüsselt, mit dem Verschlüsselungsdienst des wiederhergestellten Tresors erneut verschlüsselt und der neu verschlüsselte Wert gespeichert.
Sync-with-Vault	Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Benutzerpasswörtern im wiederhergestellten Tresor entspricht: • Aktualisiert die Benutzerpasswörter für die OCI-Kommunikation • Aktualisiert die MySQL-Benutzerpasswörter, einschließlich Root
Passwort ändern	Ändert das Passwort im Tresor und führt die koordinierten Aktionen durch.
Schlüssel ersetzen	Erstellen Sie einen neuen leeren Tresor (der andere Schlüssel als der vorhandene Tresor hat). Kopieren Sie dann die Einträge aus dem aktuellen Tresor in den neuen Tresor. Liest dann jeden verschlüsselten Wert aus der Instanz, entschlüsselt ihn mit dem Verschlüsselungsdienst des aktuellen Tresors, verschlüsselt ihn mit dem Verschlüsselungsdienst des wiederhergestellten Tresors und speichert den neu verschlüsselten Wert.

Koordinierte Maßnahmen

Server Vault

_Intern	Passwort-Hash für Benutzer in Datenbank aktualisieren
Akquisition	Passwort-Hash für Benutzer in Datenbank aktualisieren Wenn der Akquisitionssault vorhanden ist, aktualisieren Sie auch den Eintrag im Akquisitions-Vault
dwh_intern	Passwort-Hash für Benutzer in Datenbank aktualisieren

cognos_admin	Passwort-Hash für Benutzer in Datenbank aktualisieren Wenn DWH und Windows, aktualisieren Sie SANscreen/cognos/Analytics/Configuration/SANscreenAP.properties, um die Eigenschaft cognos.admin auf das Passwort zu setzen.
Stamm	Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren
Inventar	Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren
dwh	Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren Wenn DWH und Windows, aktualisieren Sie die Windows-Registrierung, um die folgenden ODBC-bezogenen Einträge auf das neue Passwort zu setzen: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud_Cost\PWD
Whuser	Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren
Hosts	Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren

Keystore_password	Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.keystore
Trustore_password	Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.trustore
Key_password	Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/sso.jks
cognos_Archive	Keine

Akquisitions-Vault

Akquisition	Keine
Trustore_password	Schreiben Sie den Keystore mit dem neuen Passwort (falls vorhanden) neu - acq/conf/cert/Client.keystore

Ausführen des Security Admin Tools - Befehlszeile

Die Syntax zum Ausführen des SA-Tools im Befehlszeilenmodus lautet:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Hinweise:

- Die Option „-i“ ist möglicherweise nicht in der Befehlszeile vorhanden (da hier der interaktive Modus ausgewählt wird).
- Für die Optionen „-s“ und „-au“:
  - „-s“ ist auf einer rau nicht zulässig
  - „-au“ ist auf DWH nicht zulässig

    - Wenn keines vorhanden ist, dann
        - Der Server-Vault wird auf Server, DWH und Dual ausgewählt
        - Der Aufnahmevault wird auf der rau ausgewählt
- Die Optionen -lu und -lp werden für die Benutzerauthentifizierung verwendet.
    - Wenn <user> angegeben ist und <password> nicht angegeben ist, wird der Benutzer zur Eingabe des Passworts aufgefordert.
    - Wenn <user> nicht bereitgestellt wird und eine Authentifizierung erforderlich ist, wird der Benutzer aufgefordert, sowohl <user> als auch <password> einzugeben.

Befehle:

Befehl	Zu Verwenden
Korrekt gespeichertes Passwort	`securityadmin [-s`
-au] [-db] -pt <key> [<value>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value 	Backup-Vault
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip
Backup-Vault	`securityadmin [-s`

-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ```	Listentasten
`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
Prüfschlüssel	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	Verify-keystore (Server)
`` securityadmin [-s] [-db] -v where -v specified command ```	Upgrade

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``
Schlüssel ersetzen	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	Restore-Vault-Backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``
Change-Password (Server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]` `where` `-up specified command ("update-password")` `-un <user> entry ("user") name to update` `-p <password> new password. If <password not supplied, user will be prompted.` `-sh for mySQL user, use strong hash`

Change-Passwort für Akquisitionsbenutzer (Akquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]` `where` `-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.`
Change-password für Truststore-_password (Akquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]` `where` `-utp specified command ("update-truststore-password") -p <password> new password. If <password not supplied, user will be prompted.`
Synchronisieren mit Tresor (Server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

Ausführen des Security Admin Tools – Interaktiver Modus

Interaktiv – Hauptmenü

Um das SA-Tool im interaktiven Modus auszuführen, geben Sie den folgenden Befehl ein:

```
 securityadmin -i
Bei einer Server- oder Doppelinstallation fordert SecurityAdmin den
Benutzer auf, entweder den Server oder die lokale Erfassungseinheit
auszuwählen.
```

Knoten der Server- und Erfassungseinheit erkannt! Wählen Sie den Knoten aus, dessen Sicherheit neu konfiguriert werden muss:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

Auf DWH wird automatisch „Server“ ausgewählt. Auf einer externen AU wird automatisch „Acquisition Unit“ ausgewählt.

Interactive - Server: Wiederherstellung des Root-Passworts

Im Server-Modus überprüft das SecurityAdmin-Tool zunächst, ob das gespeicherte Root-Passwort korrekt ist. Wenn dies nicht der Fall ist, zeigt das Tool den Bildschirm zur Wiederherstellung des Root-Passworts an.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

Interactive - Server: Korrektes Passwort

Mit der Aktion „Passwort korrigieren“ wird das im Tresor gespeicherte Passwort so geändert, dass es mit dem für die Installation erforderlichen Kennwort übereinstimmt. Dieser Befehl ist nützlich in Situationen, in denen eine Änderung an der Installation durch etwas anderes als das securityadmin-Tool vorgenommen wurde. Beispiele:

- Das Passwort für einen SQL-Benutzer wurde durch direkten Zugriff auf MySQL geändert.
- Ein Keystore wird ersetzt oder das Passwort eines Keystore wird mit keytool geändert.
- Eine OCI Datenbank wurde wiederhergestellt, und diese Datenbank enthält unterschiedliche Passwörter für die internen Benutzer

„Passwort korrigieren“ fordert den Benutzer zuerst auf, das Kennwort auszuwählen, um den richtigen Wert zu speichern.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Nach Auswahl des zu korrigenden Eintrags wird der Benutzer gefragt, wie er den Wert angeben möchte.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers
zurück.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers zurück.

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers angezeigt.

Interactive - Server: Überprüfen Sie Den Inhalt Des Tresores

Überprüfen Sie, ob Vault Contents Schlüssel enthält, die mit dem StandardVault übereinstimmen, der mit früheren OCI-Versionen verteilt ist, und überprüft, ob jeder Wert im Vault mit der Installation übereinstimmt.

Die möglichen Ergebnisse für jeden Schlüssel sind:

OK	Der Vault-Wert ist korrekt

Nicht Aktiviert	Der Wert kann nicht mit der Installation verglichen werden
SCHLECHT	Der Wert stimmt nicht mit der Installation überein
Fehlt	Ein erwarteter Eintrag fehlt.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interaktiv – Server: Sicherung

Beim Backup wird das Verzeichnis angezeigt, in dem die ZIP-Sicherungsdatei gespeichert werden soll. Das Verzeichnis muss bereits vorhanden sein, und der Dateiname lautet ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactive - Server: Anmeldung

Die Anmeldeaktion wird verwendet, um einen Benutzer zu authentifizieren und Zugriff auf Vorgänge zu erhalten, die die Installation ändern. Der Benutzer muss über Admin-Privileges verfügen. Bei der Ausführung mit dem Server kann jeder Admin-Benutzer verwendet werden; bei der Ausführung im direkten Modus muss der Benutzer ein lokaler Benutzer und kein LDAP-Benutzer sein.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

Oder

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Wenn das Passwort korrekt ist und der Benutzer ein Admin-Benutzer ist, wird das Menü eingeschränkt angezeigt.

Wenn das Passwort falsch ist, wird Folgendes angezeigt:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Wenn der Benutzer kein Administrator ist, wird Folgendes angezeigt:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive - Server: Eingeschränktes Menü

Sobald sich der Benutzer angemeldet hat, zeigt das Tool das eingeschränkte Menü an.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive - Server: Passwort Ändern

Mit der Aktion „Passwort ändern“ können Sie ein Installationspasswort in einen neuen Wert ändern.

„Kennwort ändern“ fordert den Benutzer zuerst auf, das zu ändernde Kennwort auszuwählen.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Wenn der Benutzer ein MySQL-Benutzer ist, wird der Benutzer nach der Auswahl des zu korrigenden Eintrags gefragt, ob er das Passwort stark hashing

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Anschließend wird der Benutzer zur Eingabe des neuen Passworts aufgefordert.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Wenn ein nicht leeres Passwort eingegeben wird, wird der Benutzer aufgefordert, das Passwort zu bestätigen.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Wenn die Änderung nicht erfolgreich war, wird der Fehler oder die Ausnahme angezeigt.

Interaktiv – Server: Wiederherstellen

Interactive - Server: Ändern Sie Die Verschlüsselungsschlüssel

Die Aktion Verschlüsselungsschlüssel ändern ersetzt den Verschlüsselungsschlüssel, der zum Verschlüsseln der Vault-Einträge verwendet wird, und ersetzt den Verschlüsselungsschlüssel, der für den Verschlüsselungsdienst des Tresors verwendet wird. Da der Schlüssel des Verschlüsselungsdienstes geändert wird, werden verschlüsselte Werte in der Datenbank erneut verschlüsselt; sie werden gelesen, mit dem aktuellen Schlüssel entschlüsselt, mit dem neuen Schlüssel verschlüsselt und in der Datenbank gespeichert.

Diese Aktion wird im direkten Modus nicht unterstützt, da der Server für einige Datenbankinhalte die erneute Verschlüsselung bereitstellt.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactive - Server: Installation Beheben

Mit der Aktion Installation beheben wird die Installation aktualisiert. Alle Installationspasswörter, die über das securityadmin-Tool außer root geändert werden können, werden auf die Passwörter im Tresor gesetzt.

- Die Passwörter interner OCI-Benutzer werden aktualisiert.
- Die Passwörter von MySQL-Benutzern, mit Ausnahme von root, werden aktualisiert.
- Die Passwörter der Schlüsselspeicher werden aktualisiert.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

Die Aktion wird bei der ersten nicht erfolgreichen Aktualisierung angehalten und zeigt den Fehler oder die Ausnahme an.

Sicherheitsmanagement auf dem Insight-Server

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Insight-Server verwalten. Die Sicherheitsverwaltung umfasst das Ändern von Kennwörtern, das Generieren neuer Schlüssel, das Speichern und Wiederherstellen von von von von Ihnen erstellten Sicherheitskonfigurationen oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

Verwaltung der Sicherheit auf der lokalen Erfassungseinheit

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen für den lokalen Akquisitionsbenutzer (LAU) verwalten. Die Sicherheitsverwaltung umfasst das Verwalten von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen von Sicherheitskonfigurationen, die Sie erstellen oder auf die Standardeinstellungen wiederherstellen.

Bevor Sie beginnen

Dieser muss unbedingt vorhanden sein `admin` Berechtigungen zum Ausführen von Sicherheitskonfigurationsaufgaben.

Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

Verwaltung der Sicherheit auf einer rau

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf raus verwalten. Möglicherweise müssen Sie eine Vault-Konfiguration sichern oder wiederherstellen, Verschlüsselungsschlüssel ändern oder Kennwörter für die Erfassungseinheiten aktualisieren.

Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Ein Szenario für die Aktualisierung der Sicherheitskonfiguration für die LAU/rau ist die Aktualisierung des Benutzerpassworts für die Erfassung, wenn das Kennwort für diesen Benutzer auf dem Server geändert wurde. Die LAU und alle raus verwenden das gleiche Passwort wie das des Benutzer „Acquisition“ des Servers, um mit dem Server zu kommunizieren.

Der Benutzer „Acquisition“ ist nur auf dem Insight-Server vorhanden. Die rau oder LAU melden sich als dieser Benutzer an, wenn sie eine Verbindung zum Server herstellen.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

Verwaltung der Sicherheit im Data Warehouse

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Data Warehouse-Server verwalten. Die Sicherheitsverwaltung umfasst die Aktualisierung interner Passwörter für interne Benutzer auf dem DWH-Server, das Erstellen von Backups der Sicherheitskonfiguration oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

Ändern der internen OnCommand Insight-Benutzerpasswörter

In Sicherheitsrichtlinien müssen Sie möglicherweise die Passwörter in Ihrer OnCommand

Insight-Umgebung ändern. Einige der Passwörter auf einem Server sind auf einem anderen Server in der Umgebung vorhanden, sodass Sie das Passwort auf beiden Servern ändern müssen. Wenn Sie beispielsweise das Benutzerpasswort „`inventar`“ auf dem Insight Server ändern, müssen Sie das Benutzerpasswort „`inventar`“ auf dem für diesen Insight Server konfigurierten Data Warehouse Server Connector zuordnen.

Bevor Sie beginnen

Sie sollten die Abhängigkeiten der Benutzerkonten verstehen, bevor Sie Passwörter ändern. Wenn Passwörter nicht auf allen erforderlichen Servern aktualisiert werden, kommt es zu Kommunikationsfehlern zwischen den Insight-Komponenten.

Über diese Aufgabe

In der folgenden Tabelle sind die internen Benutzerpasswörter für den Insight Server aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Passwort übereinstimmen müssen.

Passwörter Für Insight Server	Erforderliche Änderungen
_Intern	
Akquisition	LAU, RAU
dwh_intern	Data Warehouse
Hosts	
Inventar	Data Warehouse
Stamm	

In der folgenden Tabelle sind die internen Benutzerkennwörter für das Data Warehouse und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Kennwort übereinstimmen müssen.

Data Warehouse-Passwörter	Erforderliche Änderungen
cognos_admin	
dwh	
dwh_Internal (geändert mit der Server Connector-Konfigurationsoberfläche)	Insight Server
Whuser	
Hosts	

Inventarisierung (geändert mit der Server Connector-Konfigurationsoberfläche)	Insight Server
Stamm	

Ändern von Kennwörtern in der DWH Server Connection Configuration UI

In der folgenden Tabelle ist das Benutzerpasswort für DIE LAU aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern, die mit dem neuen Passwort übereinstimmen müssen.

LAU-Passwörter	Erforderliche Änderungen
Akquisition	Insight Server, rau

Ändern der Passwörter „inventar“ und „dwh_internal“ mithilfe der Benutzeroberfläche für die Serververbindungskonfiguration

Wenn Sie die Passwörter „`inventar`“ oder „`dwh_internal`“ so ändern müssen, dass sie mit denen auf dem Insight-Server übereinstimmen, verwenden Sie die Data Warehouse-Benutzeroberfläche.

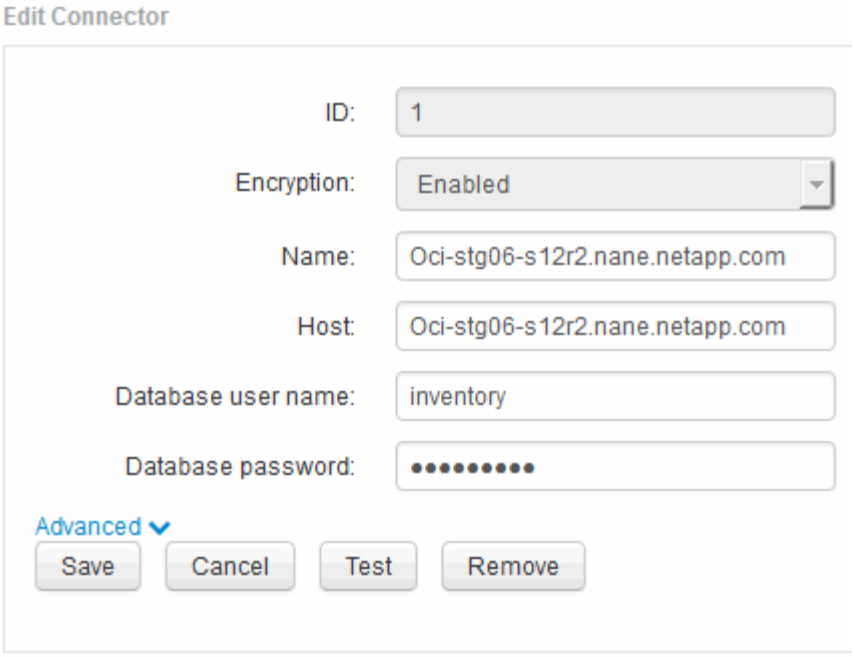
Bevor Sie beginnen

Sie müssen als Administrator angemeldet sein, um diese Aufgabe ausführen zu können.

Schritte

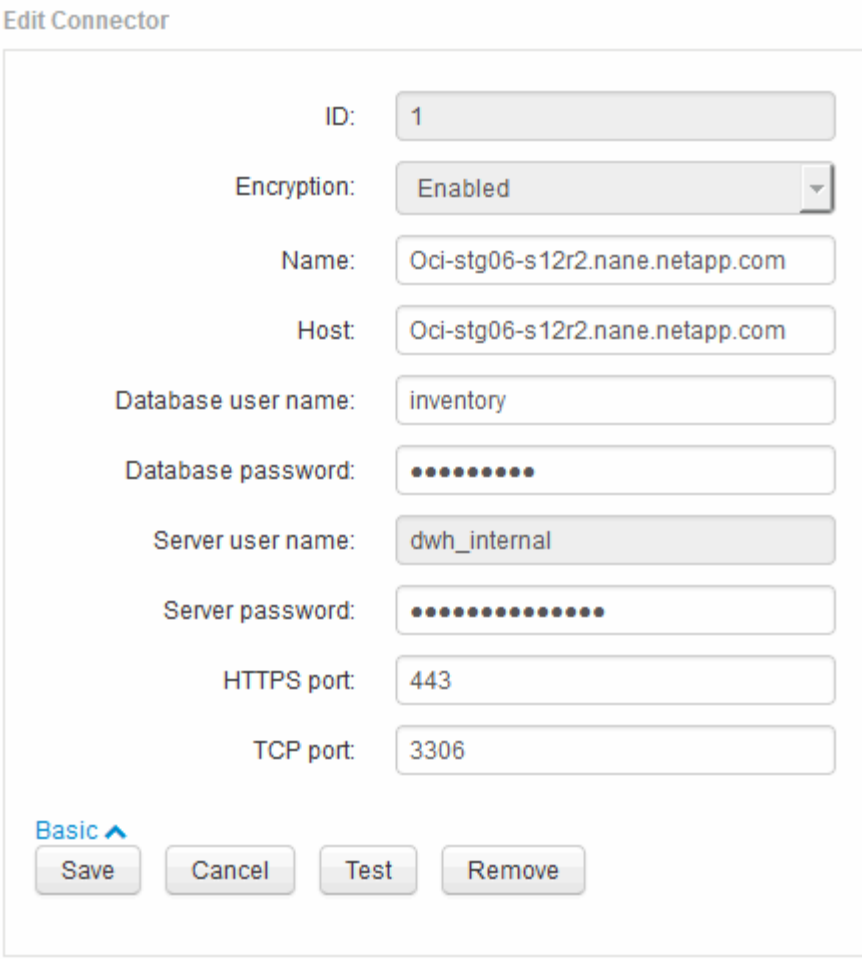
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   Der Bildschirm **Connector bearbeiten** wird angezeigt.



3. Geben Sie ein neues „`Inventory`“-Passwort für das Feld **Datenbankkennwort** ein.
4. Klicken Sie Auf **Speichern**
5. Um das Passwort „`dwh_internal`“ zu ändern, klicken Sie auf **Erweitert.**

   Der Bildschirm Edit Connector Advanced wird angezeigt.



6. Geben Sie das neue Passwort in das Feld **Server-Passwort** ein:
7. Klicken Sie auf Speichern.

Ändern des dwh-Kennworts mit dem ODBC-Verwaltungstool

Wenn Sie das Passwort für den dwh-Benutzer auf dem Insight-Server ändern, muss das Passwort auch auf dem Data Warehouse-Server geändert werden. Sie verwenden das ODBC-Datenquellenadministrator-Tool, um das Kennwort im Data Warehouse zu ändern.

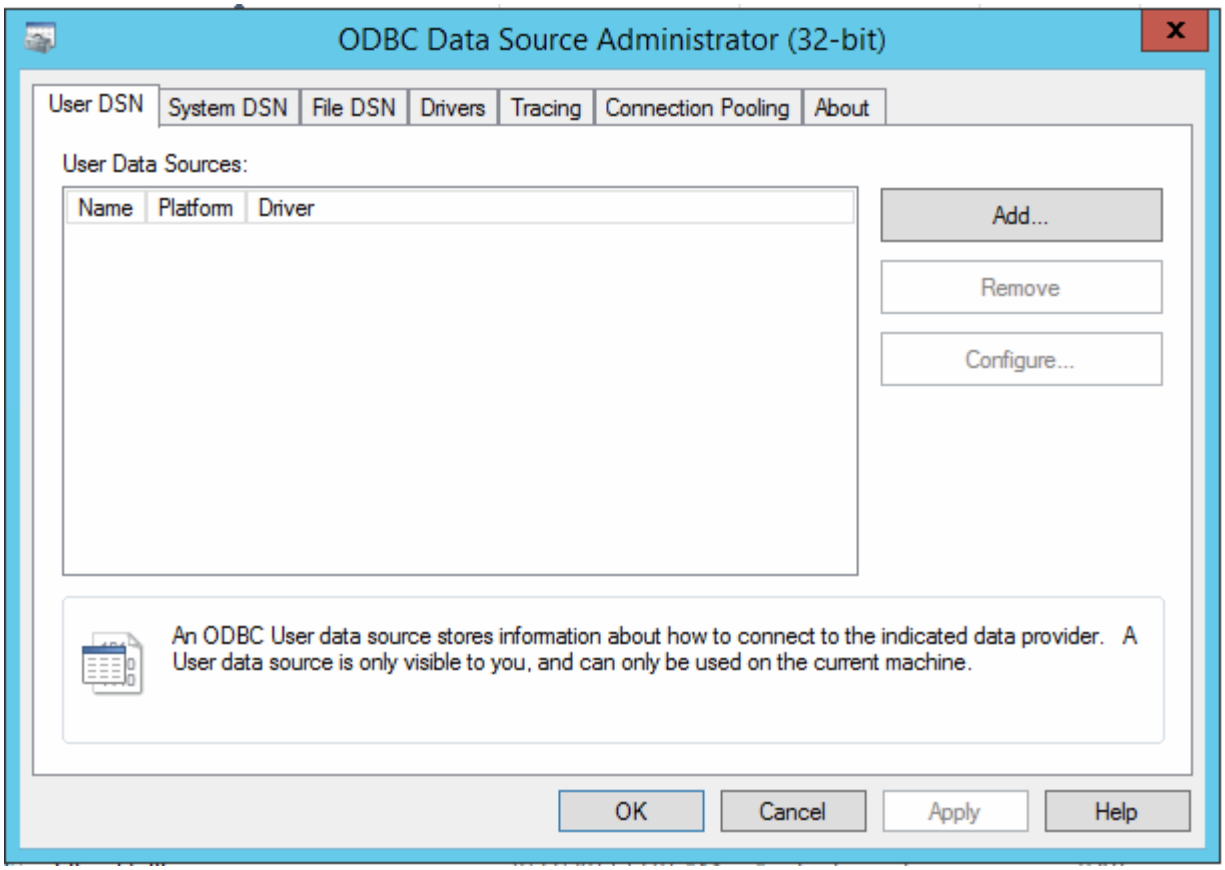
Bevor Sie beginnen

Sie müssen eine Remote-Anmeldung beim Data Warehouse-Server mit einem Konto mit Administratorrechten durchführen.

Schritte

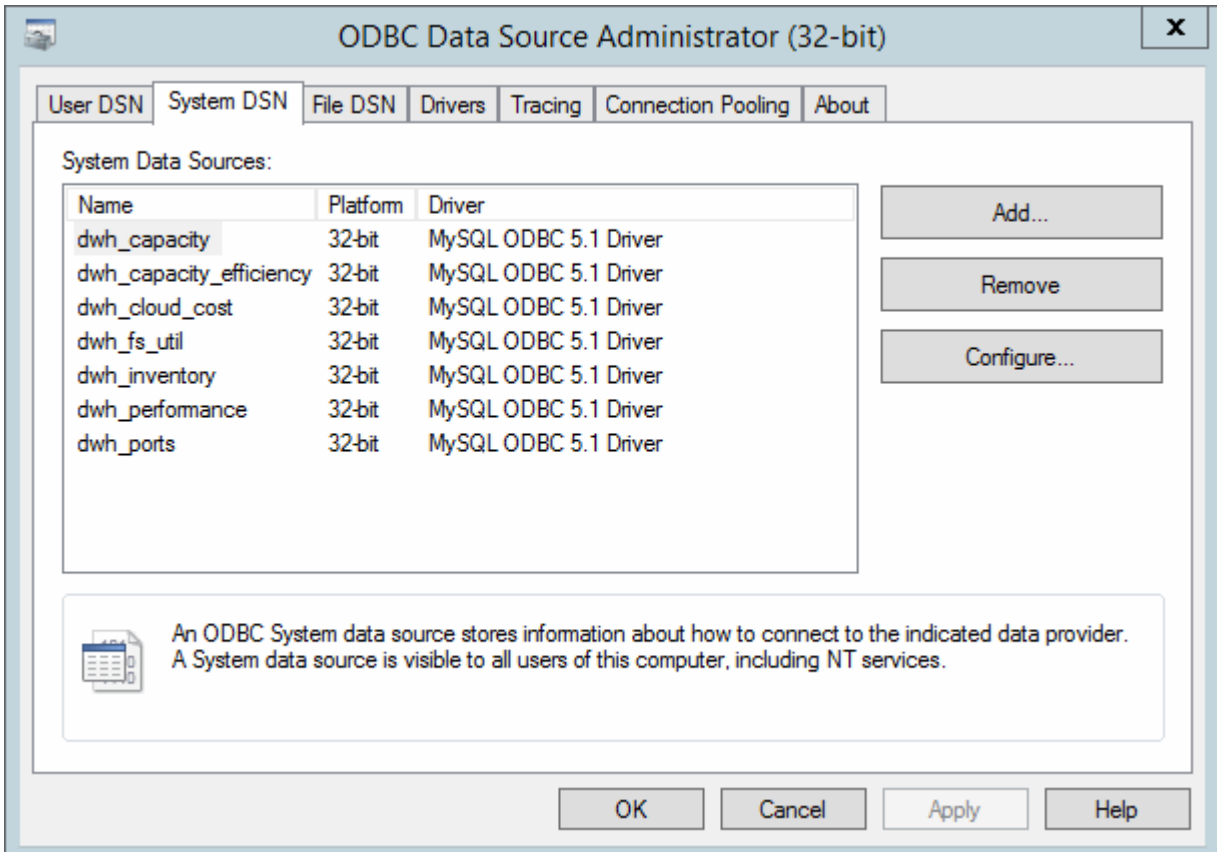
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

   Das System zeigt den ODBC-Bildschirm „Data Source Administrator“ an.



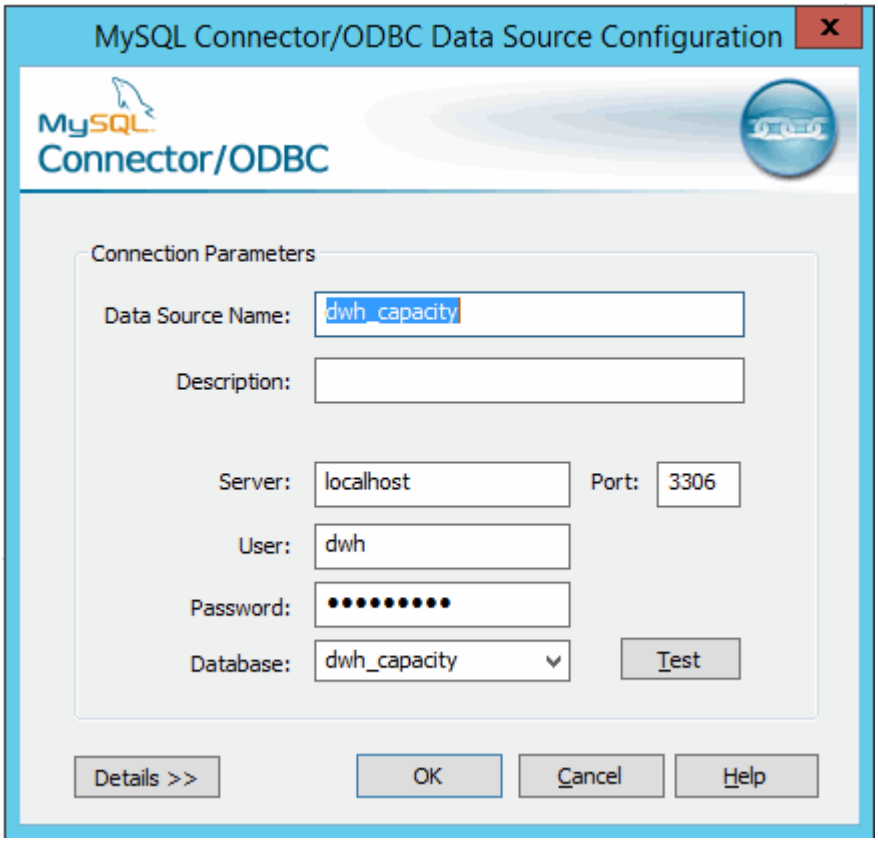
3. Klicken Sie auf **System DSN**

   Die Systemdatenquellen werden angezeigt.



4. Wählen Sie eine OnCommand Insight-Datenquelle aus der Liste aus.
5. Klicken Sie Auf **Konfigurieren**

   Der Bildschirm „Konfiguration der Datenquelle“ wird angezeigt.



6. Geben Sie das neue Passwort in das Feld **Passwort** ein.

Copyright-Informationen

Markeninformationen