Insight Sicherheit

OnCommand Insight

NetApp
April 01, 2024

Inhalt

Insight Sicherheit

In Version 7.3.1 von OnCommand Insight wurden Sicherheitsfunktionen eingeführt, mit denen Insight Umgebungen noch sicherer arbeiten können. Zu den Funktionen gehören Verbesserungen der Verschlüsselung, das Hashing von Passwörtern und die Möglichkeit, interne Benutzer-Passwörter und Schlüsselpaare zu ändern, die Passwörter verschlüsseln und entschlüsseln. Sie können diese Funktionen auf allen Servern in der Insight-Umgebung verwalten.

Die Standardinstallation von Insight beinhaltet eine Sicherheitskonfiguration, bei der alle Standorte in Ihrer Umgebung dieselben Schlüssel und dieselben Standardpasswörter verwenden. Zum Schutz sensibler Daten empfiehlt NetApp, die Standardschlüssel und das Erfassungs-Benutzerpasswort nach einer Installation oder einem Upgrade zu ändern.

Verschlüsselte Passwörter der Datenquelle werden in der Insight Server-Datenbank gespeichert. Der Server verfügt über einen öffentlichen Schlüssel und verschlüsselt Passwörter, wenn ein Benutzer sie auf einer WebUI-Datenquellkonfigurationsseite eingibt. Der Server verfügt nicht über die privaten Schlüssel, die zum Entschlüsseln der in der Server-Datenbank gespeicherten Datenquellkennwörter erforderlich sind. Nur Acquisition Units (LAU, rau) verfügen über den privaten Schlüssel der Datenquelle, der zum Entschlüsseln von Passwörtern für Datenquellen erforderlich ist.

Server werden neu keying

Die Verwendung von Standardschlüsseln führt zu einer Sicherheitsanfälligkeit in Ihrer Umgebung. Standardmäßig werden Datenquellkennwörter in der Insight-Datenbank verschlüsselt gespeichert. Sie werden verschlüsselt und verwenden einen Schlüssel, der für alle Insight-Installationen verwendet wird. In einer Standardkonfiguration enthält eine an NetApp gesendete Insight Datenbank Passwörter, die theoretisch von NetApp entschlüsselt werden können.

Ändern des Benutzerpassworts für die Erfassung

Durch die Verwendung des standardmäßigen Benutzerpassworts für die Akquisition wird die Sicherheitslücke in Ihrer Umgebung behoben. Alle Akquisitionseinheiten verwenden den Benutzer „`Acquisition`“, um mit dem Server zu kommunizieren. Raus mit Standardpasswörtern kann theoretisch eine Verbindung zu jedem Insight-Server herstellen, wobei Standardpasswörter verwendet werden.

Überlegungen zu Upgrades und Installationen

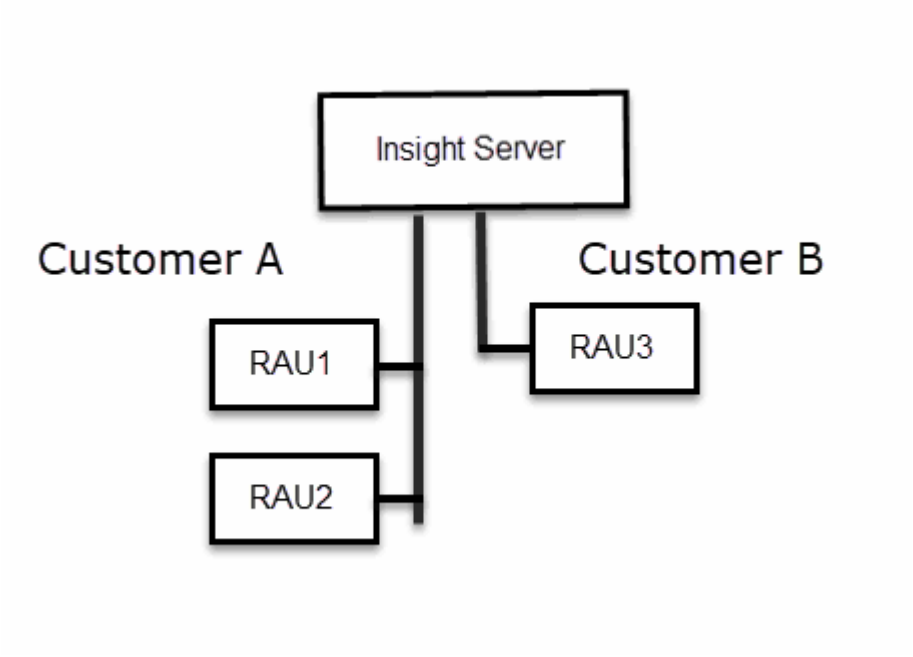
Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (Sie haben ein Rekeying durchgeführt oder Passwörter geändert), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen eines Software-Upgrades wird das System auf eine Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System auf die Standardkonfiguration zurückgesetzt wird, müssen Sie die nicht voreingestellte Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Schlüsselmanagement in einer komplexen Service-Provider-Umgebung

Ein Service-Provider kann mehrere OnCommand Insight-Kunden hosten, die Daten erfassen. Die Schlüssel

schützen Kundendaten vor unberechtigtem Zugriff durch mehrere Kunden auf dem Insight Server. Die Daten jedes Kunden werden durch spezifische Schlüsselpaare geschützt.

Diese Implementierung von Insight kann wie in der folgenden Abbildung dargestellt konfiguriert werden.



Sie müssen in dieser Konfiguration für jeden Kunden individuelle Schlüssel erstellen. Kunde A benötigt identische Schlüssel für beide raus. Kunde B benötigt einen einzigen Schlüsselsatz.

Die Schritte, die Sie Unternehmen würden, um die Verschlüsselungsschlüssel für Kunde A zu ändern:

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU1 gehostet wird.
2. Starten Sie das Sicherheitsadministrator-Tool.
3. Wählen Sie Verschlüsselungsschlüssel ändern, um die Standardschlüssel zu ersetzen.
4. Wählen Sie Backup, um eine ZIP-Sicherungsdatei der Sicherheitskonfiguration zu erstellen.
5. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU2 gehostet wird.
6. Kopieren Sie die Sicherungszip-Datei der Sicherheitskonfiguration auf RAU2.
7. Starten Sie das Sicherheitsadministrator-Tool.
8. Stellen Sie die Sicherheitssicherung von RAU1 auf dem aktuellen Server wieder her.

Die Schritte, die Sie Unternehmen würden, um die Verschlüsselungsschlüssel für Kunde B zu ändern:

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU3 gehostet wird.
2. Starten Sie das Sicherheitsadministrator-Tool.
3. Wählen Sie Verschlüsselungsschlüssel ändern, um die Standardschlüssel zu ersetzen.
4. Wählen Sie Backup, um eine ZIP-Sicherungsdatei der Sicherheitskonfiguration zu erstellen.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Insight-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.
4. Wählen Sie **Server**.

   Die folgenden Serverkonfigurationsoptionen stehen zur Verfügung:

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

     > Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Ändern des Server-Verschlüsselungsschlüssels auf einem Server - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server

   - **Verschlüsselungsschlüssel Ändern**

     Ändern Sie den Server-Verschlüsselungsschlüssel, der zum Verschlüsseln oder Entschlüsseln von Proxy-Benutzerpasswörtern, SMTP-Benutzerpasswörtern, LDAP-Benutzerpasswörtern usw. verwendet

wird.

> Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Passwort Aktualisieren**

  Ändern Sie das Passwort für die internen Konten, die von Insight verwendet werden. Folgende Optionen werden angezeigt:

  - _Intern
  - Akquisition
  - cognos_admin
  - dwh_intern
  - Hosts
  - Inventar
  - Stamm

> Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt Schlüssel und Passwörter auf die Standardwerte zurück. Standardwerte sind die Werte, die während der Installation angegeben werden.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

  a. Wählen Sie die Option aus, die Sie ändern möchten, und folgen Sie den Anweisungen.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Insight-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.
4. Wählen Sie **Local Acquisition Unit** aus, um die Sicherheitskonfiguration der Local Acquisition Unit neu zu konfigurieren.

   Folgende Optionen werden angezeigt:

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

     > Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf DEM LAU ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf jedem der Raus
   - **Verschlüsselungsschlüssel Ändern**

     Ändern Sie die AU-Verschlüsselungsschlüssel, die zum Verschlüsseln oder Entschlüsseln von Gerätepasswörtern verwendet werden.

     > Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Passwort Aktualisieren**

  Passwort für 'Acquisition'-Benutzerkonto ändern.

  > Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt das Erfassungs-Benutzerpasswort und die Erfassungs-Benutzerverschlüsselungsschlüssel auf die Standardwerte zurück. Bei der Installation werden die Standardwerte angegeben.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

5. Wählen Sie die Option aus, die Sie konfigurieren möchten, und befolgen Sie die 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 Benutzerpasswords für die 'Erfassung', wenn das Passwort für diesen Benutzer auf dem Server geändert wurde. Für die Kommunikation mit dem Server verwenden alle RAUS und DIE LAU dasselbe Passwort wie das des Benutzers „Acquisition“ des Servers.

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.

Gehen Sie wie folgt vor, um Sicherheitsoptionen auf einer rau zu verwalten:

Schritte

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem die rau ausgeführt wird
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:

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

  Das System fordert Anmeldeinformationen an.

3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.

   Das System zeigt das Menü für die rau an.

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`

   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

     > Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf einem Server ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server

   - **Verschlüsselungsschlüssel Ändern**

     Ändern Sie die rau-Verschlüsselungsschlüssel, die zum Verschlüsseln oder Entschlüsseln von Gerätekennwörtern verwendet werden.

     > Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

   - **Passwort Aktualisieren**

     Passwort für 'Acquisition'-Benutzerkonto ändern.

     > Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

   - **Auf die Standardeinstellungen zurücksetzen**

     Setzt die Verschlüsselungsschlüssel und Passwörter auf die Standardwerte zurück. Standardwerte

sind die Werte, die während der Installation angegeben werden.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Data Warehouse-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.

   Das System zeigt das Menü Sicherheitsverwaltung für das Data Warehouse an:

   - **Backup**

     Erstellt eine ZIP-Sicherungsdatei des Tresors, die alle Kennwörter und Schlüssel enthält, und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an dem Standardspeicherort ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

> Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf einem Server ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server
>
> +

- **Chiffrierschlüssel ändern**

  Ändern Sie den DWH-Verschlüsselungsschlüssel, der zum Verschlüsseln oder Entschlüsseln von Kennwörtern wie Verbindungskennwörtern und SMPT-Kennwörtern verwendet wird.

- **Passwort Aktualisieren**

  Kennwort für ein bestimmtes Benutzerkonto ändern.

  - _Intern
  - Akquisition
  - cognos_admin
  - dwh
  - dwh_intern
  - Whuser
  - Hosts
  - Inventar
  - Stamm

> Wenn Sie die Kennwörter für dwhuser, Hosts, Inventar oder Root ändern, haben Sie die Möglichkeit, SHA-256-Passwort-Hashing zu verwenden. Für diese Optionen müssen alle Clients, die auf die Konten zugreifen, SSL-Verbindungen verwenden.

+

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt die Verschlüsselungsschlüssel und Passwörter auf die Standardwerte zurück. Standardwerte sind die Werte, die während der Installation angegeben werden.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

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.

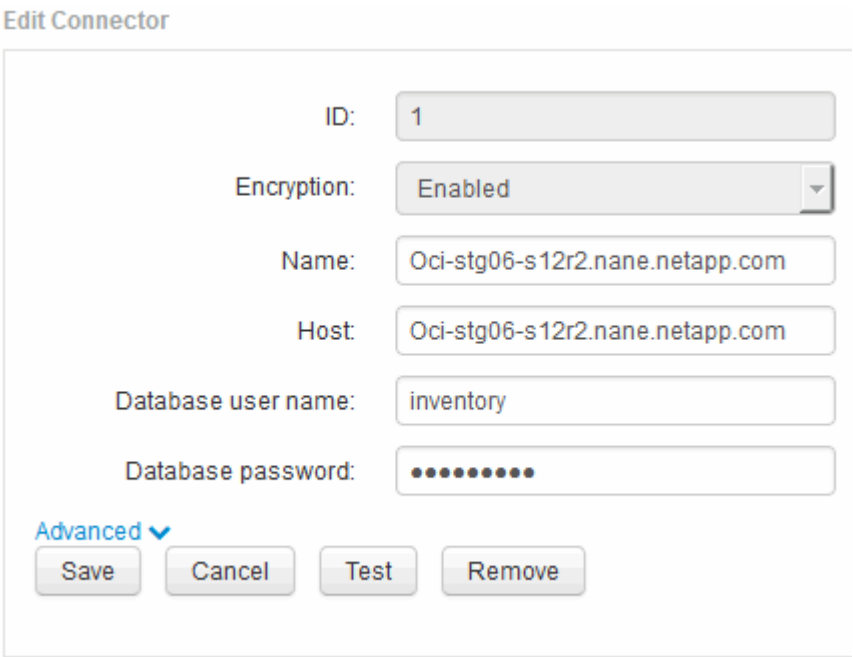
Bevor Sie beginnen

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

Schritte

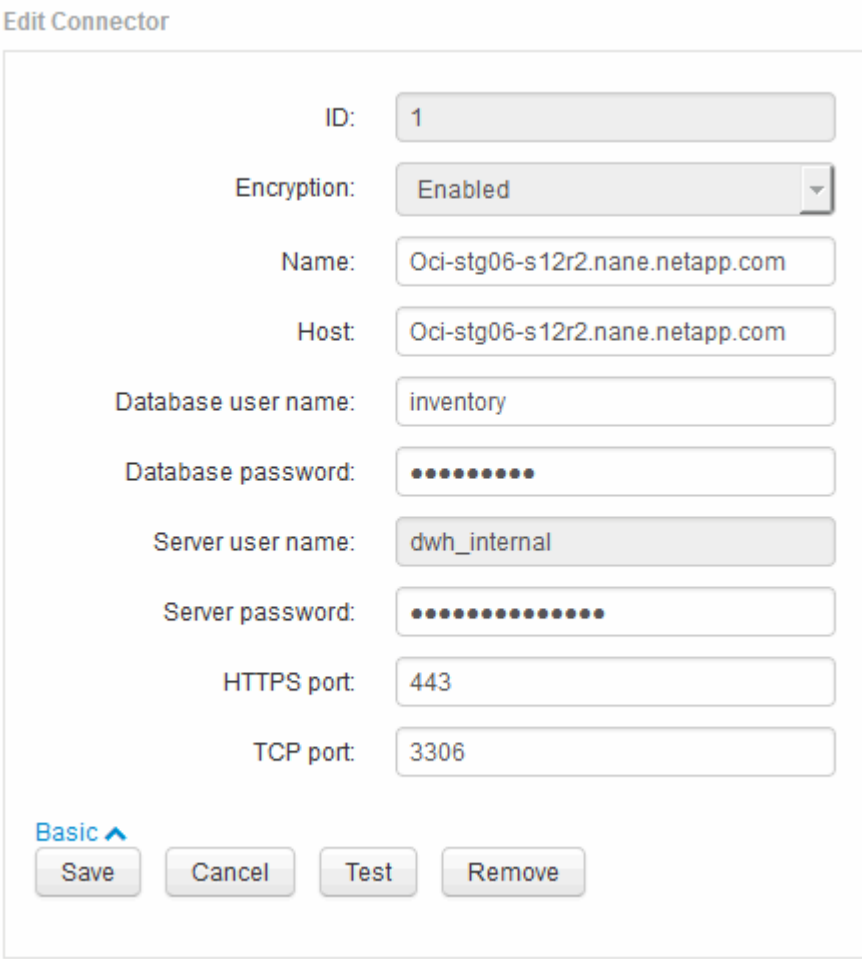
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   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.

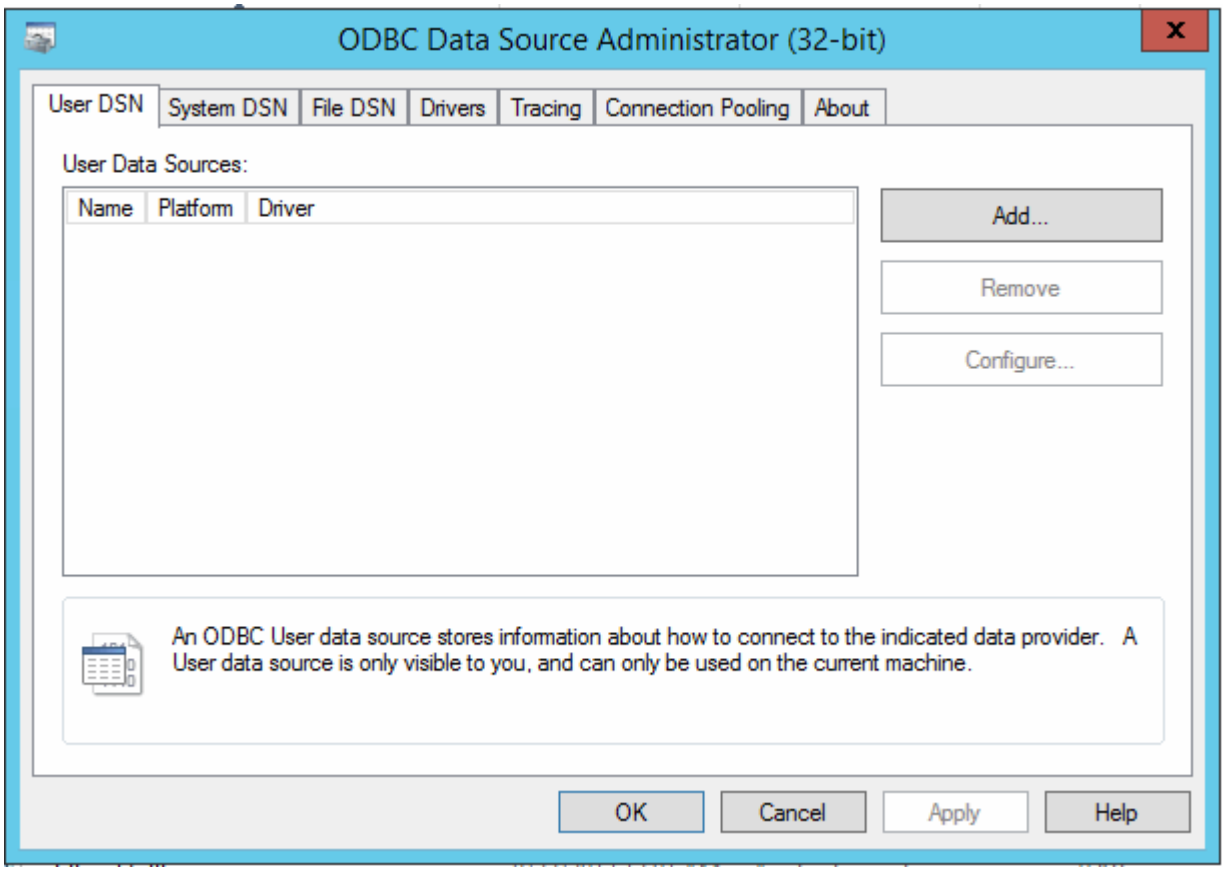
Bevor Sie beginnen

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

Schritte

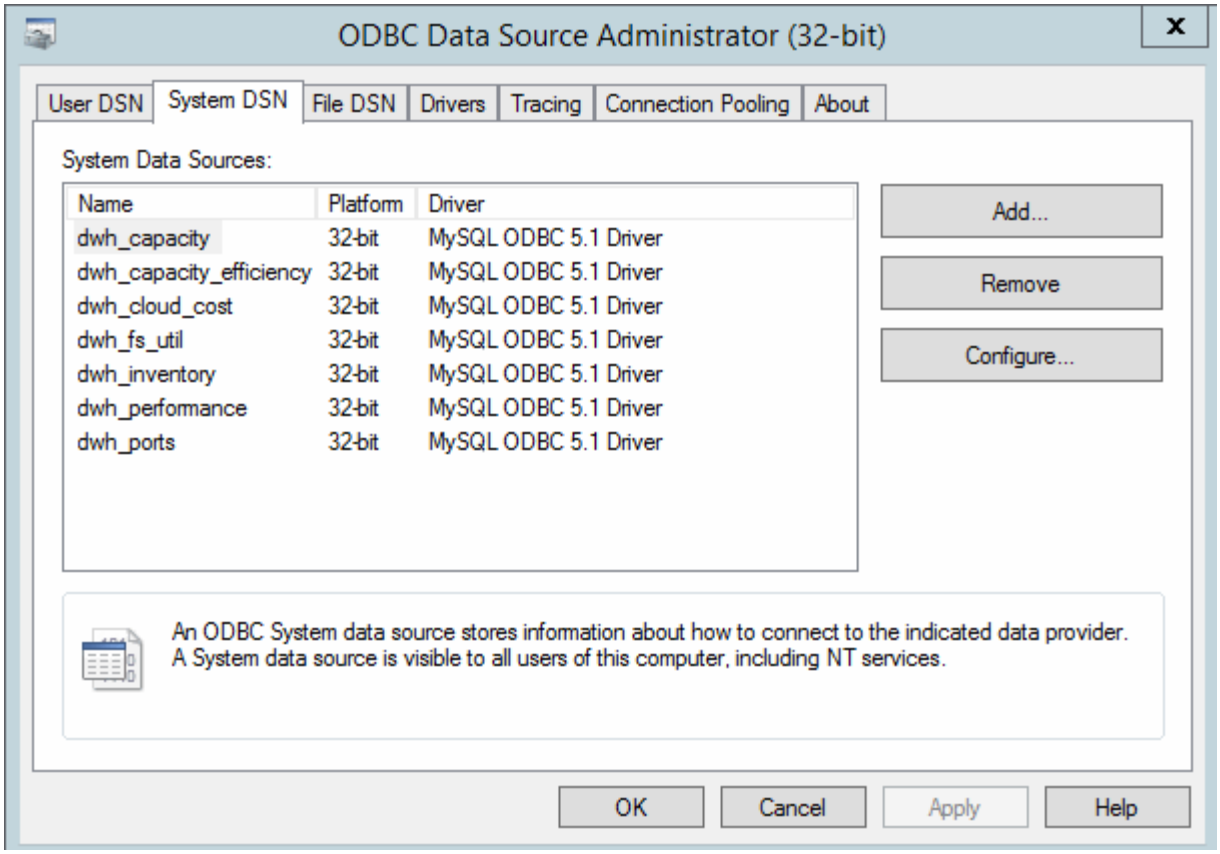
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

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



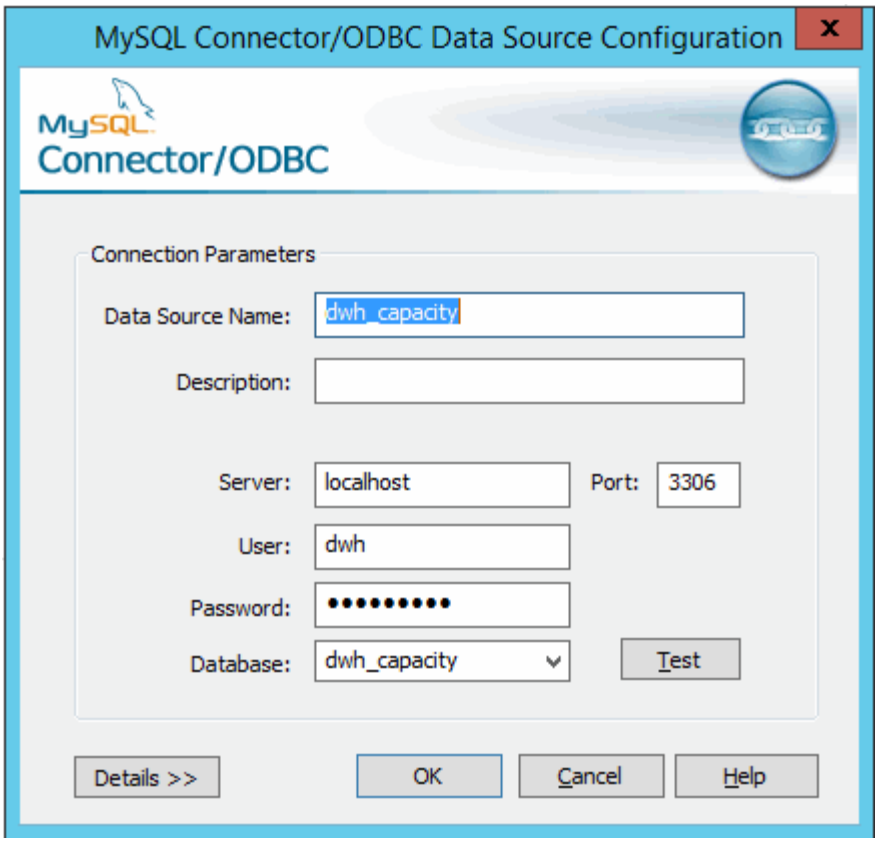
3. Klicken Sie auf **System DSN**

   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.