



# **Sécurité des données Insight**

## **OnCommand Insight**

NetApp  
April 01, 2024

# Sommaire

- Sécurité des données Insight . . . . . 1
  - Génération de nouvelles clés sur les serveurs . . . . . 1
  - Modification du mot de passe utilisateur acquisition . . . . . 1
  - Mise à niveau et installation . . . . . 1
  - La gestion des clés dans un environnement complexe de fournisseurs de services . . . . . 1
  - Gestion de la sécurité sur le serveur Insight . . . . . 2
  - Gestion de la sécurité sur l'unité d'acquisition locale . . . . . 4
  - Gestion de la sécurité sur un RAU . . . . . 6
  - Gestion de la sécurité dans l'entrepôt de données . . . . . 8
  - Modification des mots de passe des utilisateurs internes OnCommand Insight . . . . . 9

# Sécurité des données Insight

La version 7.3.1 de OnCommand Insight a introduit des fonctions de sécurité qui permettent aux environnements Insight de fonctionner avec une sécurité renforcée. Les fonctionnalités comprennent des améliorations au cryptage, le hachage des mots de passe et la possibilité de modifier les mots de passe et les paires de clés d'utilisateur internes qui cryptent et décryptent les mots de passe. Vous pouvez gérer ces fonctionnalités sur tous les serveurs de l'environnement Insight.

L'installation par défaut d'Insight inclut une configuration de sécurité dans laquelle tous les sites de votre environnement partagent les mêmes clés et les mêmes mots de passe par défaut. Pour protéger vos données sensibles, NetApp vous recommande de modifier les clés par défaut et le mot de passe utilisateur acquisition après une installation ou une mise à niveau.

Les mots de passe cryptés de la source de données sont stockés dans la base de données Insight Server. Le serveur dispose d'une clé publique et crypte les mots de passe lorsqu'un utilisateur les saisit dans une page de configuration de source de données WebUI. Le serveur ne dispose pas des clés privées requises pour décrypter les mots de passe de la source de données stockés dans la base de données du serveur. Seules les unités d'acquisition (LAU, RAU) possèdent la clé privée de la source de données requise pour décrypter les mots de passe de la source de données.

## Génération de nouvelles clés sur les serveurs

L'utilisation de clés par défaut introduit une vulnérabilité de sécurité dans votre environnement. Par défaut, les mots de passe des sources de données sont stockés et cryptés dans la base de données Insight. Elles sont chiffrées à l'aide d'une clé commune à toutes les installations d'Insight. Dans une configuration par défaut, une base de données Insight envoyée à NetApp inclut des mots de passe qui pourraient théoriquement être déchiffrés par NetApp.

## Modification du mot de passe utilisateur acquisition

L'utilisation du mot de passe utilisateur « acquisition » par défaut introduit une vulnérabilité de sécurité dans votre environnement. Toutes les unités d'acquisition utilisent l'utilisateur « acquisition » pour communiquer avec le serveur. Raus avec des mots de passe par défaut peut théoriquement se connecter à n'importe quel serveur Insight en utilisant des mots de passe par défaut.

## Mise à niveau et installation

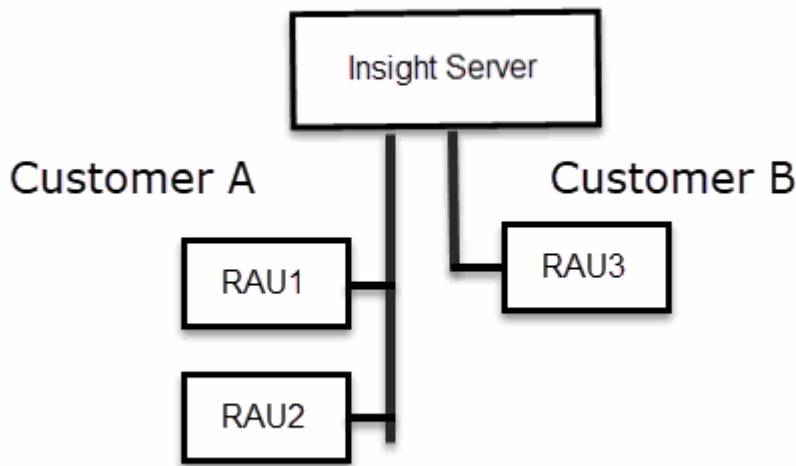
Lorsque votre système Insight contient des configurations de sécurité autres que celles par défaut (vous avez changé ou changé de mot de passe), vous devez sauvegarder vos configurations de sécurité. L'installation de nouveaux logiciels ou, dans certains cas, la mise à niveau de logiciels restaure la configuration de sécurité par défaut de votre système. Lorsque votre système revient à la configuration par défaut, vous devez restaurer la configuration non par défaut pour que le système fonctionne correctement.

## La gestion des clés dans un environnement complexe de fournisseurs de services

Un fournisseur de services peut héberger plusieurs clients OnCommand Insight qui recueillent des données. Ces clés protègent les données des clients contre tout accès non autorisé par plusieurs clients sur le serveur

Insight. Les données de chaque client sont protégées par des paires de clés spécifiques.

Cette implémentation d'Insight peut être configurée comme indiqué dans l'illustration suivante.



Vous devez créer des clés individuelles pour chaque client dans cette configuration. Le client A nécessite des clés identiques pour les deux Raus. Le client B nécessite un seul jeu de clés.

Procédure à suivre pour modifier les clés de cryptage du client A :

1. Effectuez une connexion à distance au serveur hébergeant RAU1.
2. Démarrez l'outil d'administration de la sécurité.
3. Sélectionnez Modifier la clé de cryptage pour remplacer les clés par défaut.
4. Sélectionnez Sauvegarder pour créer un fichier zip de sauvegarde de la configuration de sécurité.
5. Effectuez une connexion à distance au serveur hébergeant RAU2.
6. Copiez le fichier zip de sauvegarde de la configuration de sécurité dans RAU2.
7. Démarrez l'outil d'administration de la sécurité.
8. Restaurez la sauvegarde de sécurité de RAU1 vers le serveur actuel.

Procédure à suivre pour modifier les clés de cryptage du client B :

1. Effectuez une connexion à distance au serveur hébergeant RAU3.
2. Démarrez l'outil d'administration de la sécurité.
3. Sélectionnez Modifier la clé de cryptage pour remplacer les clés par défaut.
4. Sélectionnez Sauvegarder pour créer un fichier zip de sauvegarde de la configuration de sécurité.

## Gestion de la sécurité sur le serveur Insight

Le `securityadmin` Cet outil vous permet de gérer les options de sécurité sur le serveur Insight. La gestion de la sécurité inclut la modification des mots de passe, la génération

de nouvelles clés, l'enregistrement et la restauration des configurations de sécurité que vous créez ou la restauration des configurations par défaut.

## Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

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

## Étapes

1. Effectuez une connexion à distance au serveur Insight.
2. Démarrez l'outil d'administration de la sécurité en mode interactif :
  - Vitres - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
  - Linux : `/bin/oci-securityadmin.sh -i`

Le système demande des informations d'identification de connexion.
3. Entrez le nom d'utilisateur et le mot de passe d'un compte avec les informations d'identification « Admin ».
4. Sélectionnez **serveur**.

Les options de configuration de serveur suivantes sont disponibles :

- **Sauvegarde**

Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou aux emplacements par défaut suivants :

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

- **Restaurer**

Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.



La restauration peut être utilisée pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple : - Modifier la clé de cryptage du serveur sur un serveur - Créer une sauvegarde du coffre-fort - Restaurer la sauvegarde du coffre-fort sur le second serveur

- **Changer la clé de cryptage**

Modifiez la clé de cryptage du serveur utilisée pour crypter ou décrypter les mots de passe des utilisateurs proxy, les mots de passe des utilisateurs SMTP, les mots de passe des utilisateurs LDAP, etc.



Lorsque vous modifiez des clés de cryptage, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

#### ◦ **Mettre à jour le mot de passe**

Modifiez le mot de passe des comptes internes utilisés par Insight. Les options suivantes sont affichées :

- \_interne
- acquisition
- cognos\_admin
- dwh\_interne
- hôtes
- inventaire
- racine



Certains comptes doivent être synchronisés lorsque les mots de passe sont modifiés. Par exemple, si vous modifiez le mot de passe de l'utilisateur 'acquisition' sur le serveur, vous devez modifier le mot de passe de l'utilisateur 'acquisition' sur LAU, RAU et DWH pour qu'il corresponde. De même, lorsque vous modifiez des mots de passe, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

#### • **Rétablir les valeurs par défaut**

Réinitialise les clés et les mots de passe aux valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

#### • **Quitter**

Quittez le `securityadmin` outil.

- a. Choisissez l'option que vous souhaitez modifier et suivez les invites.

## **Gestion de la sécurité sur l'unité d'acquisition locale**

Le `securityadmin` L'outil vous permet de gérer les options de sécurité de l'utilisateur d'acquisition local (LAU). La gestion de la sécurité inclut la gestion des clés et des mots de passe, l'enregistrement et la restauration des configurations de sécurité que vous créez ou restaurez aux paramètres par défaut.

### **Avant de commencer**

Vous devez avoir `admin` privilèges permettant d'effectuer des tâches de configuration de la sécurité.

## Description de la tâche

Vous utilisez le securityadmin outil de gestion de la sécurité :

- Vitres - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux : /bin/oci-securityadmin.sh

## Étapes

1. Effectuez une connexion à distance au serveur Insight.
2. Démarrez l'outil d'administration de la sécurité en mode interactif :

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

Le système demande des informations d'identification de connexion.

3. Entrez le nom d'utilisateur et le mot de passe d'un compte avec les informations d'identification « Admin ».
4. Sélectionnez **unité d'acquisition locale** pour reconfigurer la configuration de sécurité de l'unité d'acquisition locale.

Les options suivantes sont affichées :

- **Sauvegarde**

Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou aux emplacements par défaut suivants :

- Vitres - C:\Program Files\SANscreen\backup\vault
- Linux : /var/log/netapp/oci/backup/vault

- **Restaurer**

Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.



Restore peut être utilisé pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple : - Modifier les clés de cryptage sur LE LAU - Créer une sauvegarde du coffre-fort - Restaurer la sauvegarde du coffre-fort sur chacun des Raus

- **Changer les clés de cryptage**

Modifiez les clés de cryptage au utilisées pour crypter ou décrypter les mots de passe des périphériques.



Lorsque vous modifiez des clés de cryptage, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

- **Mettre à jour le mot de passe**

Modifier le mot de passe du compte utilisateur « acquisition ».



Certains comptes doivent être synchronisés lorsque les mots de passe sont modifiés. Par exemple, si vous modifiez le mot de passe de l'utilisateur 'acquisition' sur le serveur, vous devez modifier le mot de passe de l'utilisateur 'acquisition' sur LAU, RAU et DWH pour qu'il corresponde. De même, lorsque vous modifiez des mots de passe, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

- **Rétablir les valeurs par défaut**

Réinitialise le mot de passe de l'utilisateur d'acquisition et les clés de cryptage de l'utilisateur d'acquisition sur les valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

- **Quitter**

Quittez le `securityadmin` outil.

5. Choisissez l'option que vous souhaitez configurer et suivez les invites.

## Gestion de la sécurité sur un RAU

Le `securityadmin` L'outil vous permet de gérer les options de sécurité sur Raus. Vous devrez peut-être sauvegarder ou restaurer une configuration de coffre-fort, modifier les clés de cryptage ou mettre à jour les mots de passe des unités d'acquisition.

### Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

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

Un scénario de mise à jour de la configuration de sécurité pour LE LAU, RAU est de mettre à jour le mot de passe utilisateur 'acquisition' lorsque le mot de passe de cet utilisateur a été modifié sur le serveur. Tous les Raus, et LE LAU utilisent le même mot de passe que celui de l'utilisateur d'acquisition du serveur pour communiquer avec le serveur.

L'utilisateur 'acquisition' n'existe que sur le serveur Insight. Le RAU ou LAU se connecte en tant qu'utilisateur lorsqu'il se connecte au serveur.

Procédez comme suit pour gérer les options de sécurité d'une unité RAU :

### Étapes

1. Effectuez une connexion à distance au serveur exécutant la RAU
2. Démarrez l'outil d'administration de la sécurité en mode interactif :

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

Le système demande des informations d'identification de connexion.



3. Entrez le nom d'utilisateur et le mot de passe d'un compte avec les informations d'identification « Admin ».

Le système affiche le menu de l'unité RAU.

- **Sauvegarde**

Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou aux emplacements par défaut suivants :

- Vitres - C:\Program Files\SANscreen\backup\vault
- Linux : /var/log/netapp/oci/backup/vault

- **Restaurer**

Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.



La restauration peut être utilisée pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple : - Modifier les clés de cryptage sur un serveur - Créer une sauvegarde du coffre-fort - Restaurer la sauvegarde du coffre-fort sur le second serveur

- **Changer les clés de cryptage**

Modifiez les clés de cryptage RAU utilisées pour crypter ou décrypter les mots de passe du terminal.



Lorsque vous modifiez des clés de cryptage, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

- **Mettre à jour le mot de passe**

Modifiez le mot de passe du compte utilisateur « acquisition ».



Certains comptes doivent être synchronisés lorsque les mots de passe sont modifiés. Par exemple, si vous modifiez le mot de passe de l'utilisateur 'acquisition' sur le serveur, vous devez modifier le mot de passe de l'utilisateur 'acquisition' sur LAU, RAU et DWH pour qu'il corresponde. De même, lorsque vous modifiez des mots de passe, vous devez sauvegarder votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

- **Rétablir les valeurs par défaut**

Réinitialise les clés de cryptage et les mots de passe aux valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

- **Quitter**

Quittez le securityadmin outil.

# Gestion de la sécurité dans l'entrepôt de données

Le `securityadmin` L'outil vous permet de gérer les options de sécurité sur le serveur Data Warehouse. La gestion de la sécurité inclut la mise à jour des mots de passe internes des utilisateurs internes sur le serveur DWH, la création de sauvegardes de la configuration de sécurité ou la restauration des configurations par défaut.

## Description de la tâche

Vous utilisez le `securityadmin` outil de gestion de la sécurité :

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

## Étapes

1. Effectuez une connexion à distance au serveur Data Warehouse.

2. Démarrez l'outil d'administration de la sécurité en mode interactif :

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

Le système demande des informations d'identification de connexion.

3. Entrez le nom d'utilisateur et le mot de passe d'un compte avec les informations d'identification « Admin ».

Le système affiche le menu d'administration de la sécurité pour l'entrepôt de données :

- **Sauvegarde**

Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou à l'emplacement par défaut :

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

- **Restaurer**

Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.



La restauration peut être utilisée pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple : - Modifier les clés de cryptage sur un serveur - Créer une sauvegarde du coffre-fort - Restaurer la sauvegarde du coffre-fort sur le second serveur

+

- **Changer les clés de cryptage**

Modifiez la clé de cryptage DWH utilisée pour crypter ou décrypter des mots de passe tels que les

mots de passe de connecteur et les mots de passe SMPT.

- **Mettre à jour le mot de passe**

Modifier le mot de passe d'un compte utilisateur spécifique.

- \_interne
- acquisition
- cognos\_admin
- dwh
- dwh\_interne
- dwhuser
- hôtes
- inventaire
- racine



Lorsque vous modifiez les mots de passe dwhuser, hosts, Inventory ou root, vous avez la possibilité d'utiliser le hachage de mot de passe SHA-256. Cette option nécessite que tous les clients accédant aux comptes utilisent des connexions SSL.

+

- **Rétablir les valeurs par défaut**

Réinitialise les clés de cryptage et les mots de passe aux valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

- **Quitter**

Quittez le securityadmin outil.

## Modification des mots de passe des utilisateurs internes OnCommand Insight

Les stratégies de sécurité peuvent vous obliger à modifier les mots de passe dans votre environnement OnCommand Insight. Certains mots de passe d'un serveur existent sur un serveur différent dans l'environnement, ce qui nécessite que vous modifiez le mot de passe sur les deux serveurs. Par exemple, lorsque vous modifiez le mot de passe utilisateur « Inventory » sur le serveur Insight Server, vous devez faire correspondre le mot de passe utilisateur « Inventory » sur le connecteur du serveur Data Warehouse configuré pour ce serveur Insight Server.

### Avant de commencer



Vous devez comprendre les dépendances des comptes d'utilisateur avant de modifier les mots de passe. Si vous ne mettez pas à jour les mots de passe sur tous les serveurs requis, les problèmes de communication entre les composants Insight seront à l'origine de ces échecs.

## Description de la tâche

Le tableau suivant répertorie les mots de passe des utilisateurs internes pour Insight Server et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe du serveur Insight	Modifications requises
_interne	
acquisition	LAU, RAU
dwh_interne	Entrepôt de données
hôtes	
inventaire	Entrepôt de données
racine	

Le tableau suivant répertorie les mots de passe des utilisateurs internes pour l'entrepôt de données et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe d'entrepôt de données	Modifications requises
cognos_admin	
dwh	
dwh_Internal (modifié à l'aide de l'interface utilisateur de configuration du connecteur du serveur)	Serveur Insight
dwhuser	
hôtes	
Inventaire (modifié à l'aide de l'interface utilisateur de configuration de Server Connector)	Serveur Insight
racine	

## Modification des mots de passe dans l'interface utilisateur de configuration de la connexion au serveur DWH

Le tableau suivant répertorie le mot de passe utilisateur POUR LAU et répertorie les composants Insight qui ont des mots de passe dépendants qui doivent correspondre au nouveau mot de passe.

Mots de passe LAU	Modifications requises
acquisition	Insight Server, RAU

## Modification des mots de passe “Inventory” et “dwh\_Internal” à l’aide de l’interface utilisateur Server Connection Configuration

Si vous devez modifier les mots de passe « Inventory » ou « dwh\_Internal » pour qu’ils correspondent à ceux du serveur Insight, vous utilisez l’interface utilisateur Data Warehouse.

### Avant de commencer

Vous devez être connecté en tant qu’administrateur pour effectuer cette tâche.

### Étapes

1. Connectez-vous au portail Data Warehouse à l’adresse <https://hostname/dwh>, Où hostname est le nom du système sur lequel est installé l’entrepôt de données OnCommand Insight.
2. Dans le volet de navigation de gauche, cliquez sur **connecteurs**.

L’écran **Edit Connector** s’affiche.

**Edit Connector**

ID:


Encryption:

Name:

Host:

Database user name:

Database password:

Advanced 

3. Entrez un nouveau mot de passe « inventaire » pour le champ **Mot de passe de la base de données**.
4. Cliquez sur **Enregistrer**
5. Pour modifier le mot de passe "dwh\_Internal", cliquez sur **Avancé**.

L’écran Editer connecteur avancé s’affiche.

### Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>
Server user name:	<input type="text" value="dwh_internal"/>
Server password:	<input type="password" value="....."/>
HTTPS port:	<input type="text" value="443"/>
TCP port:	<input type="text" value="3306"/>

Basic ^

6. Entrez le nouveau mot de passe dans le champ **Mot de passe du serveur** :

7. Cliquez sur enregistrer.

## Modification du mot de passe dwh à l'aide de l'outil d'administration ODBC

Lorsque vous modifiez le mot de passe sur pour l'utilisateur dwh sur le serveur Insight, le mot de passe doit également être modifié sur le serveur Data Warehouse. Vous utilisez l'outil Administrateur de source de données ODBC pour modifier le mot de passe de l'entrepôt de données.

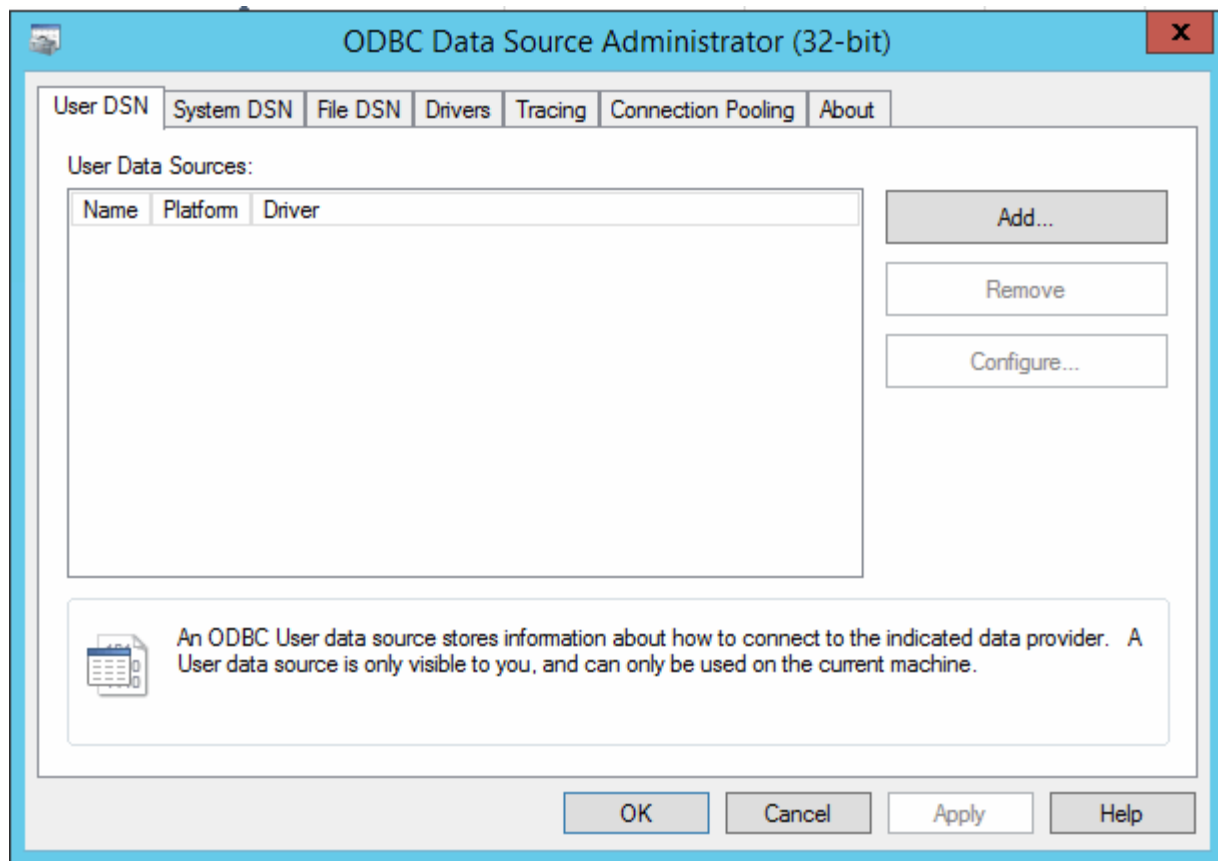
### Avant de commencer

Vous devez ouvrir une session à distance sur le serveur Data Warehouse à l'aide d'un compte disposant de privilèges d'administrateur.

### Étapes

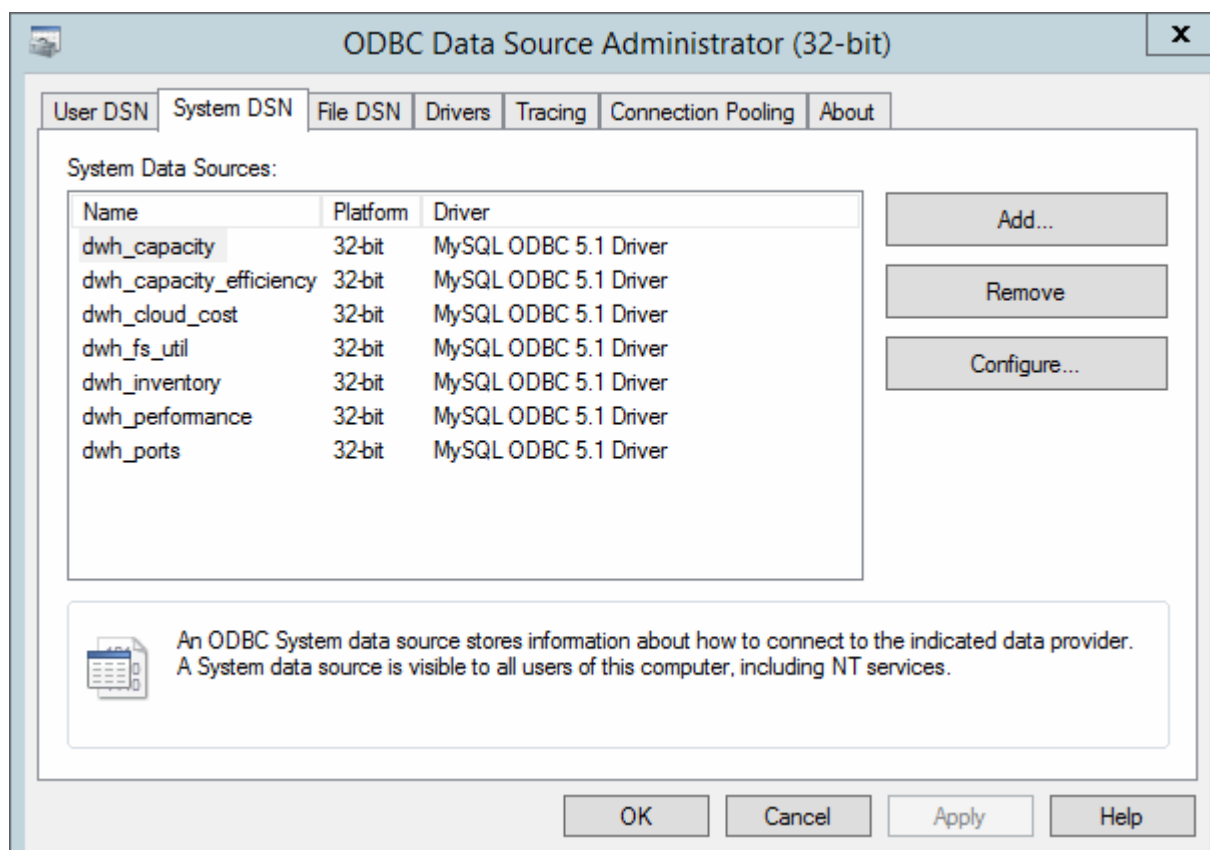
1. Effectuez une connexion à distance au serveur hébergeant cet entrepôt de données.
2. Accédez à l'outil d'administration ODBC à l'adresse C:\Windows\SysWOW64\odbcad32.exe

Le système affiche l'écran Administrateur de source de données ODBC.



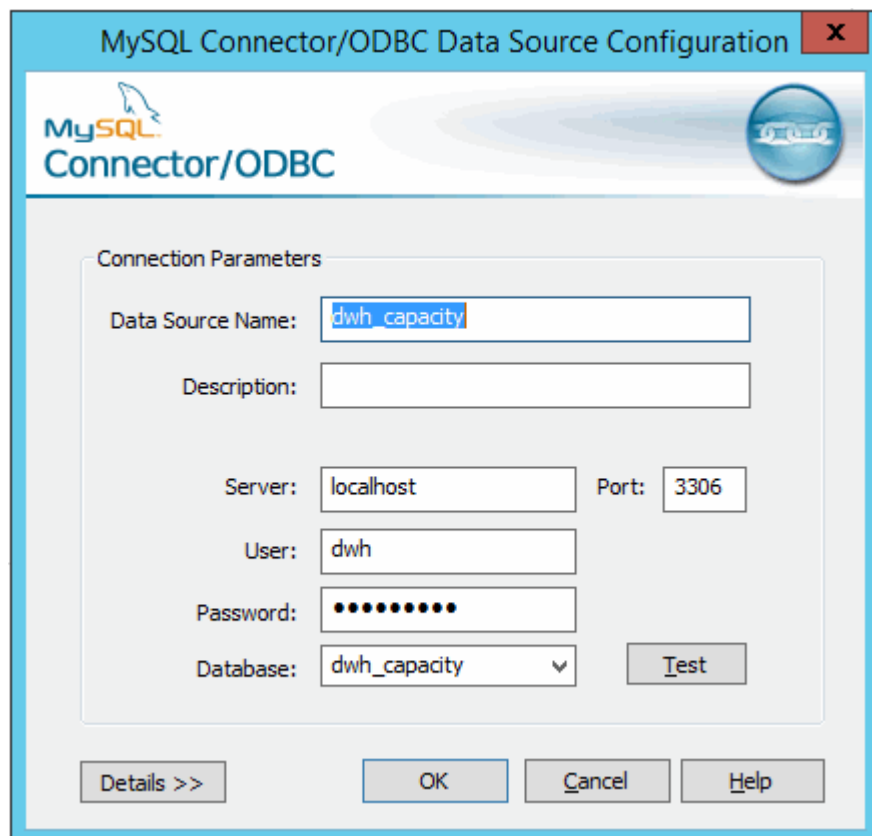
### 3. Cliquez sur **DSN système**

Les sources de données système s'affichent.



4. Sélectionnez une source de données OnCommand Insight dans la liste.
5. Cliquez sur **configurer**

L'écran Configuration de la source de données s'affiche.



The screenshot shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The title bar includes the text 'MySQL Connector/ODBC Data Source Configuration' and a close button. The dialog features the MySQL logo and a 'Connector/ODBC' label. The main section is titled 'Connection Parameters' and contains the following fields and controls:

- Data Source Name:** A text box containing 'dwh\_capacity'.
- Description:** An empty text box.
- Server:** A text box containing 'localhost'.
- Port:** A text box containing '3306'.
- User:** A text box containing 'dwh'.
- Password:** A text box filled with ten dots.
- Database:** A dropdown menu showing 'dwh\_capacity'.
- Test:** A button next to the Database dropdown.

At the bottom of the dialog, there are four buttons: 'Details >>', 'OK', 'Cancel', and 'Help'.

6. Entrez le nouveau mot de passe dans le champ **Mot de passe**.



## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.