Insight Security (outil SecurityAdmin)

OnCommand Insight

NetApp
October 24, 2024

Sommaire

Outil SecurityAdmin

OnCommand Insight fournit des fonctionnalités qui permettent aux environnements Insight de fonctionner avec une sécurité renforcée. Ces fonctionnalités comprennent le cryptage, le hachage de mot de passe et la possibilité de modifier les mots de passe des utilisateurs internes et les paires de clés qui chiffrent et déchiffrent les mots de passe. Vous pouvez gérer ces fonctionnalités sur tous les serveurs de l'environnement Insight à l'aide de **SecurityAdmin Tool**.

Qu'est-ce que l'outil SecurityAdmin ?

L'outil d'administration de la sécurité prend en charge les modifications apportées au contenu des coffres-forts ainsi que les modifications coordonnées apportées à l'installation de OnCommand Insight.

Les principales utilisations de l'outil SecurityAdmin sont **Backup** et **Restore** de la configuration de la sécurité (c'est-à-dire du coffre-fort) et des mots de passe. Par exemple, vous pouvez sauvegarder le coffre-fort sur une unité d'acquisition locale et le restaurer sur une unité d'acquisition distante, assurant ainsi la coordination des mots de passe dans l'ensemble de votre environnement. Ou si votre environnement comporte plusieurs serveurs OnCommand Insight, vous pouvez effectuer une sauvegarde du coffre-fort du serveur et le restaurer sur d'autres serveurs pour conserver les mêmes mots de passe. Ce ne sont que deux exemples de la façon dont SecurityAdmin peut être utilisé pour assurer la cohésion dans vos environnements.

Il est fortement recommandé de **sauvegarder le coffre-fort** chaque fois que vous sauvegardez une base de données OnCommand Insight. Le non-respect de cette consigne peut entraîner une perte d'accès.

L'outil fournit à la fois les modes **interactif** et **ligne de commande**.

De nombreuses opérations de l'outil SecurityAdmin modifient le contenu du coffre-fort et modifient également l'installation, en s'assurant que le coffre-fort et l'installation restent synchronisés.

Par exemple :

- Lorsque vous modifiez le mot de passe d'un utilisateur Insight, l'entrée de l'utilisateur dans le tableau SANscreen.users est mise à jour avec le nouveau hachage.
- Lorsque vous modifiez le mot de passe d'un utilisateur MySQL, l'instruction SQL appropriée est exécutée pour mettre à jour le mot de passe de l'utilisateur dans l'instance MySQL.

Dans certains cas, plusieurs modifications seront apportées à l'installation :

- Lorsque vous modifiez l'utilisateur MySQL dwh, en plus de mettre à jour le mot de passe dans la base de données MySQL, plusieurs entrées de registre pour ODBC seront également mises à jour.

Dans les sections suivantes, le terme « changements coordonnés » est utilisé pour décrire ces changements.

Modes d'exécution

- Fonctionnement normal/par défaut - le service serveur SANscreen doit être en cours d'exécution

  Pour le mode d'exécution par défaut, l'outil SecurityAdmin requiert que le service **SANscreen Server** soit en cours d'exécution. Le serveur est utilisé pour l'authentification et de nombreuses modifications

coordonnées de l'installation sont effectuées en appelant le serveur.

- Fonctionnement direct - le service serveur SANscreen peut être en cours d'exécution ou arrêté.

  Lorsqu'il est exécuté sur une installation d'OCI Server ou DWH, l'outil peut également être exécuté en mode « direct ». Dans ce mode, l'authentification et les modifications coordonnées sont effectuées à l'aide de la base de données. Le service serveur n'est pas utilisé.

  Le fonctionnement est le même que le mode normal, à l'exception des cas suivants :

- L'authentification est prise en charge uniquement pour les utilisateurs non administrateurs de domaine. (Utilisateurs dont le mot de passe et les rôles sont dans la base de données, et non LDAP).
- L'opération « remplacer les clés » n'est pas prise en charge.
- L'étape de re-chiffrement de la restauration du coffre-fort est ignorée.
- Mode de récupération l'outil peut également être exécuté même si l'accès au serveur et à la base de données n'est pas possible (par exemple parce que le mot de passe racine dans le coffre-fort est incorrect).

  Lorsqu'elle est exécutée dans ce mode, l'authentification n'est pas possible et, par conséquent, aucune opération avec une modification coordonnée de l'installation ne peut être effectuée.

  Le mode de récupération peut être utilisé pour :

- déterminez les entrées du coffre-fort incorrectes (à l'aide de l'opération de vérification)
- remplacez le mot de passe root incorrect par la valeur correcte. (Ceci ne modifie pas le mot de passe. L'utilisateur doit saisir le mot de passe actuel.)

> Si le mot de passe root du coffre-fort est incorrect et que le mot de passe n'est pas connu et qu'il n'y a pas de sauvegarde du coffre-fort avec le mot de passe root correct, l'installation ne peut pas être récupérée à l'aide de l'outil SecurityAdmin. La seule façon de récupérer l'installation est de réinitialiser le mot de passe de l'instance MySQL en suivant la procédure décrite à https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Après avoir effectué la procédure de réinitialisation, utilisez l'opération correct-stocké-password pour entrer le nouveau mot de passe dans le coffre-fort.

Commandes

Commandes non restreintes

Les commandes non restreintes modifient l'installation de manière coordonnée (sauf les magasins de confiance). Des commandes non restreintes peuvent être exécutées sans authentification de l'utilisateur.

Commande	Description

archivage sécurisé	Créez un fichier zip contenant le coffre-fort. Le chemin relatif vers les fichiers du coffre-fort correspond au chemin du coffre-fort par rapport à la racine d'installation. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Notez qu'il est fortement recommandé de sauvegarder le coffre-fort chaque fois que vous sauvegardez une base de données OnCommand Insight.
vérifiez-les-clés-par-défaut	Vérifiez si les clés du coffre-fort correspondent à celles du coffre-fort par défaut utilisé dans les instances antérieures à 7.3.16.
mot de passe-stocké-correct	Remplacez un mot de passe (incorrect) stocké dans le coffre-fort par le mot de passe correct connu de l'utilisateur. Ceci peut être utilisé lorsque le coffre-fort et l'installation ne sont pas cohérents. **Notez qu'il ne modifie pas le mot de passe réel dans l'installation.**
	Changer-confiance-mot-de-passe-magasin modifiez le mot de passe utilisé pour un magasin de confiance et stockez le nouveau mot de passe dans le coffre-fort. Le mot de passe actuel du magasin de confiance doit être « connu ».
vérifier-keystore	vérifiez si les valeurs dans le coffre-fort sont correctes: • Pour les utilisateurs d'OCI, le hachage du mot de passe correspond-t-il à la valeur de la base de données • Pour les utilisateurs de MySQL, une connexion à la base de données peut-elle être établie • pour les magasins de clés, le magasin de clés peut-il être chargé et ses clés (le cas échéant) peuvent-elles être lues
touches de liste	répertorier les entrées dans le coffre-fort (sans afficher la valeur stockée)

Commandes restreintes

L'authentification est requise pour toute commande non masquée qui apporte des modifications coordonnées à l'installation :

Commande	Description

restauration-archivage-sauvegarde	Remplace le coffre-fort actuel par le coffre-fort contenu dans le fichier de sauvegarde de coffre-fort spécifié. Exécute toutes les actions coordonnées pour mettre à jour l'installation en fonction des mots de passe du coffre-fort restauré : • Mettez à jour les mots de passe des utilisateurs de communication OCI • Mettez à jour les mots de passe utilisateur MySQL, y compris root • pour chaque magasin de clés, si le mot de passe du magasin de clés est « connu », mettez à jour le magasin de clés à l'aide des mots de passe du coffre-fort restauré. Lorsqu'elle est exécutée en mode normal, elle lit également chaque valeur chiffrée de l'instance, la décrypte à l'aide du service de cryptage du coffre-fort actuel, la re-crypte à l'aide du service de cryptage du coffre-fort restauré et stocke la valeur de nouveau cryptage.
synchroniser-avec-coffre-fort	Exécute toutes les actions coordonnées pour mettre à jour l'installation en fonction des mots de passe utilisateur dans le coffre-fort restauré : • Met à jour les mots de passe des utilisateurs de communication OCI • Met à jour les mots de passe utilisateur MySQL, y compris root
changer-mot-de-passe	Modifie le mot de passe dans le coffre-fort et exécute les actions coordonnées.
remplacer les clés	Créez un nouveau coffre-fort vide (qui aura des clés différentes de celles du coffre-fort existant). Copiez ensuite les entrées du coffre-fort actuel dans le nouveau coffre-fort. Lit ensuite chaque valeur chiffrée de l'instance, la déchiffre à l'aide du service de cryptage du coffre-fort actuel, la recrypte à l'aide du service de cryptage du coffre-fort restauré et stocke la valeur re-chiffrée.

Actions coordonnées

Coffre-fort du serveur

_interne	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données
acquisition	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données si le coffre-fort d'acquisition est présent, mettez également à jour l'entrée dans le coffre-fort d'acquisition
dwh_interne	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données

cognos_admin	mettre à jour le hachage du mot de passe pour l'utilisateur dans la base de données Si DWH et Windows, mettez à jour SANscreen/cognos/analytics/configuration/SANscreenAP.properties pour définir la propriété cognos.admin sur le mot de passe.
racine	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
inventaire	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
dwh	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL Si DWH et Windows, mettez à jour le registre Windows pour définir les entrées liées ODBC suivantes sur le nouveau mot de passe : • 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
dwhuser	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL

hôtes	Exécutez SQL pour mettre à jour le mot de passe utilisateur dans l'instance MySQL
keystore_password	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/server.keystore
truststore_password	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/server.trustore
mot_de_passe_clé	réécrivez le magasin de clés avec le nouveau mot de passe : wildfly/standalone/configuration/sso.jks
cognos_archive	Aucune

Coffre-fort d'acquisition

acquisition	Aucune
truststore_password	réécrivez le magasin de clés avec le nouveau mot de passe (s'il existe) - acq/conf/cert/client.keystore

Exécution de l'outil d'administration de sécurité - ligne de commande

La syntaxe pour exécuter l'outil sa en mode ligne de commande est la suivante :

```
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
```

Remarques :

- L'option "-i" peut ne pas être présente sur la ligne de commande (car cela sélectionne le mode interactif).

- pour les options "-s" et "-au" :
  - "-s" n’est pas autorisé sur un RAU
  - "-au" n’est pas autorisé sur DWH
  - si aucune n’est présente, alors
    - Le coffre-fort du serveur est sélectionné sur Server, DWH et Dual
    - Le coffre-fort d’acquisition est sélectionné sur RAU
- Les options -lu et -lp sont utilisées pour l’authentification utilisateur.
  - Si <user> est spécifié et que <password> n’est pas, l’utilisateur est invité à entrer le mot de passe.
  - Si <user> n’est pas fourni et que l’authentification est requise, l’utilisateur est invité à entrer <user> et <password>.

Commandes :

Commande	Du stockage
mot de passe-stocké-correct	`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
 	
` `
	archivage sécurisé

`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 ` `

archivage sécurisé	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	touches de liste
`securityadmin [-s`	-au] [-db] -l where -l specified command ` `
touches de vérification	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ` `	vérifier-keystore (serveur)

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	mise à niveau

`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 ``
remplacer les clés	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restauration-archivage-sauvegarde
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

modifier le mot de passe (serveur)	`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`

modifier le mot de passe de l'utilisateur d'acquisition (acquisition)	`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 for truststore-_password (acquisition)	`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.`

synchroniser-avec-vault (serveur)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Exécution de l’outil d’administration de sécurité - mode interactif

Interactif - Menu principal

Pour exécuter l’outil sa en mode interactif, entrez la commande suivante :

```
 securityadmin -i
Sur un serveur ou une installation double, SecurityAdmin invite
l'utilisateur à sélectionner le serveur ou l'unité d'acquisition locale.
```

Nœuds de serveur et d’unité d’acquisition détectés ! Sélectionnez le nœud dont la sécurité doit être reconfigurée :

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

Sur DWH, "serveur" est automatiquement sélectionné. Sur un au distant, « unité d’acquisition » est automatiquement sélectionné.

Interactive - Server : récupération du mot de passe root

En mode serveur, l’outil SecurityAdmin vérifie d’abord que le mot de passe root enregistré est correct. Si ce n’est pas le cas, l’outil affiche l’écran de récupération du mot de passe racine.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Si l’option 1 est sélectionnée, l’utilisateur est invité à entrer le mot de passe correct.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Si le mot de passe correct est saisi, le message suivant s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe saisi est incorrect, le message suivant s'affiche

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Appuyez sur ENTER pour revenir au menu de récupération.
```

Si l'option 2 est sélectionnée, l'utilisateur est invité à fournir le nom d'un fichier de sauvegarde à partir duquel lire le mot de passe correct :

```
 Enter Backup File Location:
Si le mot de passe de la sauvegarde est correct, le message suivant
s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe de la sauvegarde est incorrect, le message suivant s'affiche

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Appuyez sur ENTER pour revenir au menu de récupération.
```

Interactive - serveur : mot de passe correct

L'action « Mot de passe correct » est utilisée pour modifier le mot de passe stocké dans le coffre-fort afin qu'il corresponde au mot de passe réel requis par l'installation. Cette commande est utile dans les situations où une modification de l'installation a été faite par quelque chose d'autre que l'outil securityadmin. Voici quelques exemples :

- Le mot de passe d'un utilisateur SQL a été modifié par l'accès direct à MySQL.
- Un magasin de clés est remplacé ou le mot de passe d'un magasin de clés est modifié à l'aide de keytool.
- Une base de données OCI a été restaurée et cette base de données a des mots de passe différents pour les utilisateurs internes

« Mot de passe correct » invite d'abord l'utilisateur à sélectionner le mot de passe pour enregistrer la valeur correcte.

```
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:
```

Après avoir sélectionné l'entrée à corriger, l'utilisateur est invité à indiquer la façon dont il souhaite fournir la valeur.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Si l'option 1 est sélectionnée, l'utilisateur est invité à entrer le mot de passe correct.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Si le mot de passe correct est saisi, le message suivant s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour revenir au menu sans restriction du serveur.
```

Si le mot de passe saisi est incorrect, le message suivant s'affiche

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

Appuyez sur entrée pour revenir au menu sans restriction du serveur.

Si l'option 2 est sélectionnée, l'utilisateur est invité à fournir le nom d'un fichier de sauvegarde à partir duquel lire le mot de passe correct :

```
 Enter Backup File Location:
Si le mot de passe de la sauvegarde est correct, le message suivant
s'affiche.
```

```
 Password verified.  Vault updated
Appuyez sur entrée pour afficher le menu sans restriction du serveur.
```

Si le mot de passe de la sauvegarde est incorrect, le message suivant s'affiche

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

Appuyez sur entrée pour afficher le menu sans restriction du serveur.

Interactive - serveur : vérifiez le contenu du coffre-fort

Vérifier le contenu du coffre-fort vérifiera si le coffre-fort a des clés qui correspondent au coffre-fort par défaut distribué avec les versions antérieures d'OCI et vérifiera si chaque valeur du coffre-fort correspond à l'installation.

Les résultats possibles pour chaque clé sont les suivants :

OK	La valeur du coffre-fort est correcte
Non cochée	La valeur ne peut pas être vérifiée par rapport à l'installation
MAUVAIS	La valeur ne correspond pas à l'installation
Manquant	Une entrée attendue est manquante.

```
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
```

Interactive - serveur : sauvegarde

Backup demande le répertoire dans lequel le fichier zip de sauvegarde doit être stocké. Le répertoire doit déjà exister et le nom du fichier sera 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 - serveur : connexion

L'action de connexion permet d'authentifier un utilisateur et d'accéder aux opérations qui modifient l'installation. L'utilisateur doit avoir admin Privileges. Lors de l'exécution avec le serveur, tout utilisateur administrateur peut être utilisé ; lors de l'exécution en mode direct, l'utilisateur doit être un utilisateur local plutôt qu'un utilisateur LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

ou

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

UserName: admin

Password:
```

Si le mot de passe est correct et que l'utilisateur est un utilisateur admin, le menu restreint s'affiche.

Si le mot de passe est incorrect, le message suivant s'affiche :

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

UserName: admin

Password:

Login Failed!
```

Si l'utilisateur n'est pas un administrateur, les informations suivantes s'affichent :

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

Interactive - serveur : menu restreint

Une fois l'utilisateur connecté, l'outil affiche le menu restreint.

```
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 - serveur : modification du mot de passe

L'action « Modifier le mot de passe » permet de modifier un mot de passe d'installation en une nouvelle valeur.

« Modifier le mot de passe » invite d'abord l'utilisateur à sélectionner le mot de passe à modifier.

```
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:
```

Après avoir sélectionné l'entrée à corriger, si l'utilisateur est un utilisateur MySQL, l'utilisateur sera invité à confirmer le hachage du mot de passe

```
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
```

Ensuite, l'utilisateur est invité à entrer le nouveau mot de passe.

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

Password is empty - cancelling operation
```

Si un mot de passe non vide est saisi, l'utilisateur est invité à confirmer le mot de passe.

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

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Si la modification échoue, l'erreur ou l'exception s'affiche.

Interactive - serveur : restauration

Interactive - serveur : modification des clés de cryptage

L'action Modifier les clés de cryptage remplace la clé de cryptage utilisée pour crypter les entrées du coffre-fort et remplace la clé de cryptage utilisée pour le service de cryptage du coffre-fort. Comme la clé du service de chiffrement est modifiée, les valeurs cryptées dans la base de données sont à nouveau chiffrées ; elles sont lues, déchiffrées avec la clé actuelle, cryptées avec la nouvelle clé et enregistrées à nouveau dans la base de données.

Cette action n'est pas prise en charge en mode direct car le serveur fournit l'opération de re-chiffrement pour certains contenus de base de données.

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

Confirm (y/N): y

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

Interactive - serveur : installation fixe

L'action réparer l'installation mettra à jour l'installation. Tous les mots de passe d'installation modifiables via l'outil securityadmin, à l'exception de root, seront définis sur les mots de passe du coffre-fort.

- Les mots de passe des utilisateurs internes d'OCI seront mis à jour.
- Les mots de passe des utilisateurs MySQL, sauf root, seront mis à jour.
- Les mots de passe des keystores seront mis à jour.

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

Confirm:  (y/N): y

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

L'action s'arrête à la première mise à jour ayant échoué et affiche l'erreur ou l'exception.

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`

Pour plus d'informations, reportez-vous à la "Admin sécurité"documentation.

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`

Pour plus d'informations, reportez-vous aux "Outil SecurityAdmin"instructions.

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 consiste à mettre à jour le mot de passe utilisateur d'acquisition lorsque le mot de passe de cet utilisateur a été modifié sur le serveur. Le LAU et tous les Raus 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.

Pour plus d'informations, reportez-vous aux "Outil SecurityAdmin"instructions.

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`

Pour plus d'informations, reportez-vous à la "Admin sécurité"documentation.

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 modifiiez 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.

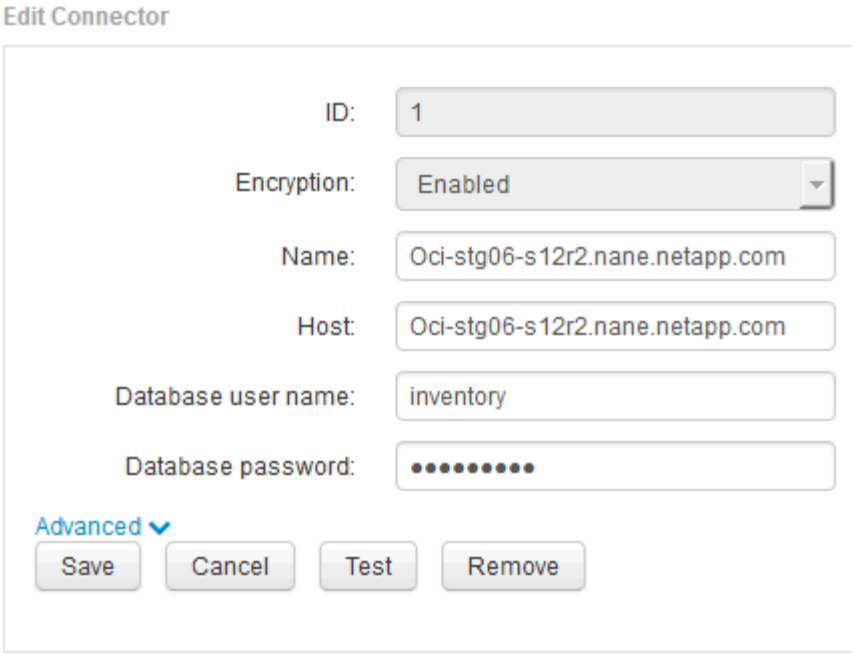
Avant de commencer

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

Étapes

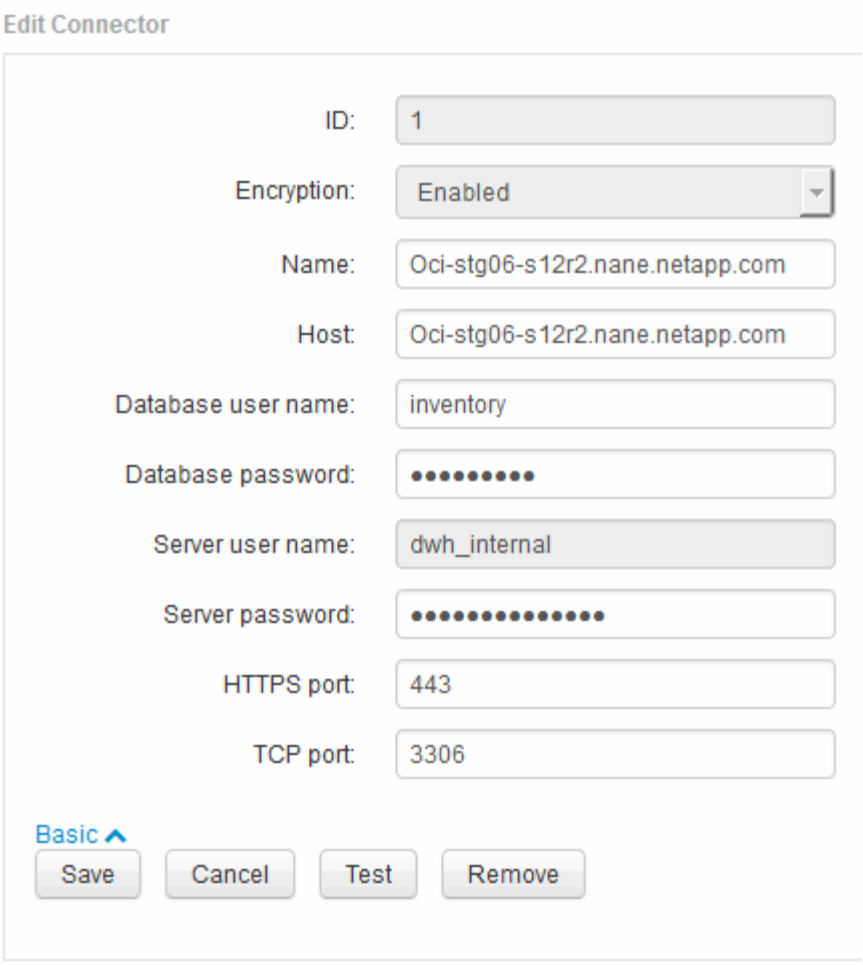
1. Connectez-vous au portail Data Warehouse à l'adresse https://hostname/dwh, Où hostname est le nom du système sur lequel est installé l'entrepôt de données OnCommand Insight.
2. Dans le volet de navigation de gauche, cliquez sur **connecteurs**.

   L'écran **Edit Connector** s'affiche.



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.



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.

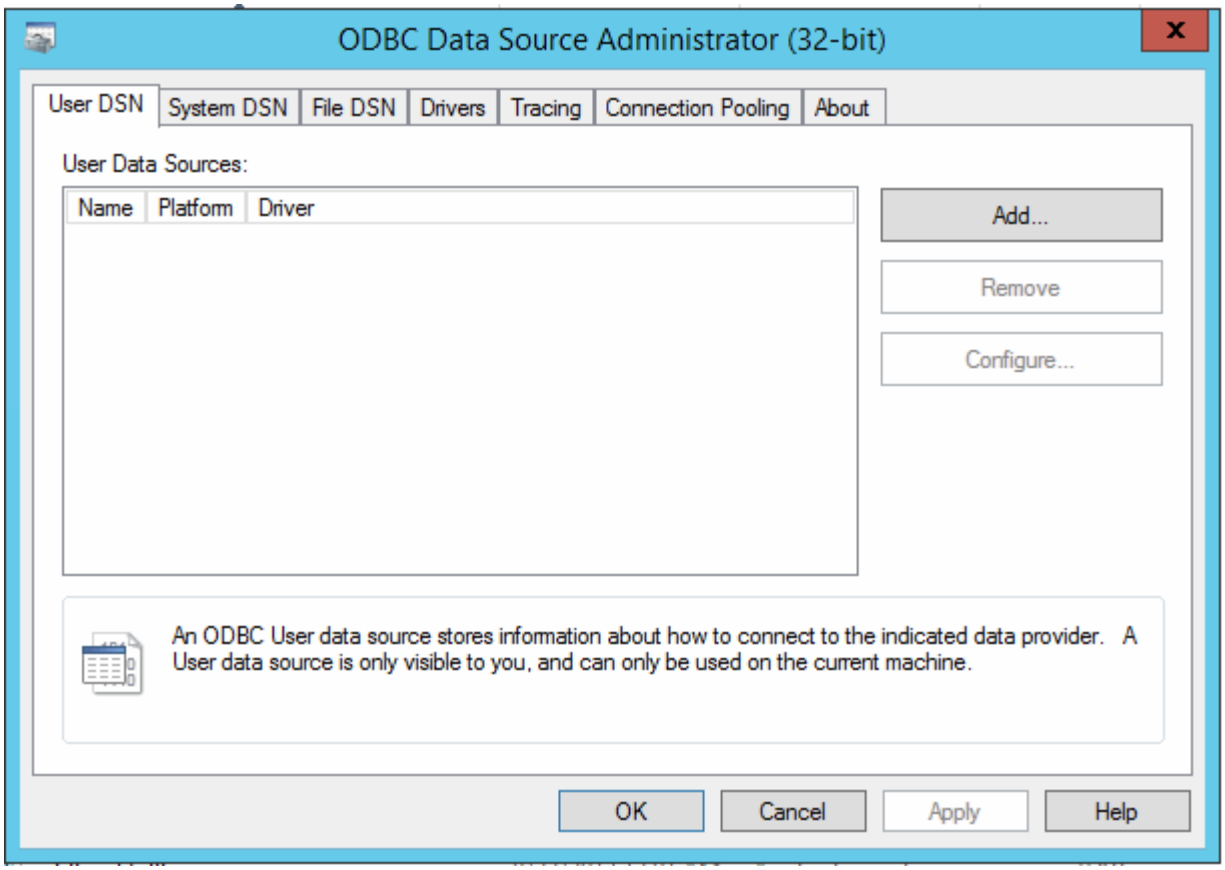
Avant de commencer

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

Étapes

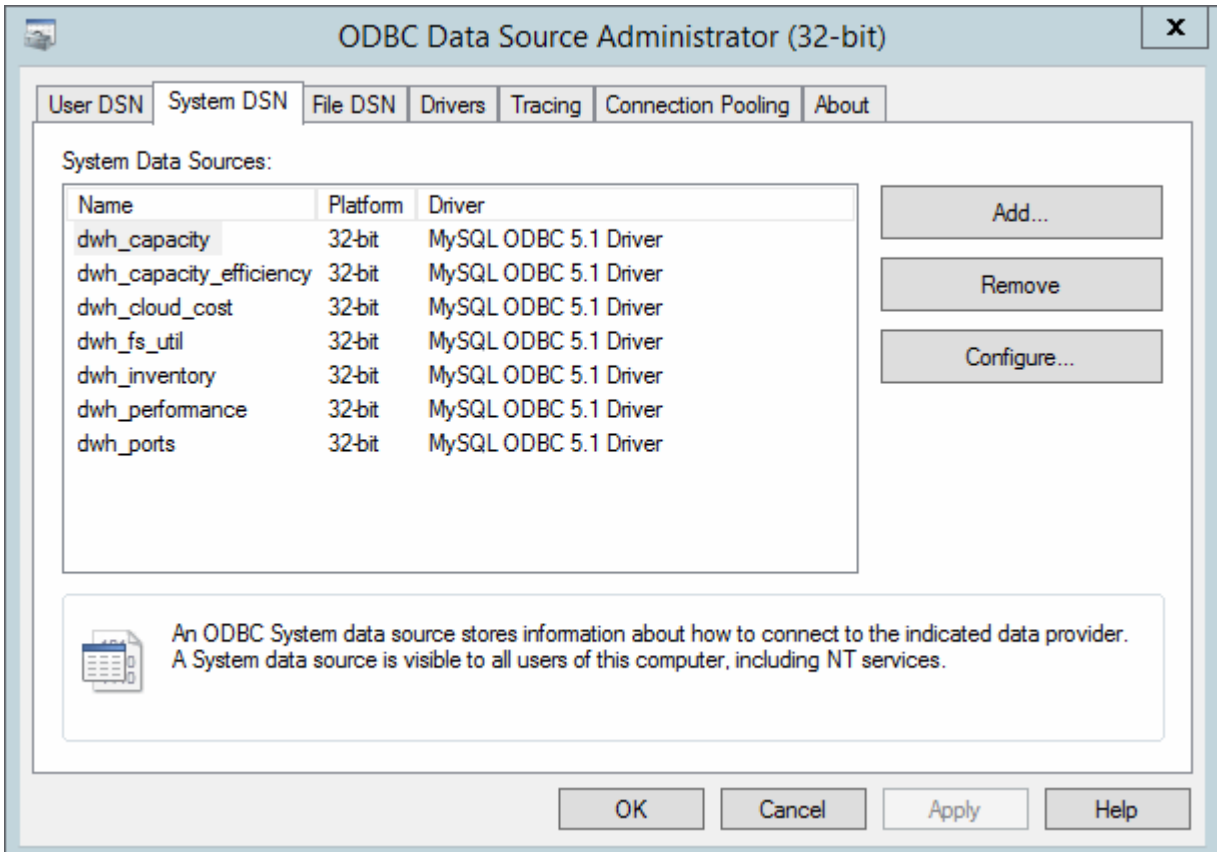
1. Effectuez une connexion à distance au serveur hébergeant cet entrepôt de données.
2. Accédez à l'outil d'administration ODBC à l'adresse `C:\Windows\SysWOW64\odbcad32.exe`

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



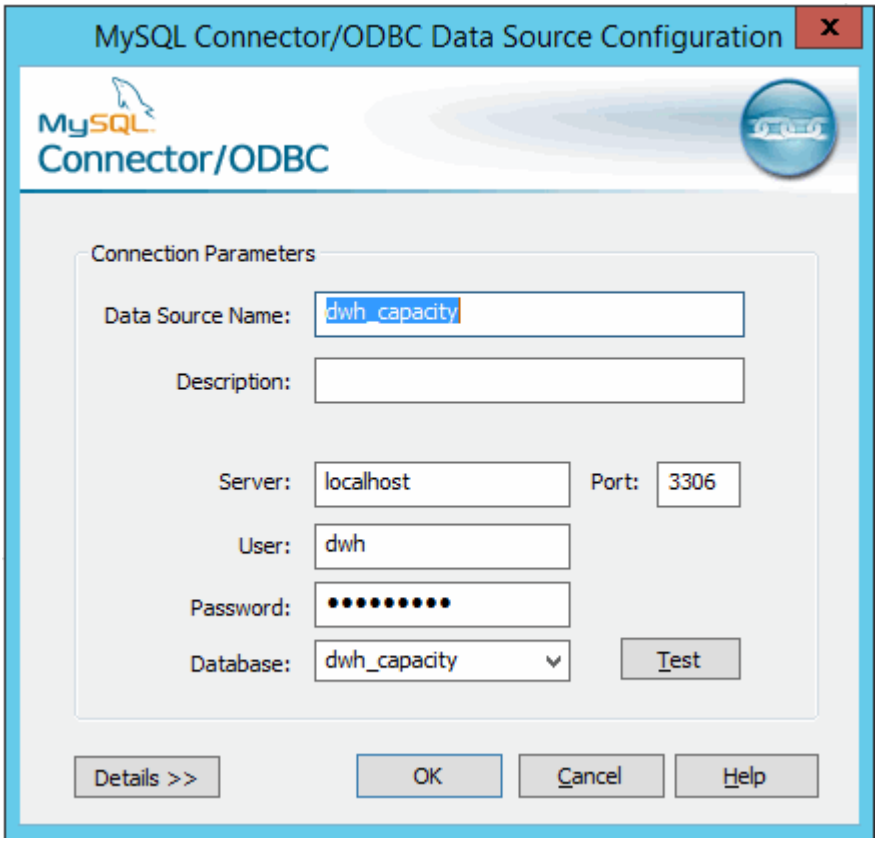
3. Cliquez sur **DSN système**

   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.



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

Informations sur le copyright

Informations sur les marques commerciales