Insight Security (herramienta SecurityAdmin)

OnCommand Insight

NetApp
October 24, 2024

Tabla de contenidos

Herramienta securityadmin

OnCommand Insight ofrece funciones que permiten a los entornos de Insight operar con seguridad mejorada. Estas características incluyen cifrado, hash de contraseñas y la capacidad de cambiar contraseñas de usuario internas y pares de claves que cifran y descifran contraseñas. Puede administrar estas funciones en todos los servidores del entorno Insight utilizando la herramienta **SecurityAdmin Tool**.

¿Qué es la herramienta SecurityAdmin?

La herramienta de administración de seguridad permite realizar cambios en el contenido de los almacenes, así como realizar cambios coordinados en la instalación de OnCommand Insight.

Los usos principales de la herramienta SecurityAdmin son para **Backup** y **Restore** de la configuración de seguridad (es decir, vault) y contraseñas. Por ejemplo, puede realizar una copia de seguridad del almacén en una unidad de adquisición local y restaurarlo en una unidad de adquisición remota, lo que garantiza la coordinación de contraseñas en todo el entorno. O bien, si tiene varios servidores OnCommand Insight en su entorno, puede que desee realizar una copia de seguridad del almacén del servidor y restaurarla en otros servidores para mantener las contraseñas iguales. Estos son solo dos ejemplos de las formas en que SecurityAdmin se puede utilizar para garantizar la cohesión en sus entornos.

Se recomienda encarecidamente **hacer una copia de seguridad del almacén** siempre que realice una copia de seguridad de una base de datos OnCommand Insight. Si no lo hace, puede producirse la pérdida de acceso.

La herramienta proporciona los modos **interactive** y **command line**.

Muchas de las operaciones de SecurityAdmin Tool cambian el contenido del almacén y también realizan cambios en la instalación, lo que garantiza que el almacén y la instalación permanecen sincronizados.

Por ejemplo:

- Al cambiar una contraseña de usuario de Insight, la entrada del usuario en la tabla SANscreen.users se actualizará con el nuevo hash.
- Al cambiar la contraseña de un usuario MySQL, se ejecutará la sentencia SQL adecuada para actualizar la contraseña del usuario en la instancia MySQL.

En algunas situaciones, se realizarán varios cambios en la instalación:

- Al modificar el usuario de dwh MySQL, además de actualizar la contraseña en la base de datos MySQL, también se actualizarán varias entradas de registro para ODBC.

En las siguientes secciones se utiliza el término “cambios coordinados” para describir estos cambios.

Modos de ejecución

- Operación normal/predeterminada: El servicio de servidor SANscreen debe estar en ejecución

  Para el modo de ejecución predeterminado, la herramienta SecurityAdmin requiere que el servicio **SANscreen Server** esté en ejecución. El servidor se utiliza para la autenticación, y muchos cambios coordinados en la instalación se realizan realizando llamadas al servidor.

- Operación directa: El servicio del servidor SANscreen puede estar en ejecución o detenido.

  Cuando se ejecuta en una instalación de servidor OCI o DWH, la herramienta también se puede ejecutar en modo “directo”. En este modo, la autenticación y los cambios coordinados se realizan mediante la base de datos. El servicio Servidor no se utiliza.

  El funcionamiento es el mismo que el modo normal, con las siguientes excepciones:

- La autenticación solo es compatible para usuarios administradores que no son de dominio. (Usuarios cuya contraseña y roles están en la base de datos, no LDAP).
- No se admite la operación de sustitución de claves.
- Se omite el paso de nuevo cifrado de la restauración del almacén.
- Modo de recuperación La herramienta también se puede ejecutar incluso cuando el acceso al servidor y a la base de datos no es posible (por ejemplo, porque la contraseña raíz en el almacén es incorrecta).

  Cuando se ejecuta en este modo, la autenticación no es posible y, por lo tanto, no se puede realizar ninguna operación con un cambio coordinado en la instalación.

  El modo de recuperación se puede usar para:

- determine qué entradas del almacén son erróneas (mediante la operación de verificación)
- sustituya la contraseña raíz incorrecta por el valor correcto. (Esto no cambia la contraseña. El usuario debe introducir la contraseña actual.)

> Si la contraseña raíz del almacén es incorrecta y la contraseña no se conoce y no hay copia de seguridad del almacén con la contraseña raíz correcta, la instalación no se puede recuperar con la herramienta SecurityAdmin. La única forma de recuperar la instalación es restablecer la contraseña de la instancia MySQL siguiendo el procedimiento documentado en https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Después de realizar el procedimiento de restablecimiento, utilice la operación de contraseña guardada correcta para introducir la nueva contraseña en el almacén.

Comandos

Comandos sin restricciones

Los comandos sin restricciones realizan cualquier cambio coordinado en la instalación (excepto los almacenes de confianza). Se pueden realizar comandos sin restricciones sin autenticación de usuario.

Comando	Descripción

backup-vault	Cree un archivo zip que contenga el almacén. La ruta relativa a los archivos del almacén coincidirá con la ruta de los almacenes en relación con la raíz de instalación. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Tenga en cuenta que se recomienda encarecidamente realizar una copia de seguridad del almacén cada vez que realice una copia de seguridad de una base de datos OnCommand Insight.
compruebe las teclas predeterminadas	Compruebe si las claves del almacén coinciden con las del almacén predeterminado utilizado en instancias anteriores a 7.3.16.
corrija la contraseña almacenada	Reemplace una contraseña (incorrecta) almacenada en el almacén con la contraseña correcta conocida por el usuario. Esto se puede utilizar cuando el almacén y la instalación no son consistentes. **Tenga en cuenta que no cambia la contraseña real en la instalación.**
	Change-trust-store-password Cambie la contraseña utilizada para un almacén de confianza y almacene la nueva contraseña en el almacén. La contraseña actual del almacén de confianza debe ser conocida.
verify-keystore	compruebe si los valores del almacén son correctos: • Para los usuarios OCI, ¿coincide el valor hash de la contraseña con el valor de la base de datos • Para los usuarios de MySQL, se puede establecer una conexión a la base de datos • para los almacenes de claves, se puede cargar el almacén de claves y leer sus claves (si las hay)
teclas de lista	listar las entradas en el almacén (sin mostrar el valor almacenado)

Comandos restringidos

La autenticación es necesaria para cualquier comando no oculto que realice cambios coordinados en la instalación:

Comando	Descripción

restaurar-almacén-backup	Reemplaza el almacén actual con el almacén incluido en el archivo de copia de seguridad del almacén especificado. Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas del almacén restaurado: • Actualice las contraseñas de usuario de comunicación OCI • Actualice las contraseñas de usuario de MySQL, incluido el root • para cada almacén de claves, si la contraseña del almacén de claves es conocida, actualice el almacén de claves con las contraseñas del almacén restaurado. Cuando se ejecuta en modo normal, también lee cada valor cifrado de la instancia, lo descifra utilizando el servicio de cifrado del almacén actual, lo vuelve a cifrar utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.
sincronizar con almacén	Realiza todas las acciones coordinadas para actualizar la instalación para que coincida con las contraseñas de usuario en el almacén restaurado: • Actualiza las contraseñas de usuario de comunicación OCI • Actualiza las contraseñas de usuario MySQL, incluido el root
change-password	Cambia la contraseña en el almacén y realiza las acciones coordinadas.
sustituir-llaves	Cree un nuevo almacén vacío (que tendrá claves diferentes a las del almacén existente). A continuación, copie las entradas del almacén actual en el nuevo almacén. A continuación, lee cada valor cifrado de la instancia, descifra el valor utilizando el servicio de cifrado del almacén actual, vuelve a cifrarlo utilizando el servicio de cifrado del almacén restaurado y almacena el valor re-cifrado.

Acciones coordinadas

Almacén del servidor

_interno	actualizar hash de contraseña para el usuario en la base de datos
adquisición	actualizar hash de contraseña para el usuario en la base de datos si el almacén de adquisición está presente, actualice también la entrada en el almacén de adquisición
dwh_internal	actualizar hash de contraseña para el usuario en la base de datos

cognos_admin	actualizar hash de contraseña para el usuario en la base de datos Si DWH y windows, actualice SANscreen/cognos/analytics/configuration/SANscreenAP.properties para establecer la propiedad cognos.admin en la contraseña.
raíz	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
inventario	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
dwh	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL Si DWH y Windows, actualice el registro de Windows para establecer las siguientes entradas relacionadas con ODBC en la nueva contraseña: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_CAPACIDAD_EFICIENCIA\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_RENDIMIENTO\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
dwususer	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
hosts	Ejecute SQL para actualizar la contraseña de usuario en la instancia de MySQL
contraseña_almacén_claves	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/server.keystore

truststore_password	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/server.trustore
contraseña_clave	vuelva a escribir el almacén de claves con la nueva contraseña: wildfly/standalone/configuration/sso.jks
cognos_archive	ninguno

Vault de adquisición

adquisición	ninguno
truststore_password	vuelva a escribir el almacén de claves con la nueva contraseña (si existe): acq/conf/cert/client.keystore

Ejecución de la Herramienta de administración de seguridad - Línea de comandos

La sintaxis para ejecutar la herramienta SA en el modo de línea de comandos es:

```
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
```

Notas:

- La opción «-i» puede no estar presente en la línea de comandos (ya que selecciona el modo interactivo).
- para las opciones «-s» y «-au»:
  - No se permite '-s' en una RAU
  - No se permite el uso de DWH
  - si ninguno de los dos está presente, entonces
    - El almacén del servidor está seleccionado en Servidor, DWH y Dual

        - El almacén de adquisición se selecciona en RAU
- Las opciones -lu y -lp se utilizan para la autenticación de usuarios.
    - Si se especifica <user> y <password> no, se solicitará al usuario la contraseña.
    - Si no se proporciona <user> y se requiere autenticación, se solicitará al usuario tanto <user> como <password>.

Comandos:

Comando	Uso
corrija la contraseña almacenada	`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 ```	teclas de lista
`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
teclas de comprobación	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	verify-keystore (servidor)
`` securityadmin [-s] [-db] -v where -v specified command ```	actualice

`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 ``
sustituir-llaves	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restaurar-almacén-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``
change-password (servidor)	`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-password para el usuario de adquisición (adquisición)	`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 para truststore-_password (adquisición)	`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.`
sincronizar con almacén (servidor)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>` `where` `-sv specified command`

Ejecución de la Herramienta de administración de seguridad - Modo interactivo

Interactivo: Menú principal

Para ejecutar la herramienta SA en modo interactivo, introduzca el siguiente comando:

```
 securityadmin -i
En un servidor o en una instalación doble, SecurityAdmin solicitará al
usuario que seleccione el servidor o la unidad de adquisición local.
```

Se han detectado nodos de servidor y unidad de adquisición. Seleccione el nodo cuya seguridad se debe volver a configurar:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

En DWH, el servidor se selecciona automáticamente. En una unidad de control remota, se seleccionará automáticamente la unidad de adquisición.

Interactive - Server: Recuperación de contraseña root

En el modo Servidor, la herramienta SecurityAdmin primero comprobará que la contraseña raíz almacenada es correcta. Si no es así, la herramienta mostrará la pantalla de recuperación de contraseña raíz.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de

seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Si pulsa ENTER, volverá al menú de recuperación.
```

Interactivo - Servidor: Contraseña correcta

La acción Corregir contraseña se utiliza para cambiar la contraseña almacenada en el almacén de forma que coincida con la contraseña real requerida por la instalación. Este comando es útil en situaciones en las que un cambio en la instalación ha sido realizado por algo distinto de la herramienta securityadmin. Entre los ejemplos se incluyen:

- La contraseña de un usuario SQL fue modificada por acceso directo a MySQL.
- Se reemplaza un almacén de claves o se cambia la contraseña de un almacén de claves mediante keytool.
- Se restauró una base de datos OCI y esa base de datos tiene contraseñas diferentes para los usuarios internos

En primer lugar, la contraseña correcta solicitará al usuario que seleccione la contraseña que desea almacenar el valor correcto.

```
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:
```

Después de seleccionar la entrada que se va a corregir, se le solicita al usuario cómo desea proporcionar el valor.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Si se selecciona la opción 1, se solicitará al usuario la contraseña correcta.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Si se introduce la contraseña correcta, se mostrará lo siguiente.
```

```
 Password verified.  Vault updated
Si pulsa ENTER, volverá al menú sin restricciones del servidor.
```

Si se introduce una contraseña incorrecta, se mostrará lo siguiente

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

Si pulsa ENTER, volverá al menú sin restricciones del servidor.

Si se selecciona la opción 2, se solicitará al usuario que proporcione el nombre de un archivo de copia de seguridad desde el que leer la contraseña correcta:

```
 Enter Backup File Location:
Si la contraseña de la copia de seguridad es correcta, se mostrará lo
siguiente.
```

```
 Password verified.  Vault updated
Al pulsar ENTER se mostrará el menú server unrestricted.
```

Si la contraseña de la copia de seguridad es incorrecta, se mostrará lo siguiente

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

Al pulsar ENTER se mostrará el menú server unrestricted.

Interactivo - Servidor: Verifique el contenido del almacén

Verifique que el contenido del almacén compruebe si el almacén tiene claves que coincidan con el almacén predeterminado distribuido con versiones anteriores de OCI y comprobará si cada valor del almacén coincide con la instalación.

Los posibles resultados para cada clave son:

DE ACUERDO	El valor del almacén es correcto

No activado	No se puede comprobar el valor con respecto a la instalación
MALO	El valor no coincide con la instalación
Ausente	Falta una entrada esperada.

```
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
```

Interactivo - Servidor: Respaldo

La copia de seguridad solicitará el directorio en el que se debe almacenar el archivo zip de copia de seguridad. El directorio ya debe existir y el nombre del archivo será ServerSecurityBackup-aaaa-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
```

Interactivo - Servidor: Inicio de sesión

La acción de inicio de sesión se utiliza para autenticar un usuario y obtener acceso a las operaciones que modifican la instalación. El usuario debe tener Privileges de administrador. Cuando se ejecuta con el servidor, se puede utilizar cualquier usuario administrador; cuando se ejecuta en modo directo, el usuario debe ser un usuario local en lugar de un usuario LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

o.

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

UserName: admin

Password:
```

Si la contraseña es correcta y el usuario es un usuario administrador, se mostrará el menú restringido.

Si la contraseña no es correcta, se mostrará lo siguiente:

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

UserName: admin

Password:

Login Failed!
```

Si el usuario no es un administrador, se mostrará lo siguiente:

```
Authenticating via server. Enter user and password

UserName: user

Password:

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

Interactivo - Servidor: Menú restringido

Una vez que el usuario inicia sesión, la herramienta muestra el menú Restringido.

```
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:
```

Interactivo - Servidor: Cambiar contraseña

La acción de cambio de contraseña se utiliza para cambiar una contraseña de instalación a un nuevo valor.

“Cambiar contraseña” primero le pedirá al usuario que seleccione la contraseña que desea cambiar.

```
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:
```

Después de seleccionar qué entrada corregir, si el usuario es un usuario de MySQL, se le preguntará al usuario si debe proteger el hash de la contraseña

```
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
```

A continuación, se solicita al usuario la nueva contraseña.

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

Password is empty - cancelling operation
```

Si se introduce una contraseña no vacía, se le solicita al usuario que confirme la contraseña.

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

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Si el cambio no se realiza correctamente, se mostrará el error o la excepción.

Interactive - Servidor: Restauración

Interactivo - Servidor: Cambie las claves de cifrado

La acción Cambiar claves de cifrado reemplazará la clave de cifrado utilizada para cifrar las entradas del almacén y reemplazará la clave de cifrado utilizada para el servicio de cifrado del almacén. Como la clave del servicio de cifrado cambia, los valores cifrados de la base de datos se volverán a cifrar; se leerán, descifrarán con la clave actual, se cifrarán con la nueva clave y se guardarán de nuevo en la base de datos.

Esta acción no está soportada en modo directo ya que el servidor proporciona la operación de nuevo cifrado para algún contenido de la base de datos.

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

Confirm (y/N): y

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

Interactivo - Servidor: Instalación corregida

La acción Fix Installation actualizará la instalación. Todas las contraseñas de instalación que se pueden cambiar a través de la herramienta securityadmin, excepto root, se establecerán en las contraseñas en el almacén.

- Se actualizarán las contraseñas de los usuarios internos de OCI.
- Las contraseñas de los usuarios MySQL, excepto root, se actualizarán.
- Se actualizarán las contraseñas de los almacenes de claves.

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

Confirm:  (y/N): y

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

La acción se detendrá en la primera actualización que no se haya realizado correctamente y mostrará el error o la excepción.

Gestión de la seguridad en el servidor de Insight

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en el servidor de Insight. La gestión de seguridad incluye cambiar contraseñas, generar claves nuevas, guardar y restaurar configuraciones de seguridad creadas o restaurar configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

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

Consulte "Securityadmin"la documentación para obtener más información.

Gestión de la seguridad en la unidad de adquisición local

La `securityadmin` La herramienta permite administrar las opciones de seguridad en el usuario de adquisición local (LAU). La gestión de seguridad incluye la gestión de claves y contraseñas, el guardado y la restauración de configuraciones de seguridad que se crean o restauran con la configuración predeterminada.

Antes de empezar

Debe tener `admin` privilegios para realizar tareas de configuración de seguridad.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

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

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en una RAU

La `securityadmin` La herramienta le permite gestionar las opciones de seguridad en Raus. Es posible que necesite realizar una copia de seguridad o restaurar una configuración de almacén, cambiar las claves de cifrado o actualizar las contraseñas de las unidades de adquisición.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

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

Un escenario para actualizar la configuración de seguridad de la LAU/RAU es actualizar la contraseña de usuario de 'adquisición' cuando la contraseña de ese usuario se haya cambiado en el servidor. La LAU y todos los raus utilizan la misma contraseña que la del usuario de 'adquisición' del servidor para comunicarse con el servidor.

El usuario de "adquisición" solo existe en el servidor de Insight. La RAU o LAU inicia sesión como ese usuario cuando se conectan al servidor.

Consulte "Herramienta securityadmin"las instrucciones para obtener más información.

Gestión de la seguridad en el almacén de datos

La `securityadmin` La herramienta le permite administrar las opciones de seguridad en el servidor del almacén de datos. La administración de seguridad incluye actualizar las contraseñas internas de los usuarios internos en el servidor DWH, crear copias de seguridad de la configuración de seguridad o restaurar las configuraciones con la configuración predeterminada.

Acerca de esta tarea

Utilice la `securityadmin` herramienta para gestionar la seguridad:

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

Consulte "Securityadmin"la documentación para obtener más información.

Cambiar contraseñas de usuario interno de OnCommand Insight

Las directivas de seguridad pueden requerir cambiar las contraseñas en el entorno OnCommand Insight. Algunas de las contraseñas de un servidor existen en un servidor diferente del entorno, lo que requiere que cambie la contraseña en ambos servidores.

Por ejemplo, al cambiar la contraseña de usuario de "'Inventory'" en Insight Server, debe coincidir con la contraseña de usuario "'Inventory'" en el conector del servidor del almacén de datos configurado para ese Insight Server.

Antes de empezar

Debe comprender las dependencias de las cuentas de usuario antes de cambiar las contraseñas. Si no se actualizan las contraseñas en todos los servidores necesarios, se generarán errores de comunicación entre los componentes de Insight.

Acerca de esta tarea

En la siguiente tabla se enumeran las contraseñas de usuario interno de Insight Server y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas de Insight Server	Cambios necesarios
_interno	
adquisición	LAU, RAU
dwh_internal	Almacén de datos
hosts	
inventario	Almacén de datos
raíz	

En la tabla siguiente se enumeran las contraseñas de usuario internas del almacén de datos y se enumeran los componentes de Insight que tienen contraseñas dependientes que coinciden con la nueva contraseña.

Contraseñas de almacén de datos	Cambios necesarios
cognos_admin	
dwh	
dwh_Internal (se cambia mediante la interfaz de usuario de configuración del conector del servidor)	Servidor de Insight
dwususer	
hosts	
Inventario (modificado con la interfaz de usuario de configuración de Server Connector)	Servidor de Insight

raíz	

Cambio de contraseñas en la interfaz de usuario de configuración de la conexión del servidor DWH

En la siguiente tabla se muestra la contraseña de usuario de la LAU y se enumeran los componentes de Insight que tienen contraseñas dependientes que deben coincidir con la nueva contraseña.

Contraseñas DE LAU	Cambios necesarios
adquisición	Insight Server, RAU

Cambio de las contraseñas “Inventory” y “dwh_Internal” mediante la interfaz de usuario de configuración de la conexión al servidor

Si necesita cambiar las contraseñas «'inventory'» o «dwh_internal» para que coincidan con las del servidor Insight, utilice la interfaz de usuario del almacén de datos.

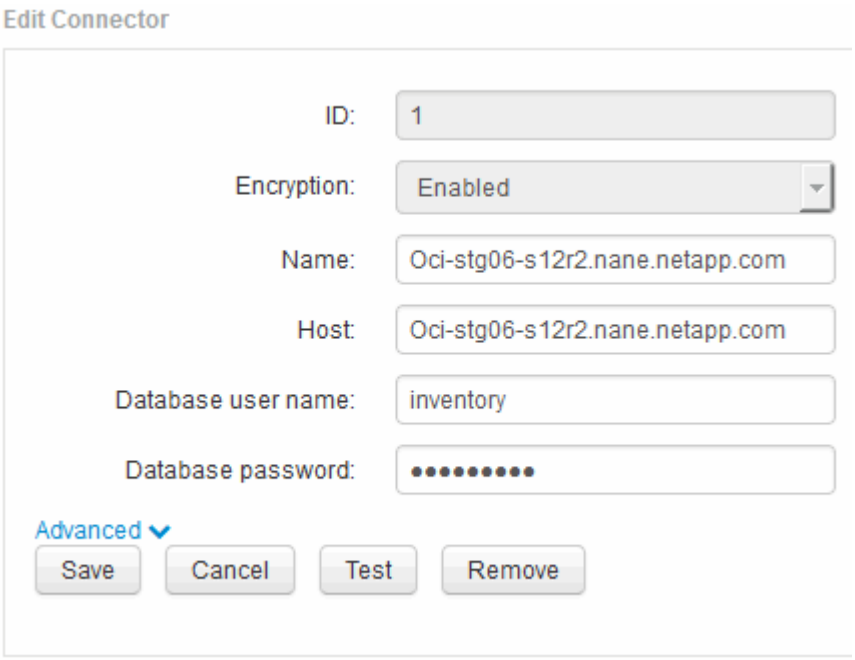
Antes de empezar

Debe iniciar sesión como administrador para realizar esta tarea.

Pasos

1. Inicie sesión en el portal del almacén de datos en https://hostname/dwh, Donde hostname es el nombre del sistema donde está instalado el almacén de datos OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

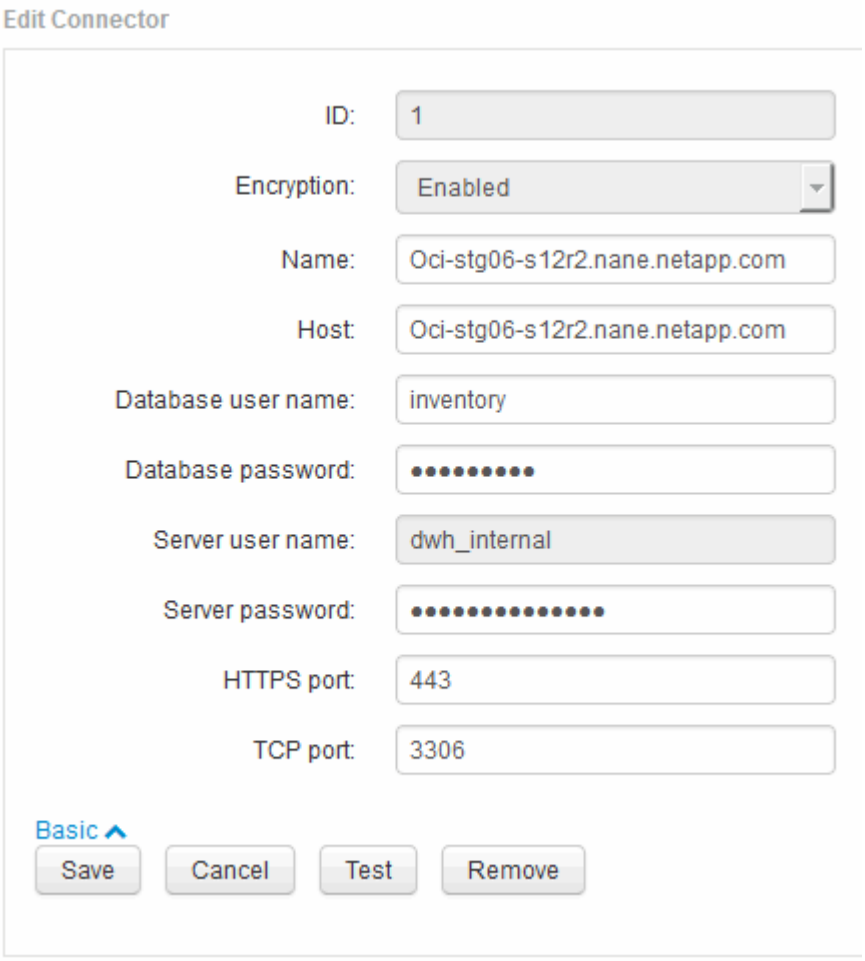
   Aparece la pantalla **Editar conector**.



3. Introduzca una nueva contraseña de "'Inventory'" para el campo **Contraseña de base de datos**.

4. Haga clic en **Guardar**
5. Para cambiar la contraseña "dwh_internal", haga clic en **Avanzado**

   Aparece la pantalla Editar conector avanzado.



6. Introduzca la nueva contraseña en el campo **Contraseña del servidor**:
7. Haga clic en Guardar.

Cambio de la contraseña dwh mediante la herramienta de administración de ODBC

Cuando se cambia la contraseña para el usuario dwh en el servidor de Insight, la contraseña también se debe cambiar en el servidor de almacén de datos. Utilice la herramienta Administrador de orígenes de datos ODBC para cambiar la contraseña en el almacén de datos.

Antes de empezar

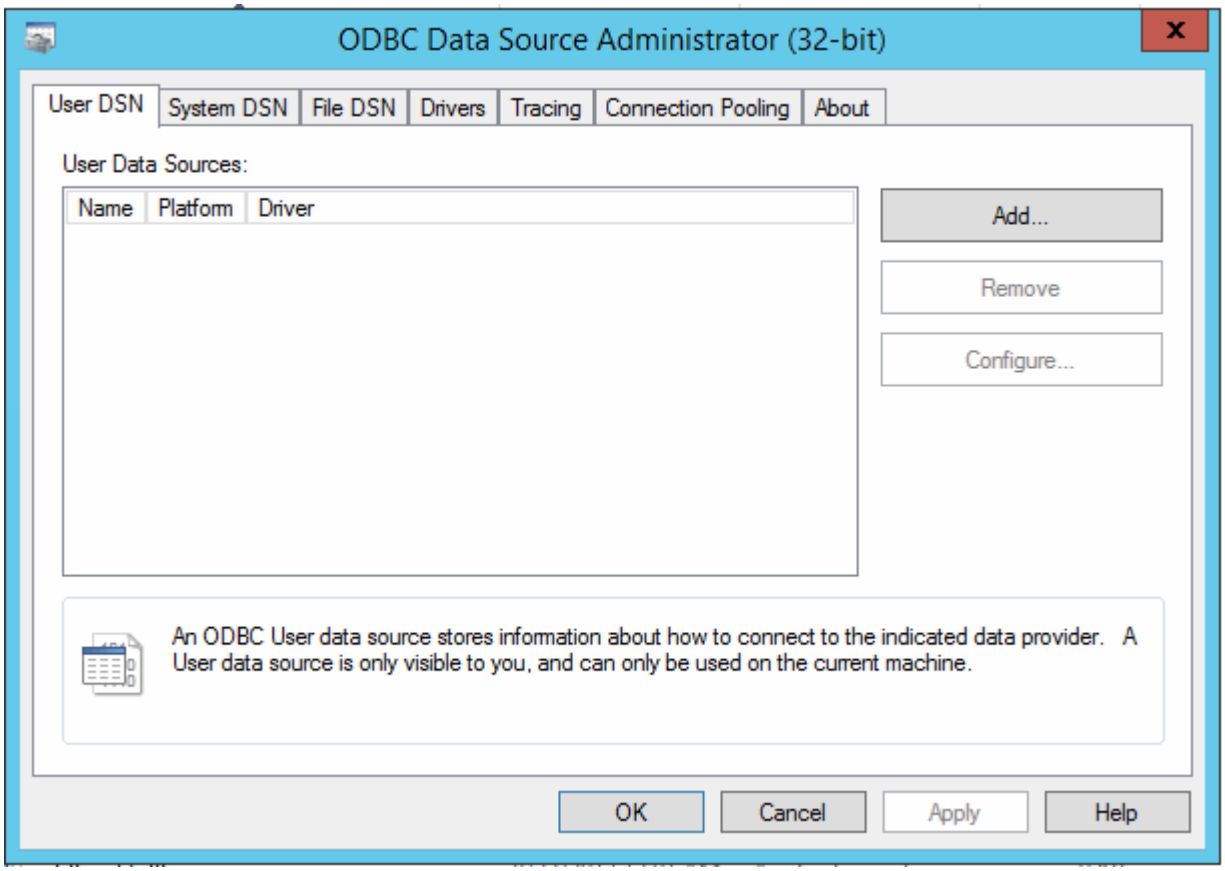
Debe realizar un inicio de sesión remoto en el servidor de almacén de datos utilizando una cuenta con privilegios de administrador.

Pasos

1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.

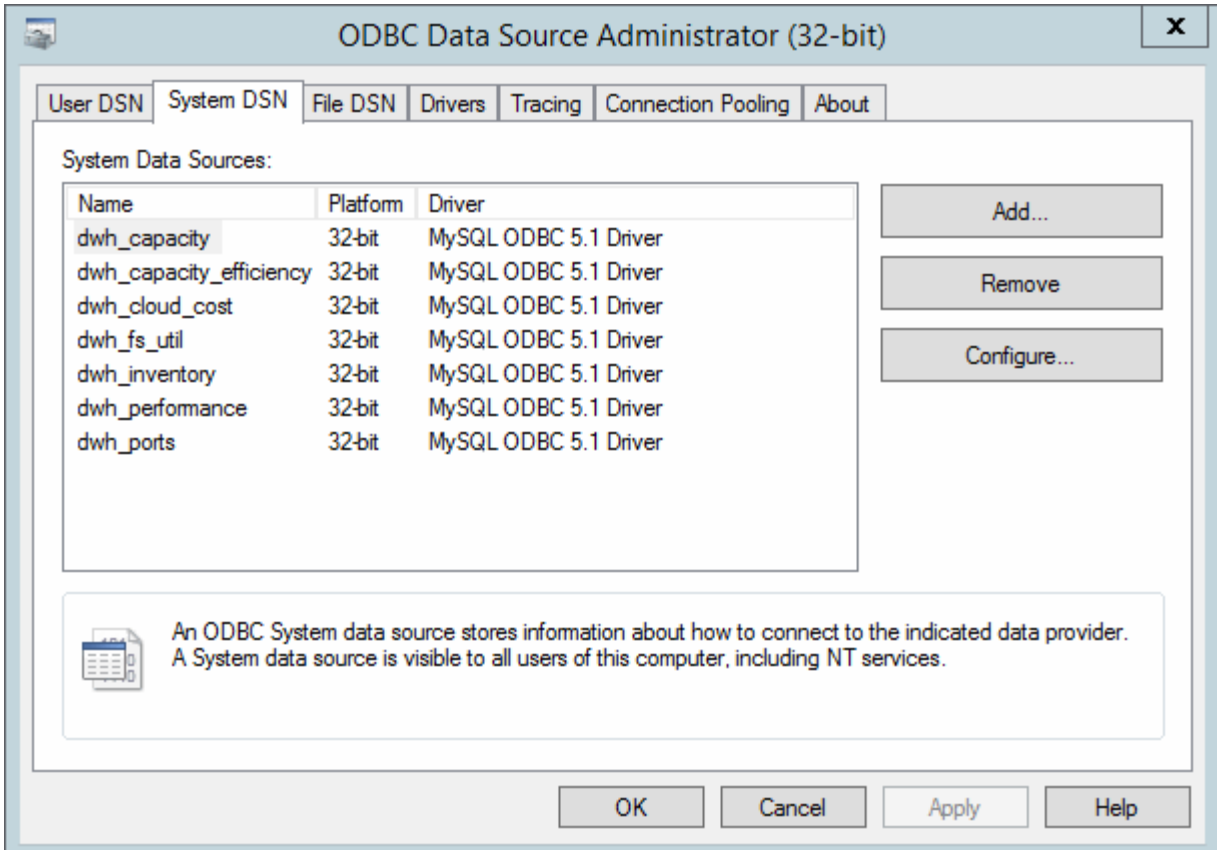
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

   El sistema muestra la pantalla del Administrador de orígenes de datos ODBC.



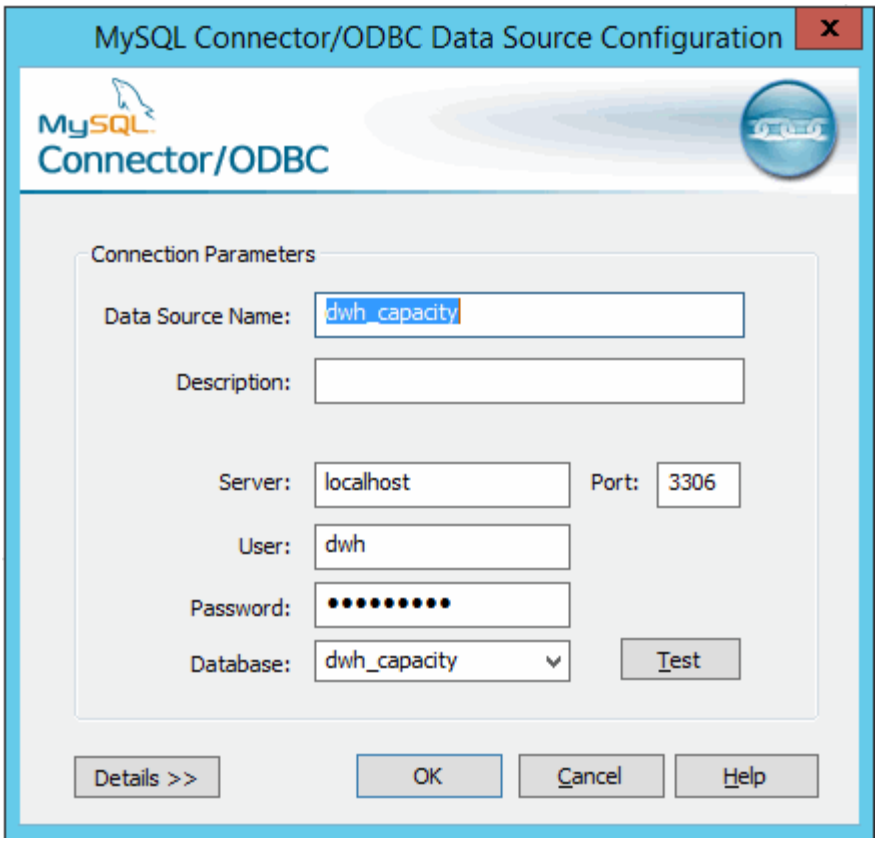
3. Haga clic en **DSN de sistema**

   Se muestran los orígenes de datos del sistema.



4. Seleccione un origen de datos OnCommand Insight de la lista.
5. Haga clic en **Configurar**

   Aparece la pantalla Configuración del origen de datos.



6. Introduzca la nueva contraseña en el campo **Contraseña**.

Información de copyright

Información de la marca comercial