# Seguridad de Insight

## OnCommand Insight

NetApp
April 01, 2024

# Tabla de contenidos

# Seguridad de Insight

La versión 7.3.1 de OnCommand Insight introdujo funciones de seguridad que permiten a los entornos de Insight funcionar con seguridad mejorada. Entre las características se incluyen mejoras en el cifrado, el hashing de contraseñas y la capacidad de cambiar contraseñas de usuario internas y pares de claves que cifran y descifran contraseñas. Puede gestionar estas funciones en todos los servidores del entorno Insight.

La instalación predeterminada de Insight incluye una configuración de seguridad donde todos los sitios del entorno comparten las mismas claves y las mismas contraseñas predeterminadas. Para proteger los datos confidenciales, NetApp recomienda cambiar las claves predeterminadas y la contraseña de usuario Acquisition después de una instalación o actualización.

Las contraseñas cifradas de origen de datos se almacenan en la base de datos de Insight Server. El servidor tiene una clave pública y cifra las contraseñas cuando un usuario las introduce en una página de configuración de origen de datos de WebUI. El servidor no tiene las claves privadas necesarias para descifrar las contraseñas de origen de datos almacenadas en la base de datos del servidor. Sólo las unidades de adquisición (LAU, RAU) tienen la clave privada de origen de datos necesaria para descifrar contraseñas de origen de datos.

## Cambio de claves de servidores

El uso de claves predeterminadas introduce una vulnerabilidad de seguridad en el entorno. De forma predeterminada, las contraseñas de origen de datos se almacenan cifradas en la base de datos de Insight. Se cifran utilizando una clave común a todas las instalaciones de Insight. En una configuración predeterminada, la base de datos de Insight que se envía a NetApp incluye contraseñas que, en teoría, NetApp podría descifrar.

## Cambiar la contraseña de usuario de adquisición

Con la contraseña de usuario predeterminada de "adquisición" se introduce una vulnerabilidad de seguridad en el entorno. Todas las unidades de adquisición utilizan el usuario "'Acquisition'" para comunicarse con el servidor. Raus con contraseñas predeterminadas puede teóricamente conectarse a cualquier servidor de Insight utilizando contraseñas predeterminadas.

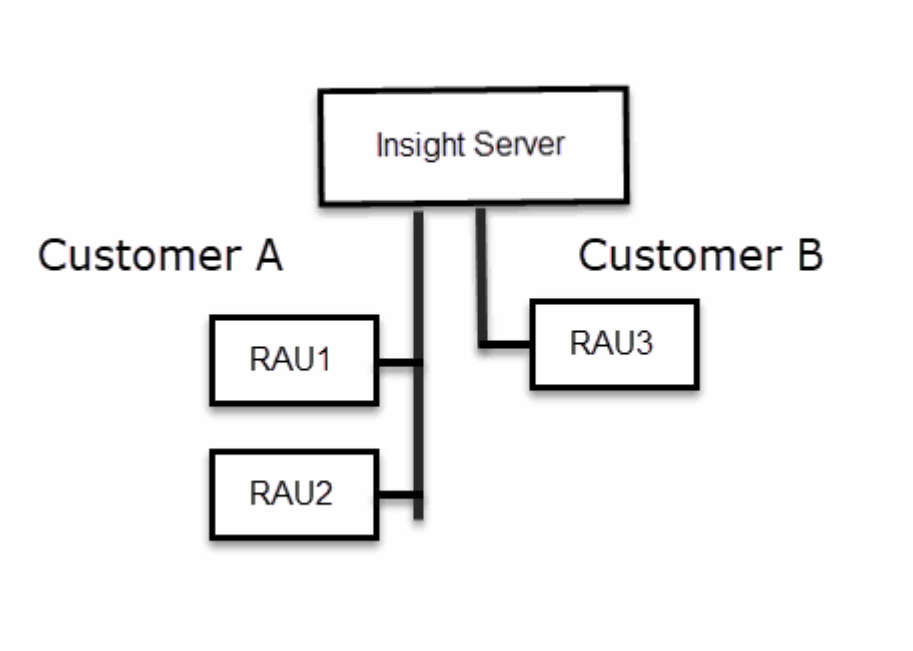
## Consideraciones sobre la actualización y la instalación

Cuando el sistema Insight contiene configuraciones de seguridad no predeterminadas (ha cambiado las contraseñas o recodificado), debe realizar una copia de seguridad de sus configuraciones de seguridad. La instalación de software nuevo o, en algunos casos, la actualización de software, revierte el sistema a una configuración de seguridad predeterminada. Cuando el sistema vuelve a la configuración predeterminada, debe restaurar la configuración no predeterminada para que el sistema funcione correctamente.

## Gestionar las claves en un entorno de proveedor de servicios complejo

Un proveedor de servicios puede alojar varios clientes de OnCommand Insight que recopilan datos. Las claves protegen los datos del cliente del acceso no autorizado por múltiples clientes en Insight Server. Los datos de cada cliente se protegen con sus pares de claves específicos.

Esta implementación de Insight se podría configurar como se muestra en la siguiente ilustración.




Debe crear claves individuales para cada cliente en esta configuración. El cliente A requiere claves idénticas para ambos raus. El cliente B requiere un único conjunto de claves.

Los pasos que debe seguir para cambiar las claves de cifrado del cliente A:

1. Realice un inicio de sesión remoto en el servidor que aloja RAU1.
2. Inicie la herramienta de administración de seguridad.
3. Seleccione Cambiar clave de cifrado para reemplazar las claves predeterminadas.
4. Seleccione copia de seguridad para crear un archivo zip de copia de seguridad de la configuración de seguridad.
5. Ejecute un inicio de sesión remoto en el servidor que aloja RAU2.
6. Copie el archivo zip de copia de seguridad de la configuración de seguridad a RAU2.
7. Inicie la herramienta de administración de seguridad.
8. Restaure la copia de seguridad de RAU1 al servidor actual.

Los pasos que debe seguir para cambiar las claves de cifrado del cliente B:

1. Inicie sesión de forma remota en el servidor que aloja RAU3.
2. Inicie la herramienta de administración de seguridad.
3. Seleccione Cambiar clave de cifrado para reemplazar las claves predeterminadas.
4. Seleccione copia de seguridad para crear un archivo zip de copia de seguridad de la configuración de seguridad.

# 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`

## Pasos

1. Inicie sesión de forma remota en Insight Server.
2. Inicie la herramienta de administración de seguridad en modo interactivo:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux: `/bin/oci-securityadmin.sh -i`

     El sistema solicita credenciales de inicio de sesión.
3. Introduzca el nombre de usuario y la contraseña de una cuenta con las credenciales "'Admin'".
4. Seleccione **servidor**.

   Están disponibles las siguientes opciones de configuración del servidor:

   - **Backup**

     Crea un archivo zip de copia de seguridad del almacén que contiene todas las contraseñas y claves y coloca el archivo en una ubicación especificada por el usuario o en las siguientes ubicaciones predeterminadas:

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

     Restaura la copia de seguridad zip del almacén que se creó. Una vez restaurada, todas las contraseñas y claves se revierten a valores existentes en el momento de la creación del backup.

     > Restore se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo: - Cambiar la clave de cifrado del servidor en un servidor - Crear una copia de seguridad del almacén - Restaurar la copia de seguridad del almacén en el segundo servidor
   - **Cambiar clave de cifrado**

     Cambie la clave de cifrado del servidor que se utiliza para cifrar o descifrar contraseñas de usuario proxy, contraseñas de usuario SMTP, contraseñas de usuario LDAP, etc.

> Al cambiar las claves de cifrado, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

- **Actualizar contraseña**

  Cambiar contraseña de las cuentas internas que usa Insight. Se muestran las siguientes opciones:

  - _interno
  - adquisición
  - cognos_admin
  - dwh_internal
  - hosts
  - inventario
  - raíz

> Algunas cuentas necesitan sincronizarse cuando se cambian las contraseñas. Por ejemplo, si cambia la contraseña del usuario de "adquisición" en el servidor, deberá cambiar la contraseña del usuario de "adquisición" en la LAU, la RAU y las DWH para que coincidan. Además, al cambiar contraseñas, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

- **Restablecer valores predeterminados**

  Restablece las claves y las contraseñas a los valores predeterminados. Los valores predeterminados son los que se proporcionan durante la instalación.

- **Salida**

  Salga de la `securityadmin` herramienta.

  a. Elija la opción que desea cambiar y siga las indicaciones.

# 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`

## Pasos

1. Inicie sesión de forma remota en Insight Server.
2. Inicie la herramienta de administración de seguridad en modo interactivo:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux: `/bin/oci-securityadmin.sh -i`

     El sistema solicita credenciales de inicio de sesión.
3. Introduzca el nombre de usuario y la contraseña de una cuenta con las credenciales "'Admin'".
4. Seleccione **Unidad de adquisición local** para volver a configurar la configuración de seguridad de la unidad de adquisición local.

   Se muestran las siguientes opciones:

   - **Backup**

     Crea un archivo zip de copia de seguridad del almacén que contiene todas las contraseñas y claves y coloca el archivo en una ubicación especificada por el usuario o en las siguientes ubicaciones predeterminadas:

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

     Restaura la copia de seguridad zip del almacén que se creó. Una vez restaurada, todas las contraseñas y claves se revierten a valores existentes en el momento de la creación del backup.

     > Restore se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo: - Cambiar claves de cifrado en la LAU - Crear una copia de seguridad del almacén - Restaurar la copia de seguridad del almacén en cada uno de los raus
   - **Cambiar claves de cifrado**

     Cambie las claves de cifrado AU utilizadas para cifrar o descifrar las contraseñas del dispositivo.

     > Al cambiar las claves de cifrado, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.
   - **Actualizar contraseña**

     Cambiar la contraseña de la cuenta de usuario de "adquisición".

> Algunas cuentas necesitan sincronizarse cuando se cambian las contraseñas. Por ejemplo, si cambia la contraseña del usuario de "adquisición" en el servidor, deberá cambiar la contraseña del usuario de "adquisición" en la LAU, la RAU y las DWH para que coincidan. Además, al cambiar contraseñas, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

- **Restablecer valores predeterminados**

  Restablece la contraseña de usuario de adquisición y las claves de cifrado de usuario de adquisición a los valores predeterminados, los valores predeterminados son los que se proporcionan durante la instalación.

- **Salida**

  Salga de la `securityadmin` herramienta.

5. Elija la opción que desea configurar y siga las instrucciones.

# 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 para la LAU, RAU es actualizar la contraseña de usuario de "adquisición" cuando se haya cambiado la contraseña para ese usuario en el servidor. Todos los raus y LAU utilizan la misma contraseña que el 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.

Siga estos pasos para administrar las opciones de seguridad en una RAU:

## Pasos

1. Realice un inicio de sesión remoto en el servidor que ejecuta la RAU
2. Inicie la herramienta de administración de seguridad en modo interactivo:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux: `/bin/oci-securityadmin.sh -i`

El sistema solicita credenciales de inicio de sesión.

3. Introduzca el nombre de usuario y la contraseña de una cuenta con las credenciales "'Admin'".

   El sistema muestra el menú de la RAU.

   - **Backup**

     Crea un archivo zip de copia de seguridad del almacén que contiene todas las contraseñas y claves y coloca el archivo en una ubicación especificada por el usuario o en las siguientes ubicaciones predeterminadas:

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

   - **Restaurar**

     Restaura la copia de seguridad zip del almacén que se creó. Una vez restaurada, todas las contraseñas y claves se revierten a valores existentes en el momento de la creación del backup.

     > Restore se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo: - Cambiar claves de cifrado en un servidor - Crear una copia de seguridad del almacén - Restaurar la copia de seguridad del almacén en el segundo servidor

   - **Cambiar claves de cifrado**

     Cambie las claves de cifrado de RAU utilizadas para cifrar o descifrar las contraseñas del dispositivo.

     > Al cambiar las claves de cifrado, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

   - **Actualizar contraseña**

     Cambiar la contraseña de la cuenta de usuario de "adquisición".

     > Algunas cuentas necesitan sincronizarse cuando se cambian las contraseñas. Por ejemplo, si cambia la contraseña del usuario de "adquisición" en el servidor, deberá cambiar la contraseña del usuario de "adquisición" en la LAU, la RAU y las DWH para que coincidan. Además, al cambiar contraseñas, debe realizar una copia de seguridad de la nueva configuración de seguridad para poder restaurarla después de una actualización o instalación.

   - **Restablecer valores predeterminados**

     Restablece los valores predeterminados de las claves de cifrado y las contraseñas. Los valores predeterminados son los que se proporcionan durante la instalación.

   - **Salida**

     Salga de la `securityadmin` herramienta.

# 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`

## Pasos

1. Inicie sesión de forma remota en el servidor del almacén de datos.
2. Inicie la herramienta de administración de seguridad en modo interactivo:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux: `/bin/oci-securityadmin.sh -i`

     El sistema solicita credenciales de inicio de sesión.
3. Introduzca el nombre de usuario y la contraseña de una cuenta con las credenciales "'Admin'".

   El sistema muestra el menú de administración de seguridad para el almacén de datos:

   - **Backup**

     Crea un archivo zip de copia de seguridad del almacén que contiene todas las contraseñas y claves y coloca el archivo en una ubicación especificada por el usuario o en la ubicación predeterminada:

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

     Restaura la copia de seguridad zip del almacén que se creó. Una vez restaurada, todas las contraseñas y claves se revierten a valores existentes en el momento de la creación del backup.

     > Restore se puede utilizar para sincronizar contraseñas y claves en varios servidores, por ejemplo: - Cambiar claves de cifrado en un servidor - Crear una copia de seguridad del almacén - Restaurar la copia de seguridad del almacén en el segundo servidor
     >
     > +

   - **Cambiar claves de cifrado**

     Cambie la clave de cifrado DWH utilizada para cifrar o descifrar contraseñas, como contraseñas de

conector y contraseñas de SMPT.

- **Actualizar contraseña**

  Cambiar la contraseña de una cuenta de usuario específica.

  - _interno
  - adquisición
  - cognos_admin
  - dwh
  - dwh_internal
  - dwususer
  - hosts
  - inventario
  - raíz

> Al cambiar las contraseñas de dwususer, hosts, inventario o root, tiene la opción de usar hash de contraseña SHA-256. Estas opciones requieren que todos los clientes que acceden a las cuentas utilicen conexiones SSL.

+

- **Restablecer valores predeterminados**

  Restablece los valores predeterminados de las claves de cifrado y las contraseñas. Los valores predeterminados son los que se proporcionan durante la instalación.

- **Salida**

  Salga de la `securityadmin` herramienta.

# 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.

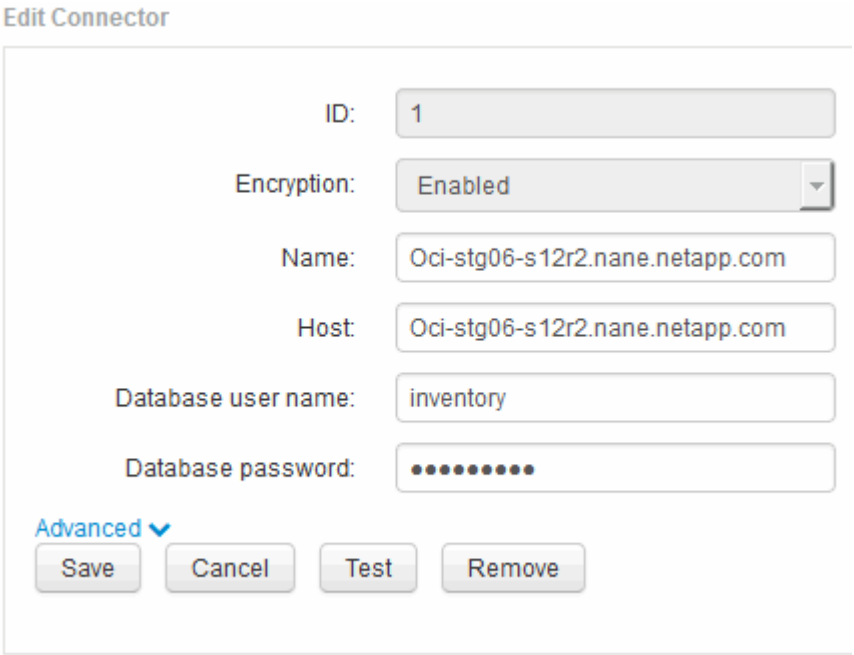
### Antes de empezar

Debe iniciar sesión como administrador para realizar esta tarea.

### Pasos

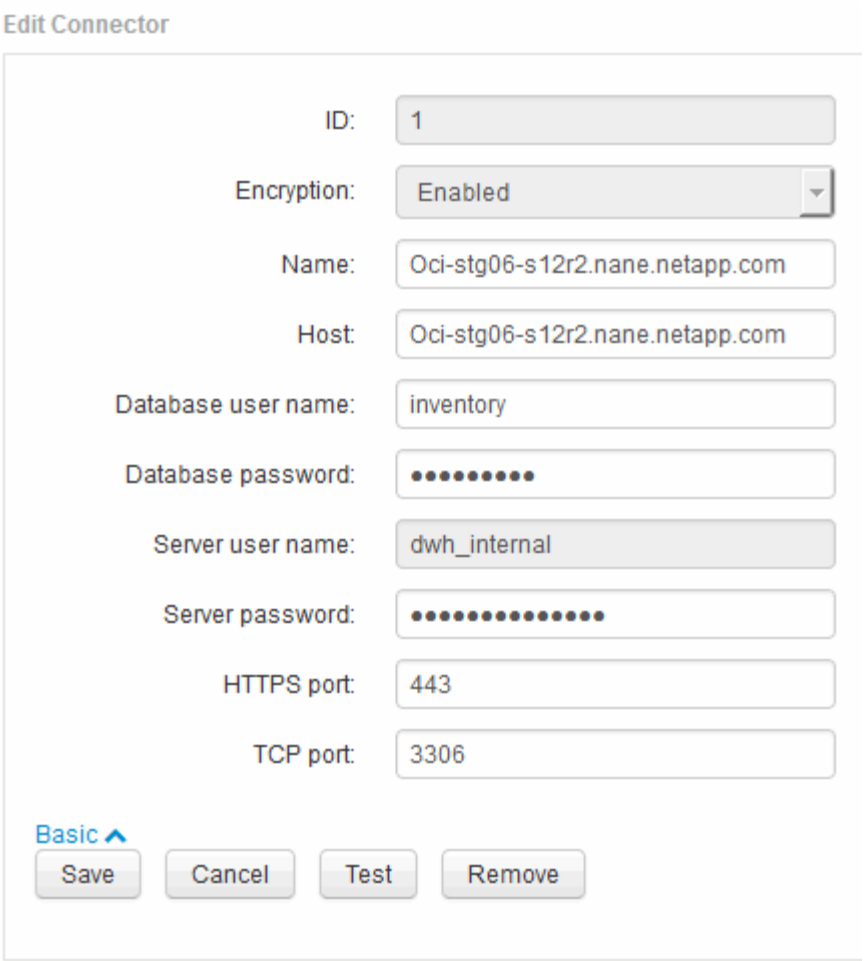
1. Inicie sesión en el portal del almacén de datos en https://hostname/dwh, Donde hostname es el nombre del sistema donde está instalado el almacén de datos OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

   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.

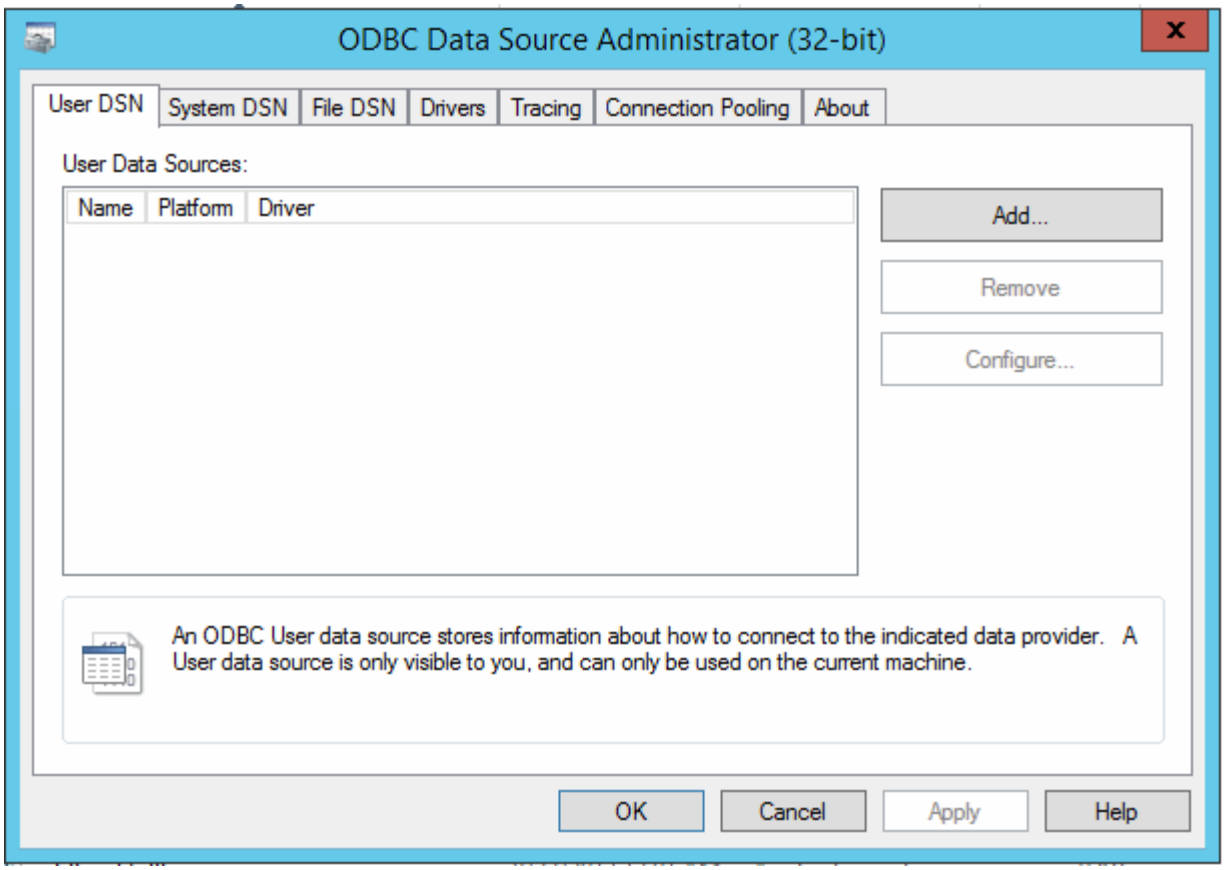
### Antes de empezar

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

### Pasos

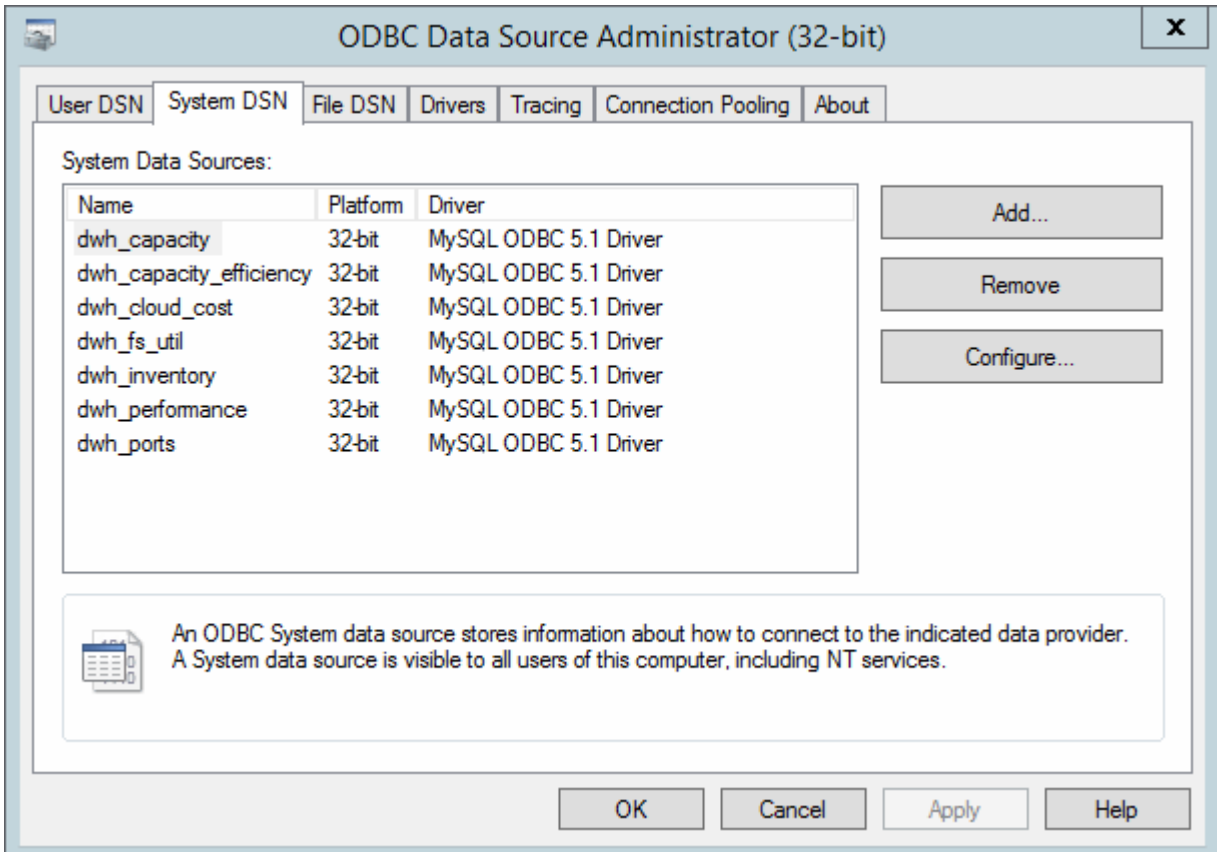
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

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



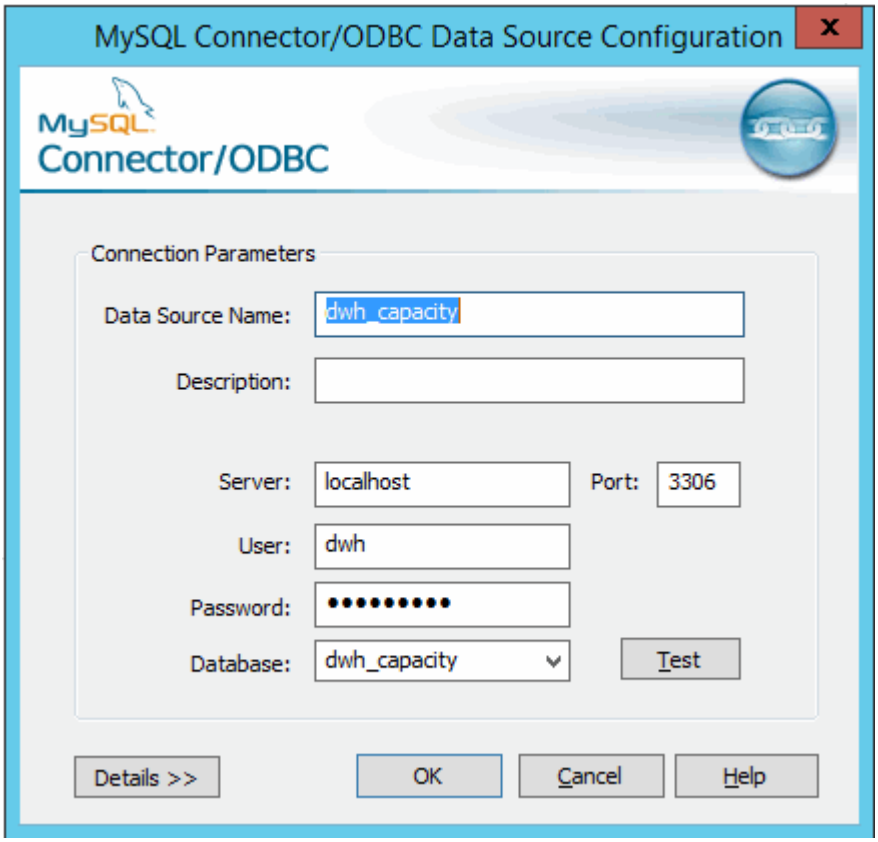

3. Haga clic en **DSN de sistema**

   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**.