



# **Configuración y administración**

## **OnCommand Insight**

NetApp  
April 01, 2024

# Tabla de contenidos

- Configuración y administración ..... 1
  - Configurar Insight ..... 1
  - Seguridad de Insight ..... 95
  - Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado ..... 109
  - Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado. .... 121
  - Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9) ..... 123
  - Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior). .... 124
  - Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9). .... 126
  - Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior). .... 128
  - Importación de certificados SSL ..... 130
  - La jerarquía de entidades de negocio ..... 133
  - Definición de anotaciones ..... 136
  - Consulta de activos ..... 151
  - Gestión de fuentes de datos de Insight ..... 159
  - Resolución del dispositivo ..... 266
  - Manteniéndose Insight ..... 285
  - Supervisión de su entorno ..... 309

# Configuración y administración

## Configurar Insight

Para configurar Insight, debe activar licencias de Insight, configurar los orígenes de datos, definir usuarios y notificaciones, habilitar backups y realizar los pasos de configuración avanzada necesarios.

Después de instalar el sistema OnCommand Insight, debe realizar las siguientes tareas de configuración:

- Instale sus licencias de Insight.
- Configure sus orígenes de datos en Insight.
- Configurar cuentas de usuario.
- Configure su correo electrónico.
- Defina sus notificaciones de SNMP, correo electrónico o syslog si es necesario.
- Habilitación de backups automáticos semanales de la base de datos de Insight.
- Realice los pasos de configuración avanzada necesarios, incluida la definición de anotaciones y umbrales.

## Acceso a la interfaz de usuario web de

Tras instalar OnCommand Insight, debe instalar sus licencias y, a continuación, configurar Insight para supervisar su entorno. Para ello, utilice un navegador web para acceder a la interfaz de usuario web de Insight.

### Pasos

1. Debe realizar una de las siguientes acciones:

- Open Insight en el servidor de Insight:

`https://fqdn`

- Abrir Insight desde cualquier otra ubicación:

`https://fqdn:port`

El número de puerto es 443 u otro puerto configurado cuando se instaló Insight Server. El número de puerto predeterminado es 443 si no se especifica en la URL.

Se muestra el cuadro de diálogo OnCommand

Insight:

2. Introduzca su nombre de usuario y contraseña y haga clic en **Login**.

Si se han instalado las licencias, se muestra la página de configuración del origen de datos.



Se agotó el tiempo de espera de una sesión en Insight Browser inactiva durante 30 minutos y se cierra la sesión automáticamente del sistema. Para mayor seguridad, se recomienda cerrar el navegador después de cerrar la sesión de Insight.

## Instalación de sus licencias de Insight

Después de recibir el archivo de licencia que contiene las claves de licencia de Insight de NetApp, podrá usar las funciones de configuración para instalar todas las licencias al mismo tiempo.

### Acerca de esta tarea

Las claves de licencia de Insight se almacenan en un `.txt` o `.lic` archivo.

### Pasos

1. Abra el archivo de licencia en un editor de texto y copie el texto.
2. Abra Insight en su navegador.
3. En la barra de herramientas Insight, haga clic en **Admin**.
4. Haga clic en **Configuración**.
5. Haga clic en la ficha **licencias**.
6. Haga clic en **Actualizar licencia**.
7. Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
8. Seleccione la operación **Actualizar (más común)**.
9. Haga clic en **Guardar**.
10. Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla **Activar el envío de información de uso a NetApp** en la sección **Enviar información de uso**. El proxy debe estar configurado y activado correctamente para el entorno.

## Después de terminar

Después de instalar las licencias, puede realizar estas tareas de configuración:

- Configurar orígenes de datos.
- Cree cuentas de usuario de OnCommand Insight.

## Licencias OnCommand Insight

OnCommand Insight funciona con licencias que permiten utilizar funciones específicas en Insight Server.

- **\* Descubra\***

Discover es la licencia básica de Insight que admite inventario. Debe tener una licencia Discover para usar OnCommand Insight y la licencia Discover debe emparejarse con, al menos, una de las licencias de Assure, Perform o Plan.

- **Asegurar**

Una licencia de Assure ofrece soporte para la funcionalidad de garantía, que incluye una política de ruta global y DE SAN, y la gestión de infracciones. Una licencia Assure también le permite ver y gestionar vulnerabilidades.

- **Realizar**

Una licencia Perform admite la supervisión del rendimiento en páginas de activos, widgets de panel, consultas, etc., así como la gestión de directivas e infracciones de rendimiento.

- **Plan**

Una licencia Plan soporta funciones de planificación, incluyendo el uso y asignación de recursos.

- **Paquete de utilización de host**

Una licencia de utilización de host admite la utilización del sistema de archivos en hosts y máquinas virtuales.

- **Creación de informes**

Una licencia de creación de informes admite autores adicionales para la creación de informes. Esta licencia requiere la licencia Plan.

Los módulos de OnCommand Insight tienen licencia por período anual o perpetuas:

- Por terabyte de capacidad supervisada para detectar, asegurar, planificar y llevar a cabo módulos
- Por número de hosts para el paquete de utilización de host
- Por número de unidades adicionales de proautores de Cognos necesarias para la creación de informes

Las claves de licencia son un conjunto de cadenas únicas que se generan para cada cliente. Puede obtener claves de licencia de su representante de OnCommand Insight.

Las licencias instaladas controlan las siguientes opciones disponibles en el software:

- **\* Descubra\***

Adquirir y gestionar inventario (Fundación)

Supervisar cambios y gestionar directivas de inventario

- **Asegurar**

Consulte y gestione las directivas e infracciones de rutas SAN

Ver y gestionar vulnerabilidades

Consulte y gestione tareas y migraciones

- **Plan**

Ver y administrar solicitudes

Ver y gestionar tareas pendientes

Ver y gestionar infracciones de reserva

Ver y gestionar infracciones de saldo de puertos

- **Realizar**

Supervise los datos de rendimiento, incluidos los datos de los widgets del panel, las páginas de activos y las consultas

Consulte y gestione las políticas de rendimiento e infracciones

En las tablas siguientes se proporcionan detalles de las funciones disponibles con y sin la licencia Perform para usuarios administradores y usuarios no administradores.

Función (administrador)	Con realizar licencia	Sin realizar licencia
Ciente más	Sí	No hay datos ni gráficos de rendimiento
Máquina virtual	Sí	No hay datos ni gráficos de rendimiento
Hipervisor	Sí	No hay datos ni gráficos de rendimiento
Host	Sí	No hay datos ni gráficos de rendimiento
Almacén de datos	Sí	No hay datos ni gráficos de rendimiento

VMDK	Sí	No hay datos ni gráficos de rendimiento
Volumen interno	Sí	No hay datos ni gráficos de rendimiento
Volumen	Sí	No hay datos ni gráficos de rendimiento
Del banco de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Disco	Sí	No hay datos ni gráficos de rendimiento
Reducida	Sí	No hay datos ni gráficos de rendimiento
Nodo de almacenamiento	Sí	No hay datos ni gráficos de rendimiento
Estructura	Sí	No hay datos ni gráficos de rendimiento
Puerto del switch	Sí	Sin datos de rendimiento ni gráficos; «'errores de puerto'» muestra «'N/A'»
Puerto de almacenamiento	Sí	Sí
Puerto NPV	Sí	No hay datos ni gráficos de rendimiento
Conmutador	Sí	No hay datos ni gráficos de rendimiento
Interruptor NPV	Sí	No hay datos ni gráficos de rendimiento
Qtrees	Sí	No hay datos ni gráficos de rendimiento
Cuota	Sí	No hay datos ni gráficos de rendimiento
Ruta	Sí	No hay datos ni gráficos de rendimiento

Zona	Sí	No hay datos ni gráficos de rendimiento
Miembro de la zona	Sí	No hay datos ni gráficos de rendimiento
Dispositivo genérico	Sí	No hay datos ni gráficos de rendimiento
Cinta	Sí	No hay datos ni gráficos de rendimiento
Enmascaramiento	Sí	No hay datos ni gráficos de rendimiento
Sesiones ISCSI	Sí	No hay datos ni gráficos de rendimiento
Portales de red ICSI	Sí	No hay datos ni gráficos de rendimiento
Búsqueda	Sí	Sí
Admin	Sí	Sí
Consola	Sí	Sí
Widgets	Sí	Parcialmente disponible (solo están disponibles los widgets de activo, consulta y administrador)
Panel de infracciones	Sí	Oculto
Panel de activos	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Gestione las políticas de rendimiento	Sí	Oculto
Gestionar anotaciones	Sí	Sí
Administrar reglas de anotación	Sí	Sí
Gestione las aplicaciones	Sí	Sí



Consultas	Sí	Sí
Administrar entidades comerciales	Sí	Sí

Función	Usuario: Con licencia Perform	Huésped - con licencia de ejecución	Usuario: Sin licencia de ejecución	Huésped - sin licencia de ejecución
Panel de activos	Sí	Sí	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)	Parcialmente disponible (los widgets de IOPS de almacenamiento y IOPS de máquina virtual están ocultos)
Consola personalizada	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)	Sólo visualización (sin opciones de creación, edición o guardado)
Gestione las políticas de rendimiento	Sí	Oculto	Oculto	Oculto
Gestionar anotaciones	Sí	Oculto	Sí	Oculto
Gestione las aplicaciones	Sí	Oculto	Sí	Oculto
Administrar entidades comerciales	Sí	Oculto	Sí	Oculto
Consultas	Sí	Ver y editar sólo (opción sin guardar)	Sí	Ver y editar sólo (opción sin guardar)

## Configurar y gestionar cuentas de usuario

Las cuentas de usuario, la autenticación de usuarios y la autorización de usuarios se pueden definir y gestionar de dos formas: En el servidor LDAP (protocolo ligero de acceso a directorios) de Microsoft Active Directory (versión 2 o 3) o en una base de datos de usuarios interna de OnCommand Insight. Disponer de una cuenta de usuario diferente para cada persona proporciona una forma de controlar los derechos de acceso, las preferencias individuales y la responsabilidad. Utilice una cuenta con privilegios de administrador para esta operación.

## Antes de empezar

Debe haber completado las siguientes tareas:

- Instale sus licencias de OnCommand Insight.
- Asigne un nombre de usuario único para cada usuario.
- Determine qué contraseñas usar.
- Asigne los roles de usuario correctos.



Las prácticas recomendadas de seguridad exigen que los administradores configuren el sistema operativo host para evitar el inicio de sesión interactivo de usuarios que no son administradores o estándar.

## Pasos

1. Abra Insight en su navegador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Seleccione la ficha **Users**.
5. Para crear un nuevo usuario, haga clic en el botón **acciones** y seleccione **Agregar usuario**.

Introduzca la dirección **Nombre**, **Contraseña**, **correo electrónico** y seleccione uno de los usuarios **roles** como Administrador, Usuario o Invitado.

6. Para cambiar la información de un usuario, seleccione el usuario en la lista y haga clic en el símbolo **Editar cuenta de usuario** situado a la derecha de la descripción del usuario.
7. Para eliminar un usuario del sistema OnCommand Insight, seleccione el usuario de la lista y haga clic en **Eliminar cuenta de usuario** a la derecha de la descripción del usuario.

## Resultados

Cuando un usuario inicia sesión en OnCommand Insight, el servidor intenta primero la autenticación a través de LDAP, si LDAP está habilitado. Si OnCommand Insight no puede localizar al usuario en el servidor LDAP, busca en la base de datos local de Insight.

## Roles de usuario Insight

A cada cuenta de usuario se le asigna uno de los tres niveles de permisos posibles.

- Guest le permite iniciar sesión en Insight y ver las distintas páginas.
- El usuario permite todos los privilegios a nivel de invitado, así como el acceso a las operaciones de Insight, como la definición de políticas y la identificación de dispositivos genéricos. El tipo de cuenta de usuario no le permite realizar operaciones de origen de datos ni agregar o editar cuentas de usuario distintas de las suyas.
- El administrador le permite realizar cualquier operación, incluida la adición de nuevos usuarios y la administración de orígenes de datos.

**Mejor práctica:** Limite el número de usuarios con permisos de Administrador creando la mayoría de cuentas para usuarios o invitados.

## Configurar Insight para LDAP

OnCommand Insight debe configurarse con opciones de protocolo ligero de acceso a directorios (LDAP) a medida que se configuran en el dominio LDAP de su empresa.

Antes de configurar Insight para su uso con LDAP o LDAP seguro (LDAPS), tome nota de la configuración de Active Directory en el entorno de su empresa. Los ajustes de Insight deben coincidir con los de la configuración de dominio LDAP de su organización. Revise los siguientes conceptos antes de configurar Insight para su uso con LDAP y consulte al administrador de dominio LDAP para ver los atributos adecuados que debe utilizar en su entorno.

Para todos los usuarios de Secure Active Directory (es decir, LDAPS), debe usar el nombre del servidor AD exactamente como se define en el certificado. No se puede utilizar la dirección IP para un inicio de sesión seguro de AD.



OnCommand Insight admite LDAP y LDAPS mediante el servidor de Microsoft Active Directory o Azure AD. Pueden funcionar implementaciones de LDAP adicionales pero no han sido aprobadas con Insight. Los procedimientos de estas guías suponen que está utilizando Microsoft Active Directory versión 2 o 3 LDAP (protocolo ligero de acceso a directorios).

### Nombre principal del usuario atributo:

El atributo Nombre principal de usuario LDAP (userPrincipalName) es lo que Insight utiliza como atributo de nombre de usuario. El nombre principal del usuario está garantizado para ser globalmente único en un bosque de Active Directory (AD), pero en muchas grandes organizaciones, el nombre principal del usuario puede no ser inmediatamente obvio o conocido por ellos. La organización puede utilizar una alternativa al atributo Nombre principal de usuario para el nombre de usuario principal.

A continuación se muestran algunos valores alternativos para el campo Nombre principal de usuario:

- **SAMAccountName**

Este atributo de usuario es el nombre de usuario anterior a Windows 2000 NT heredado - esto es lo que la mayoría de los usuarios están acostumbrados a iniciar sesión en su equipo personal de Windows. No se garantiza que esto sea único a nivel global en todo un bosque AD.



SAMAccountName distingue entre mayúsculas y minúsculas para el atributo Nombre principal del usuario.

- **correo**

En entornos AD con MS Exchange, este atributo es la dirección de correo electrónico principal para el usuario final. Esto debe ser globalmente único en un bosque AD, (y también familiar para los usuarios finales), a diferencia de su atributo userPrincipalName. El atributo de correo no existirá en la mayoría de los entornos que no son de MS Exchange.

- **referencia**

Una referencia LDAP es la forma de un controlador de dominio de indicar a una aplicación cliente que no tiene una copia de un objeto solicitado (o, más precisamente, que no contiene la sección del árbol de directorios donde sería ese objeto, si de hecho existe) y dar al cliente una ubicación que es más probable que contenga el objeto. A su vez, el cliente utiliza la referencia como base para una búsqueda DNS de un controlador de dominio. Lo ideal es que las referencias siempre hagan referencia a un controlador de dominio que, de hecho, contiene el objeto. Sin embargo, es posible que el controlador de dominio al que

se hace referencia genere otra referencia, aunque normalmente no toma mucho tiempo descubrir que el objeto no existe e informar al cliente.



Por lo general, se prefiere sAMAccountName más que el nombre principal del usuario. sAMAccountName es único en el dominio (aunque puede que no sea único en el bosque de dominio), pero es la cadena que los usuarios utilizan normalmente para iniciar sesión (por ejemplo, *netapp\username*). el nombre distintivo es el nombre único del bosque, pero generalmente no lo conocen los usuarios.



En la parte del sistema Windows del mismo dominio, siempre puede abrir un símbolo del sistema y escribir SET para encontrar el nombre de dominio adecuado (USERDOMAIN=). A continuación, el nombre de inicio de sesión de OCI USERDOMAIN\sAMAccountName.

Para el nombre de dominio **mydomain.x.y.z.com**, utilice DC=x, DC=y, DC=z, DC=com En el campo dominio de Insight.

### Puertos:

El puerto predeterminado para LDAP es 389, y el puerto predeterminado para LDAPS es 636

URL típica de LDAPS: `ldaps://<ldap_server_host_name>:636`

Los registros están en: `\\<install_directory>\SANscreen\wildfly\standalone\log\ldap.log`

De forma predeterminada, Insight espera los valores indicados en los siguientes campos. Si estos cambios se han producido en su entorno de Active Directory, asegúrese de modificarlos en la configuración de Insight LDAP.

Atributo de rol
Miembro de
Atributo de correo
correo
Atributo Nombre distintivo
DistinguishedName
Referencia
sigla

### Grupos:

Para autenticar usuarios con diferentes funciones de acceso en los servidores OnCommand Insight y DWH, debe crear grupos en Active Directory e introducir esos nombres de grupo en los servidores OnCommand Insight y DWH. Los siguientes nombres de grupo sólo son ejemplos; los nombres configurados para LDAP en

Insight deben coincidir con los configurados para su entorno de Active Directory.

Grupo de Insight	Ejemplo
Grupo de administradores de Insight Server	insight.server.admins
Grupo de administradores de Insight	insight.admins
Grupo de usuarios de Insight	insight.users
Grupo de invitados de Insight	insight.invitados
Grupo de administradores de informes	insight.report.admins
Grupo de autores profesionales de informes	insight.report.proauthors
Grupo de autores de informes	insight.report.business.authors
Grupo de consumidores de informes	insight.report.business.consuss
Grupo de destinatarios de informes	insight.report.recipients

#### Configurar definiciones de usuario con LDAP

Para configurar OnCommand Insight (OCI) para la autenticación y la autorización de usuarios desde un servidor LDAP, debe estar definido en el servidor LDAP como administrador de servidor OnCommand Insight.

#### Antes de empezar

Debe conocer los atributos de usuario y grupo que se han configurado para Insight en el dominio LDAP.

Para todos los usuarios de Secure Active Directory (es decir, LDAPS), debe usar el nombre del servidor AD exactamente como se define en el certificado. No se puede utilizar la dirección IP para un inicio de sesión seguro de AD.

#### Acerca de esta tarea

OnCommand Insight admite LDAP y LDAPS mediante el servidor de Microsoft Active Directory. Pueden funcionar implementaciones de LDAP adicionales pero no han sido aprobadas con Insight. Este procedimiento supone que está utilizando Microsoft Active Directory versión 2 o 3 LDAP (protocolo ligero de acceso a directorios).

Los usuarios LDAP se muestran junto con los usuarios definidos localmente en la lista **Admin > MENU:Setup[Users]**.

#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

2. Haga clic en **Configuración**.
3. Haga clic en la ficha **usuarios**.
4. Desplácese a la sección LDAP, tal como se muestra aquí.

#### LDAP

LDAP integration enables authentication of users via LDAP (or ActiveDirectory). This is done by assigning these users to LDAP groups. The groups are used to identify the user permissions.

☒ Enable LDAP

Please provide credentials for a user authorized for directory lookup queries.

LDAP servers:

User:

Password:

[Show more](#) ▼

5. Haga clic en **Activar LDAP** para permitir la autenticación y autorización de usuarios LDAP.
6. Rellene los campos:

- LDAP servers: Insight acepta una lista separada por comas de direcciones URL LDAP. Insight intenta conectarse a las URL proporcionadas sin validar para el protocolo LDAP.



Para importar los certificados LDAP, haga clic en **certificados** e importe automáticamente o busque manualmente los archivos de certificado.

La dirección IP o el nombre DNS que se utilizan para identificar el servidor LDAP se suelen introducir en este formato:

```
ldap://<ldap-server-address>:port
```

o bien, si se utiliza el puerto predeterminado:

```
ldap://<ldap-server-address>
```

+ Al introducir varios servidores LDAP en este campo, asegúrese de que se utiliza el número de puerto correcto en cada entrada.

- User name: Especifique las credenciales de un usuario autorizado para las consultas de búsqueda de directorios en los servidores LDAP.
- Password: Introduzca la contraseña del usuario anterior. Para confirmar esta contraseña en el servidor LDAP, haga clic en **Validar**.

7. Si desea definir este usuario LDAP con mayor precisión, haga clic en **Mostrar más** y rellene los campos de los atributos enumerados.

Esta configuración debe coincidir con los atributos configurados en el dominio LDAP. Consulte al administrador de Active Directory si no está seguro de los valores que se deben introducir para estos campos.

- **Grupo de administradores**

Grupo LDAP para usuarios con privilegios de administrador de Insight. El valor predeterminado es `insight.admins`.

- **Grupo de usuarios**

Grupo LDAP para usuarios con privilegios de Insight User. El valor predeterminado es `insight.users`.

- **Grupo de invitados**

Grupo LDAP para usuarios con privilegios de Insight Guest. El valor predeterminado es `insight.guests`.

- **Grupo de administradores del servidor**

Grupo LDAP para usuarios con privilegios de administrador de Insight Server. El valor predeterminado es `insight.server.admins`.

- **Tiempo de espera**

Tiempo de espera de una respuesta del servidor LDAP antes de que se agote el tiempo de espera, en milisegundos. el valor predeterminado es 2,000, que es adecuado en todos los casos y no debe modificarse.

- **Dominio**

Nodo LDAP donde OnCommand Insight debería empezar a buscar el usuario LDAP. Normalmente, este es el dominio de nivel superior de la organización. Por ejemplo:

```
DC=<enterprise>,DC=com
```

- **Nombre principal de usuario atributo**

Atributo que identifica a cada usuario en el servidor LDAP. El valor predeterminado es `userPrincipalName`, que es único globalmente. OnCommand Insight intenta hacer coincidir el contenido de este atributo con el nombre de usuario que se ha proporcionado anteriormente.

- **Atributo de función**

Atributo LDAP que identifica la adecuación del usuario dentro del grupo especificado. El valor predeterminado es `memberOf`.

- **Atributo de correo**

Atributo LDAP que identifica la dirección de correo electrónico del usuario. El valor predeterminado es `mail`. Esto resulta útil si desea suscribirse a los informes disponibles en OnCommand Insight. Insight recoge la dirección de correo electrónico del usuario la primera vez que cada usuario inicia sesión y no

la busca después.



Si la dirección de correo electrónico del usuario cambia en el servidor LDAP, asegúrese de actualizarla en Insight.

- **Atributo de nombre completo**

Atributo LDAP que identifica el nombre distintivo del usuario. el valor predeterminado es `distinguishedName`.

8. Haga clic en **Guardar**.

## **Cambio de contraseñas de usuario**

Un usuario con privilegios de administrador puede cambiar la contraseña de cualquier cuenta de usuario de OnCommand Insight definida en el servidor local.

### **Antes de empezar**

Deben haberse completado los siguientes elementos:

- Notificaciones a cualquier persona que inicie sesión en la cuenta de usuario que esté modificando.
- Nueva contraseña que se utilizará después de este cambio.

### **Acerca de esta tarea**

Cuando se usa este método, no es posible cambiar la contraseña de un usuario que se valida mediante LDAP.

### **Pasos**

1. Inicie sesión con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea modificar.
6. A la derecha de la información del usuario, haga clic en **Editar cuenta de usuario**.
7. Introduzca la nueva **Contraseña** y, a continuación, vuelva a introducirla en el campo de verificación.
8. Haga clic en **Guardar**.

## **Edición de una definición de usuario**

Un usuario con privilegios de administrador puede editar una cuenta de usuario para cambiar la dirección de correo electrónico o las funciones de OnCommand Insight o DWH y las funciones de generación de informes.

### **Antes de empezar**

Determine el tipo de cuenta de usuario (OnCommand Insight, DWH o una combinación) que se debe cambiar.



## Acerca de esta tarea

Para los usuarios LDAP, sólo puede modificar la dirección de correo electrónico mediante este método.

### Pasos

1. Inicie sesión con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea modificar.
6. A la derecha de la información del usuario, haga clic en el icono **Editar cuenta de usuario**.
7. Realice los cambios necesarios.
8. Haga clic en **Guardar**.

### Eliminar una cuenta de usuario

Cualquier usuario con privilegios de administrador puede eliminar una cuenta de usuario, ya sea cuando ya no se utiliza (para una definición de usuario local) o para forzar a OnCommand Insight a volver a detectar la información de usuario la próxima vez que inicie sesión (para un usuario LDAP).

### Pasos

1. Inicie sesión en OnCommand Insight con privilegios de administrador.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **Configuración**.
4. Haga clic en la ficha **usuarios**.
5. Busque la fila que muestra la cuenta de usuario que desea eliminar.
6. A la derecha de la información del usuario, haga clic en el icono **Eliminar cuenta de usuario "x"**.
7. Haga clic en **Guardar**.

## Configuración de un mensaje de advertencia de inicio de sesión

OnCommand Insight permite a los administradores establecer un mensaje de texto personalizado que se muestra cuando los usuarios inician sesión.

### Pasos

1. Para establecer el mensaje en el servidor OnCommand Insight:
  - a. Vaya al menú: Admin[solución de problemas > solución avanzada de problemas > Configuración avanzada].
  - b. Introduzca su mensaje de inicio de sesión en el área de texto.
  - c. Haga clic en la casilla de verificación **Cliente muestra el mensaje de advertencia de inicio de sesión**.

- d. Haga clic en **Guardar**.

El mensaje aparecerá al iniciar sesión para todos los usuarios.

2. Para configurar el mensaje en el almacén de datos (DWH) y en Informes (Cognos):
  - a. Vaya a **Información del sistema** y haga clic en la ficha **Advertencia de inicio de sesión**.
  - b. Introduzca su mensaje de inicio de sesión en el área de texto.
  - c. Haga clic en **Guardar**.

El mensaje aparecerá cuando DWH y Cognos Reporting inicien sesión para todos los usuarios.

## 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

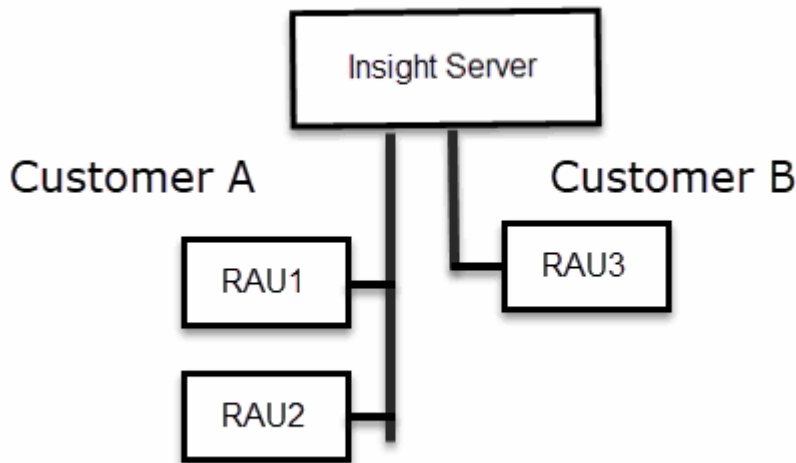
Cuando el sistema Insight contiene configuraciones de seguridad no predeterminadas (ha cambiado las contraseñas o recodificado), debe realizar una copia de seguridad de sus configuraciones de seguridad. La instalación de software nuevo o, en algunos casos, la actualización de software, revierte el sistema 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 SMTP.

#### ◦ 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
dwuser	
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**.

**Edit Connector**

ID: 1

Encryption: Enabled

Name: Oci-stg06-s12r2.nane.netapp.com

Host: Oci-stg06-s12r2.nane.netapp.com

Database user name: inventory

Database password: .....

[Advanced](#) ▼

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.

#### Edit Connector

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

Basic ^

6. 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.

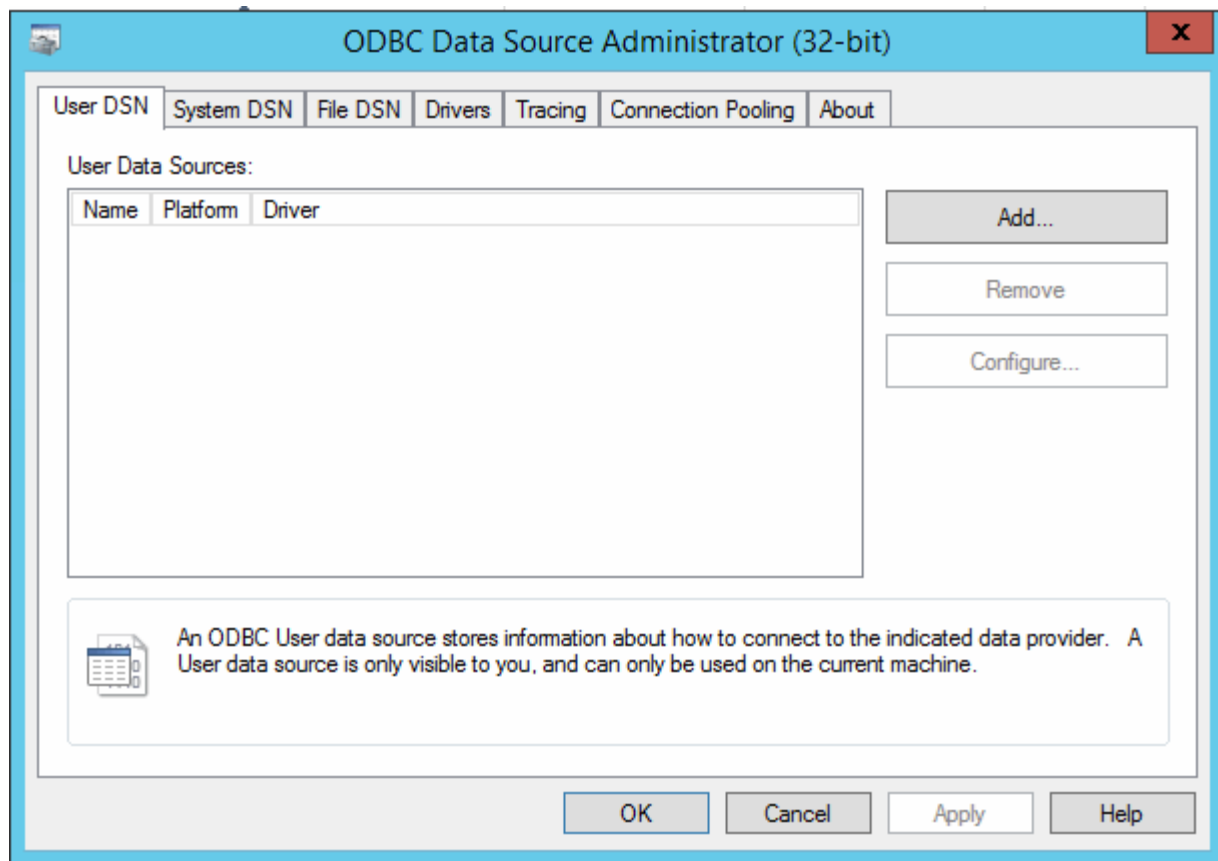
#### Antes de empezar

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

#### Pasos

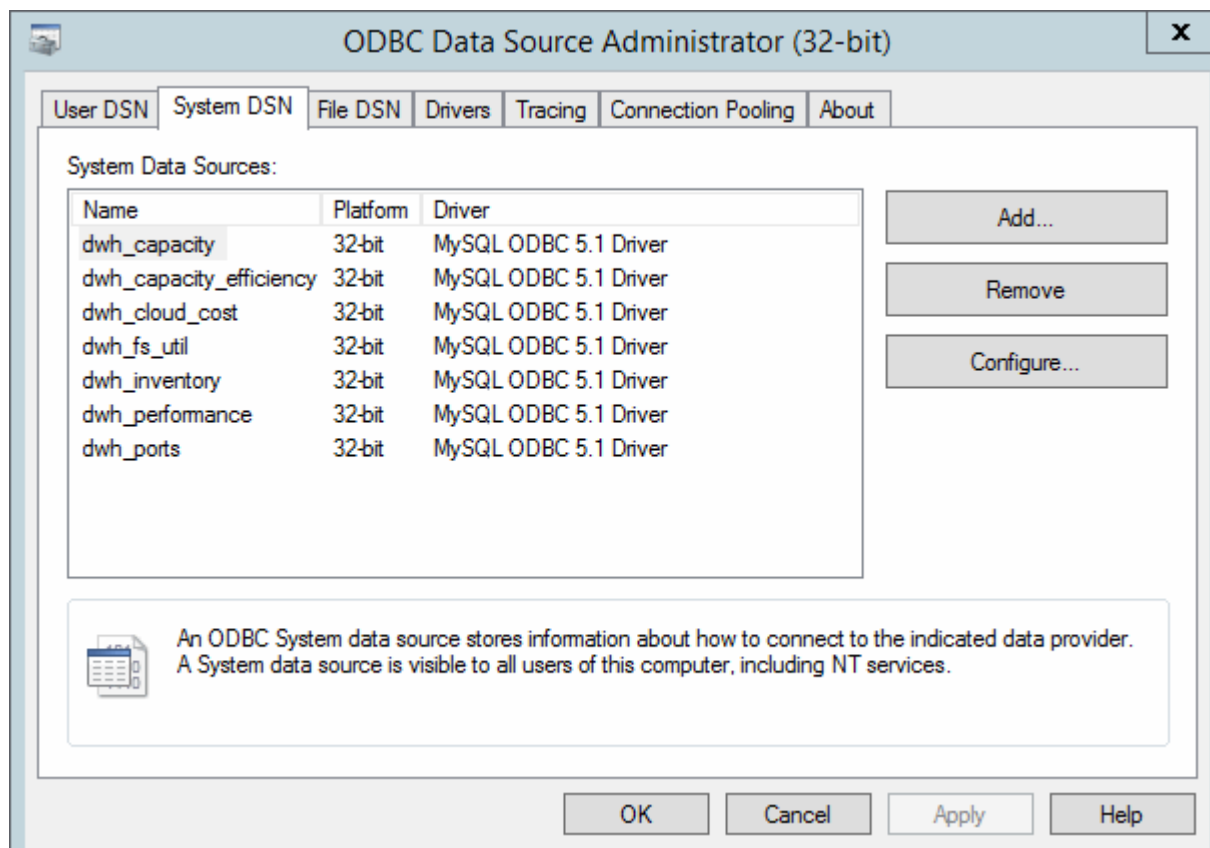
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

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



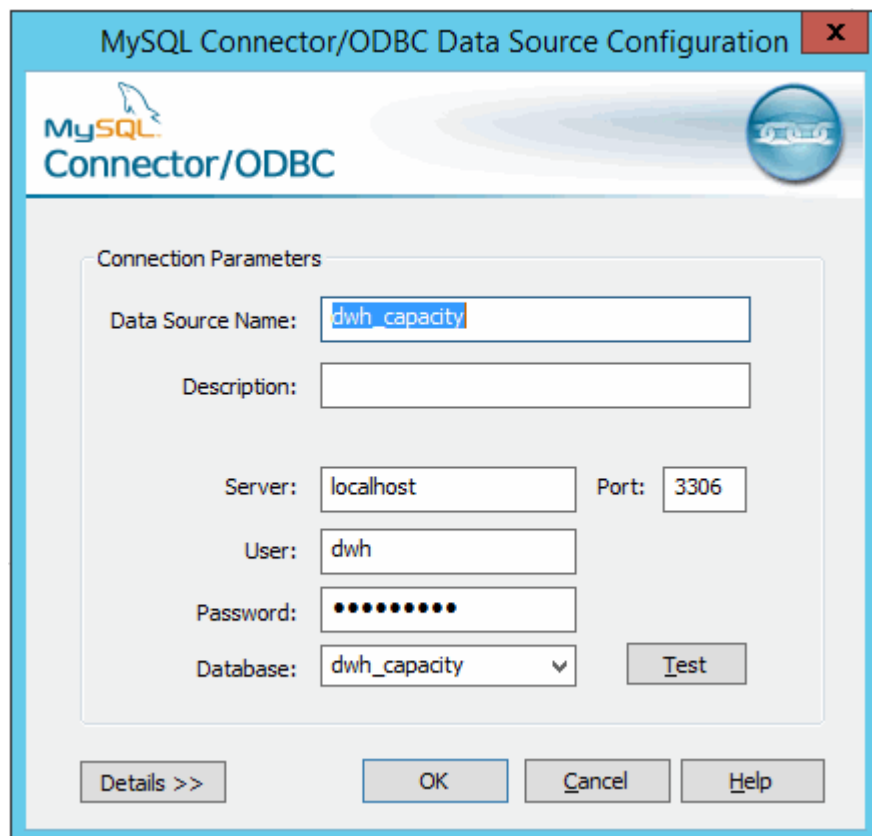
### 3. Haga clic en **DSN de sistema**

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**.

## Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight admite el uso de tarjetas inteligentes (CAC) y certificados para autenticar a los usuarios que inician sesión en los servidores de Insight. Debe configurar el sistema para habilitar estas funciones.

Después de configurar el sistema para que admita CAC y certificados, desplazarse a una nueva sesión de OnCommand Insight da como resultado que el explorador muestre un cuadro de diálogo nativo, proporcionando al usuario una lista de certificados personales entre los que elegir. Estos certificados se filtran en función del conjunto de certificados personales emitidos por entidades emisoras de certificados de confianza del servidor OnCommand Insight. La mayoría de las veces, existe una única opción. De forma predeterminada, Internet Explorer omite este cuadro de diálogo si sólo hay una opción.



Para los usuarios de CAC, las tarjetas inteligentes contienen varios certificados, sólo uno de los cuales puede coincidir con la CA de confianza. El certificado CAC para *identification* debe utilizarse.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado

Debe realizar modificaciones en la configuración del host de OnCommand Insight para admitir la tarjeta inteligente (CAC) y los inicios de sesión de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el ID de un usuario.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Pasos

1. Utilice la regedit utilidad para modificar los valores del registro en  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java:
  - a. Cambie la JVM\_OPTION DclientAuth=false para DclientAuth=true.



2. Realice una copia de seguridad del archivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra un símbolo del sistema especificando `Run as administrator`
4. Elimine el certificado autofirmado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Genere un nuevo certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Genere una solicitud de firma de certificación (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Una vez que se devuelva la CSR en el paso 6, importe el certificado y exporte el certificado en formato base-64 y colóquelo `"C:\temp" named servername.cer`.
8. Extraiga el certificado del almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extraiga una clave privada del archivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Fusione el certificado base-64 exportado en el paso 7 con la clave privada: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importe el certificado combinado al almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importe el certificado raíz: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importe el certificado raíz al servidor: `truestore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Importe el certificado intermedio: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

Repita este paso con todos los certificados intermedios.

15. Especifique el dominio en LDAP para que coincida con este ejemplo.

16. Reinicie el servidor.

### Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado

Las máquinas cliente requieren middleware y modificaciones a los exploradores para permitir el uso de tarjetas inteligentes y para el inicio de sesión de certificados. Los clientes que ya utilizan tarjetas inteligentes no deben requerir modificaciones adicionales en sus equipos cliente.

#### Antes de empezar



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

#### Acerca de esta tarea

A continuación se enumeran los requisitos comunes de configuración del cliente:

- Instalación de Smart Card middleware, como ActivClient (consulte
- Modificación del explorador de IE (consulte
- Modificación del navegador Firefox (consulte

### Activación de CAC en un servidor Linux

Se necesitan algunas modificaciones para habilitar CAC en un servidor OnCommand Insight de Linux.

#### Pasos

1. Vaya a. `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` y cambie el valor de `CLIENT_AUTH_ENABLED` a "Verdadero"
3. Importe el «'certificado raíz» que existe en  
`/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Reinicie el servidor

## Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Pasos

#### 1. Utilice regedit para modificar los valores del Registro en

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

- a. Cambie la `JVM_OPTION -DclientAuth=false` para `-DclientAuth=true`.

Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

#### 2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

- a. En una ventana de comandos, vaya a `.\SANscreen\wildfly\standalone\configuration`.
- b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

La primera palabra de cada línea indica el alias de CA.

- c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para

incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a.

..\SANscreen\wildfly\standalone\configuration y utilice la keytool comando de importación: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my\_alias -file 'path/to/my.pem' -v -trustcacerts

Mi\_alias es normalmente un alias que fácilmente identificaría la CA enkeytool -list funcionamiento.

3. En el servidor OnCommand Insight, el wildfly/standalone/configuration/standalone-full.xml El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en /subsystem=undertow/server=default-server/https-listener=default-httpsPara activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB .bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

### **Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9)**

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

#### **Antes de empezar**

Este procedimiento es para sistemas que ejecuten OnCommand Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

La primera palabra de cada línea indica el alias de CA.

c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.

d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

g. Responda `yes` cuando se le solicite que confíe en el certificado.

2. Para activar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. Para desactivar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

## Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

### 1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

#### a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

#### b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass`

```
NoPassWordSet
```

La primera palabra de cada línea indica el alias de CA.

#### c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.

#### d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

#### e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

#### f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

#### g. Responda `yes` cuando se le solicite que confíe en el certificado.

### 2. Para activar el modo CAC, realizar lo siguiente:

#### a. Configure la página salir de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, `cognos_admin`)

- (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
- (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

3. Para desactivar el modo CAC, realizar lo siguiente:

a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos\_admin)
- Haga clic en Administrar -> Configuración -> sistema -> Seguridad
- Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

### Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

#### Antes de empezar

Este procedimiento se aplica a sistemas que ejecutan OnCommny Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

#### Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

## Pasos

1. Cree un backup de `..\SANSscreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANSscreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Envíe el `encryptRequest.csr` a la entidad de certificación (CA) para obtener un certificado SSL.

Asegúrese de agregar atributos adicionales como "TAN:dns=FQDN (por ejemplo, hostname.netapp.com)" para agregar SubjectAltName. Google Chrome versión 58 y posteriores se queja si falta SubjectAltName en el certificado.

6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 al 8 c para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `Intermediate.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `root.cer` con el Bloc de notas y guarde el contenido de 9a.
  - c. Guarde el archivo como `CA.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer`

Esto establecerá `CA.cer` como entidad emisora de certificados raíz.
  - c. `ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`



Esto establecerá Cognos.cer como certificado de cifrado firmado por CA.cer.

11. Abra la configuración de IBM Cognos.
  - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
  - b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -exportcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\cognos\analítica\Configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoWordSet -alias cifrado
13. Importe "c:\temp\cognos.crt" en dwh truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -importcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\wiland\autónoma\Configuration\Server.trustore" -storeprechrit -alias cognoscert
14. Reinicie el servicio SANscreen.
15. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

### Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

#### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

#### Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

## Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANSscreen\cognos\analytics\configuration` y `..\SANSscreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aquí -H y -i van a agregar `subjectAltNames` como `dns` e `ipaddress`.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido `encryptRequest.csr` y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `root.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `Intermediate.cer` con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
  - c. Guarde el archivo como `chain.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer`
  - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer`
  - d. `ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer`
11. Abra la configuración de IBM Cognos.
  - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos

- b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
  - a. `cd "C:\Archivos de programa\SANscreen"`
  - b. `java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analítica\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias cifrado`
13. Haga una copia de seguridad del servidor de seguridad DWH  
`en..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe "c:\temp\cognos.crt" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
  - a. `cd "C:\Archivos de programa\SANscreen"`
  - b. `java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore willose\reasons\configuration\server.trustore -storepass chretosca -alias cognos3rdca`
15. Reinicie el servicio SANscreen.
16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.
  - a. `cd "%SANSSCREEN_HOME%cognos\analytics\bin\"`
  - b. `"%SANSSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
  - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"`

Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es

demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Utilice regedit para modificar los valores del Registro en

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. Cambie la JVM\_OPTION -DclientAuth=false para -DclientAuth=true.

Para Linux, modifique el clientAuth parámetro in /opt/netapp/oci/scripts/wildfly.server

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

- a. En una ventana de comandos, vaya a `..\SANscreen\wildfly\standalone\configuration`.

- b. Utilice la keytool Utilidad para enumerar las CA de confianza: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

La primera palabra de cada línea indica el alias de CA.

- c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un .pem archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a

`..\SANscreen\wildfly\standalone\configuration` y utilice la keytool comando de importación: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

Mi\_alias es normalmente un alias que fácilmente identificaría la CA enkeytool -list funcionamiento.

3. En el servidor OnCommand Insight, el wildfly/standalone/configuration/standalone-full.xml El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en /subsystem=undertow/server=default-server/https-listener=default-httpsPara activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

SO	Guión
Windows	<install dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB .bat
Linux	/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh

Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecuten OnCommand Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

La primera palabra de cada línea indica el alias de CA.

- c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un .pem archivo.
- d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.  
`..\SANscreen\cognos\analytics\configuration\certs\.`
- e. Utilice la `keytool` utilidad para importar .pem archivo: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

- f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.
- g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Para desactivar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
  - a. En una ventana de comandos, vaya a.  
`..\SANscreen\cognos\analytics\configuration\certs\`

- b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

La primera palabra de cada línea indica el alias de CA.

- c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
- d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a `..\SANscreen\cognos\analytics\configuration\certs\`.
- e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

- f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

- g. Responda `yes` cuando se le solicite que confíe en el certificado.

2. Para activar el modo CAC, realizar lo siguiente:

- a. Configure la página salir de CAC siguiendo los pasos siguientes:
- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, `cognos_admin`)
  - (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
  - (Sólo para 7.3.10 y 7.3.11) Introduzca `cacLogout.html` con la URL de redireccionamiento de cierre de sesión -> aplicar
  - Cierre el navegador.

- b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

- c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

3. Para desactivar el modo CAC, realizar lo siguiente:

- a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

- b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

- c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, `cognos_admin`)
- Haga clic en Administrar -> Configuración -> sistema -> Seguridad
- Escriba `cacLogout.html` con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados

para su entorno de Data Warehouse y Cognos.

## Antes de empezar

Este procedimiento se aplica a sistemas que ejecutan OnCommny Insight 7.3.5 a 7.3.9.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

## Pasos

1. Cree un backup de `..\SANSscreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANSscreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Envíe el `encryptRequest.csr` a la entidad de certificación (CA) para obtener un certificado SSL.

Asegúrese de agregar atributos adicionales como "TAN:dns=FQDN (por ejemplo, hostname.netapp.com)" para agregar SubjectAltName. Google Chrome versión 58 y posteriores se queja si falta SubjectAltName en el certificado.

6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios



pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:

- a. Abra el certificado .p7b en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 al 8 c para exportar todos los certificados por separado en archivos .cer.
  - g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
- a. Abra Intermediate.cer con el Bloc de notas y copie el contenido.
  - b. Abra root.cer con el Bloc de notas y guarde el contenido de 9a.
  - c. Guarde el archivo como CA.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
- a. `cd "Archivos de programa\sanscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer`
- Esto establecerá CA.cer como entidad emisora de certificados raíz.
- c. `ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`
- Esto establecerá Cognos.cer como certificado de cifrado firmado por CA.cer.
11. Abra la configuración de IBM Cognos.
- a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
  - b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
- a. `"D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -exportcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\cognos\analítica\Configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoWordSet -alias cifrado`
13. Importe "c:\temp\cognos.crt" en dwh truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
- a. `"D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -importcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\wiland\autónoma\Configuration\Server.trustore" -storeprechrit -alias cognoscert`
14. Reinicie el servicio SANscreen.
15. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

### Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANSscreen\cognos\analytics\configuration` y `..\SANSscreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: Aquí -H y -i van a agregar `subjectAltNames` como `dns` e `ipaddress`.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido `encryptRequest.csr` y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.

8. ThirdPartyCertificateTool.bat no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado .p7b en ""Extensiones de shell de cifrado"".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos .cer.
  - g. Asigne un nombre a los archivos intermediateX.cer y cognos.cer.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine root.cer y intermediateX.cer en un archivo.
  - a. Abra root.cer con el Bloc de notas y copie el contenido.
  - b. Abra Intermediate.cer con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
  - c. Guarde el archivo como chain.cer.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd ""Archivos de programa\sanscreen\cognos\analítica\bin""`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer`
  - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer`
  - d. `ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer`
11. Abra la configuración de IBM Cognos.
  - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
  - b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
  - a. `cd ""C:\Archivos de programa\SANscreen""`
  - b. `java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analítica\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias cifrado`
13. Haga una copia de seguridad del servidor de seguridad DWH  
`en.. \SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importe ""c:\temp\cognos.crt"" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
  - a. `cd ""C:\Archivos de programa\SANscreen""`
  - b. `java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore willose\reasone\configuration\server.trustore -storepass chretosca -alias cognos3rdca`
15. Reinicie el servicio SANscreen.
16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.

- a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
- b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
- c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Importación de certificados SSL

Puede añadir certificados SSL para habilitar la autenticación y el cifrado mejorados a fin de mejorar la seguridad del entorno de OnCommand Insight.

### Antes de empezar

Debe asegurarse de que el sistema cumple el nivel de bit mínimo requerido (1024 bits).

### Acerca de esta tarea



Antes de intentar realizar este procedimiento, debe realizar una copia de seguridad de la existente `server.keystore` y asigne un nombre a la copia de seguridad `server.keystore.old`. Corromper o dañar el `server.keystore` El archivo puede resultar en un servidor Insight inoperable después de reiniciar el servidor Insight. Si crea una copia de seguridad, puede revertir al archivo antiguo si se producen problemas.

### Pasos

1. Cree una copia del archivo original del almacén de claves: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old"`
2. Enumere el contenido del almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

- a. Cuando se le pida una contraseña, introduzca `changeit`.

El sistema muestra el contenido del almacén de claves. Debe haber al menos un certificado en el almacén de claves, `"ssl certificate"`.

3. Elimine el `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Genere una nueva clave: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore`

"c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"

- a. Cuando se le soliciten los nombres y apellidos, introduzca el nombre de dominio completo (FQDN) que desee utilizar.
- b. Proporcione la siguiente información acerca de la organización y la estructura de su organización:
  - País: Abreviatura ISO de dos letras para su país (por ejemplo, US)
  - Estado o provincia: Nombre del estado o provincia donde está ubicada la oficina central de su organización (por ejemplo, Massachusetts)
  - Localidad: Nombre de la ciudad donde está ubicada la oficina central de su organización (por ejemplo, Waltham)
  - Nombre organizativo: Nombre de la organización a la que se pertenece el nombre de dominio (por ejemplo, NetApp).
  - Nombre de la unidad organizativa: Nombre del departamento o grupo que utilizará el certificado (por ejemplo, Soporte)
  - Nombre de dominio/ Nombre común: El FQDN que se utiliza para las búsquedas DNS de su servidor (por ejemplo, www.example.com) el sistema responde con información similar a la siguiente: Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?
- c. Introduzca Yes Cuando el nombre común (CN) es igual al FQDN.
- d. Al solicitar la contraseña clave, introduzca la contraseña o pulse la tecla Intro para usar la contraseña del almacén de claves existente.

5. Generar un archivo de solicitud de certificado: C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr

La c:\localhost.csr archivo es el archivo de solicitud de certificado que se acaba de generar.

6. Envíe el c:\localhost.csr Archivar a la entidad emisora de certificados (CA) para su aprobación.

Una vez aprobado el archivo de solicitud de certificado, desea que se le devuelva el certificado .der formato. Es posible que el archivo no se devuelva como a. .der archivo. El formato de archivo predeterminado es .cer Para los servicios de CA de Microsoft.

Las CA de la mayoría de las organizaciones utilizan una cadena de modelo de confianza, incluida una CA raíz, que a menudo se encuentra sin conexión. Ha firmado los certificados para sólo algunas CA secundarias, conocidas como CA intermedias.

Debe obtener la clave pública (certificados) para toda la cadena de confianza: El certificado de la CA que firmó el certificado para el servidor OnCommand Insight, y todos los certificados entre esa CA firmada hasta la CA raíz de la organización y hasta ella.

En algunas organizaciones, al enviar una solicitud de firma, es posible que reciba una de las siguientes opciones:

- Archivo PKCS12 que contiene el certificado firmado y todos los certificados públicos de la cadena de confianza
- A. .zip archivo que contiene archivos individuales (incluido el certificado firmado) y todos los

certificados públicos de la cadena de confianza

- Solo el certificado firmado

Debe obtener los certificados públicos.

7. Importe el certificado aprobado para Server.keystore: C:\Program

```
Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com  
-file c:\localhost2.DER -keystore "c:\Program  
Files\SANscreen\wildfly\standalone\configuration\server.keystore"
```

- a. Al solicitar, introduzca la contraseña del almacén de claves.

Se muestra el siguiente mensaje: Certificate reply was installed in keystore

8. Importe el certificado aprobado para Server.trustore: C:\Program

```
Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com  
-file c:\localhost2.DER -keystore "c:\Program  
Files\SANscreen\wildfly\standalone\configuration\server.trustore"
```

- a. Cuando se le solicite, introduzca la contraseña de trusted.

Se muestra el siguiente mensaje: Certificate reply was installed in trustore

9. Edite el SANscreen\wildfly\standalone\configuration\standalone-full.xml archivo:

Sustituya la siguiente cadena de alias: alias="cbc-oci-02.muccbc.hq.netapp.com". Por ejemplo:

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"  
keystore-password="{VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-  
02.muccbc.hq.netapp.com" key-  
password="{VAULT::HttpsRealm::key_password::1}"/>
```

10. Reinicie el servicio del servidor SANscreen.

Una vez que Insight esté en funcionamiento, puede hacer clic en el icono de candado para ver los certificados instalados en el sistema.

Si ve un certificado que contiene información "emitida a" que coincide con la información "emitida por", todavía tiene instalado un certificado autofirmado. Los certificados autofirmados generados por el instalador de Insight tienen un vencimiento de 100 años.

NetApp no puede garantizar que este procedimiento elimine las advertencias de certificado digitales. NetApp no puede controlar el modo en que se han configurado las estaciones de trabajo de los usuarios finales. Considere los siguientes casos:

- Microsoft Internet Explorer y Google Chrome utilizan las funciones de certificado nativo de Microsoft en Windows.

Esto significa que si los administradores de Active Directory presionan los certificados de CA de su empresa en los almacenes de certificados del usuario final, los usuarios de estos exploradores verán que desaparecen las advertencias de certificado cuando los certificados autofirmados de OnCommand Insight se han reemplazado por los firmados por la infraestructura de CA interna.

- Java y Mozilla Firefox tienen sus propios almacenes de certificados.

Si los administradores del sistema no automatizan la ingestión de certificados de CA en los almacenes de certificados de confianza de estas aplicaciones, el uso del navegador Firefox puede continuar generando advertencias de certificados debido a un certificado que no es de confianza, incluso cuando el certificado autofirmado se haya reemplazado. Conseguir que la cadena de certificados de su empresa esté instalada en el almacén de verdad es un requisito adicional.

## Configuración de backups semanales para la base de datos de Insight

Puede configurar backups semanales automáticos para la base de datos de Insight para proteger los datos. Estas copias de seguridad automáticas sobrescriben los archivos en el directorio de copia de seguridad especificado.

### Acerca de esta tarea

**Mejor práctica:** Cuando se configura la copia de seguridad semanal de la base de datos OCI, es necesario almacenar las copias de seguridad en un servidor diferente al que está utilizando Insight, en caso de que falle el servidor. No almacene ninguna copia de seguridad manual en el directorio de copia de seguridad semanal porque cada copia de seguridad semanal sobrescribe los archivos en el directorio.

El archivo de copia de seguridad contendrá lo siguiente:

- Datos de inventario
- Hasta 7 días de datos de rendimiento

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin > Configuración**.
2. Haga clic en la ficha **copia de seguridad y archivo**.
3. En la sección copia de seguridad semanal, seleccione **Activar copia de seguridad semanal**.
4. Introduzca la ruta de acceso a la **ubicación de copia de seguridad**. Puede hacerlo en el servidor local de Insight o en un servidor remoto al que se puede acceder desde el servidor de Insight.



La configuración de ubicación de copia de seguridad se incluye en la copia de seguridad en sí, por lo que si restaura la copia de seguridad en otro sistema, tenga en cuenta que la ubicación de la carpeta de copia de seguridad puede no ser válida en el sistema nuevo. Compruebe dos veces la configuración de ubicación de copia de seguridad después de restaurar una copia de seguridad.

5. Seleccione la opción **Liberador de espacio** para guardar las dos últimas o las cinco últimas copias de seguridad.
6. Haga clic en **Guardar**.

### Resultados

También puede ir a **Admin > solución de problemas** para crear una copia de seguridad a petición.

### Lo que se incluye en el respaldo

Pueden utilizarse backups semanales y bajo demanda para solución de problemas o migración.

El backup semanal o bajo demanda incluye lo siguiente:

- Datos de inventario
- Datos de rendimiento (si se seleccionan para incluir en el backup)
- Orígenes de datos y configuración de orígenes de datos
- Paquetes de integración
- Unidades de adquisición remota
- Configuración de ASUP/proxy
- Configuración de ubicación de copia de seguridad
- Configuración de ubicación de archivo
- Configuración de notificaciones
- Usuarios
- Políticas de rendimiento
- Entidades y aplicaciones empresariales
- Reglas y configuración de resolución del dispositivo
- Paneles y widgets
- Widgets y paneles de páginas de activos personalizados
- Consultas
- Anotaciones y reglas de anotación

La copia de seguridad semanal no incluye:

- Configuración de herramientas de seguridad / información del almacén (copia de seguridad mediante un proceso CLI independiente)
- Registros (se pueden guardar en un archivo .zip bajo demanda)
- Datos de rendimiento (si no se seleccionan para incluir en el backup)
- Licencias



Si decide incluir datos de rendimiento en el backup, se realizará un backup de los siete días más recientes de datos. Los datos restantes estarán en el archivo si tiene activada esa función.

## Archivado de datos de rendimiento

OnCommand Insight 7.3 introduce la capacidad de archivar datos de rendimiento a diario. Esto complementa la configuración y ofrece backups de datos de rendimiento limitados.

OnCommand Insight conserva hasta 90 días de datos de rendimiento e infracciones. Sin embargo, cuando se crea una copia de seguridad de esos datos, en el backup solo se incluye la información más reciente. El archivado le permite guardar el resto de sus datos de rendimiento y cargarlos según sea necesario.

Una vez configurada la ubicación de archivado y se activa el archivado, Insight se archivarán los datos de rendimiento del día anterior para todos los objetos en la ubicación de archivado. El archivo de cada día se guarda en la carpeta de archivado en un archivo independiente. El archivado se realiza en segundo plano y



seguirá mientras se ejecute Insight.

Se conservan los 90 días más recientes de archivos; cuando se crean otros más nuevos, se eliminan los archivos de archivo antiguos 90 días.

## Permitiendo el archivado de rendimiento

Para habilitar el archivado de datos de rendimiento, siga estos pasos.

### Pasos

1. En la barra de herramientas, haga clic en **Admin > Configuración**.
2. Seleccione la ficha **copia de seguridad y archivo**.
3. En la sección Archivo de rendimiento, asegúrese de que **Habilitar archivo de rendimiento** esté activado.
4. Especifique una ubicación de archivo válida.

No puede especificar una carpeta en la carpeta de instalación de Insight.

Práctica recomendada: No especifique la misma carpeta para el archivado que la ubicación de copia de seguridad de Insight.

5. Haga clic en **Guardar**.

El proceso de archivado se gestiona en segundo plano y no interfiere con otras actividades de Insight.

## Cargando archivo de rendimiento

Para cargar el archivo de datos de rendimiento, siga estos pasos.

### Antes de empezar

Antes de cargar el archivo de datos de rendimiento, debe restaurar un backup manual o semanal válido.

### Pasos

1. En la barra de herramientas, haga clic en **Admin > solución de problemas**.
2. En la sección Restaurar, en **cargar archivo de rendimiento**, haga clic en **cargar**.



La carga de archivo se gestiona en segundo plano. La carga del archivado completo puede llevar mucho tiempo, ya que los datos de rendimiento de archivado diarios se completan en Insight. El estado de la carga del archivo se muestra en la sección de archivo de esta página.

## Configuración del correo electrónico

Debe configurar OnCommand Insight para acceder a su sistema de correo electrónico, de modo que OnCommand Insight Server pueda usar su correo electrónico con el fin de proporcionar informes a los que está suscrito y transportar información de soporte para la solución de problemas al soporte técnico de NetApp.

## Requisitos previos para la configuración del correo electrónico

Para poder configurar OnCommand Insight con el fin de acceder al sistema de correo electrónico, debe detectar el nombre de host o la dirección IP para identificar el servidor de correo (SMTP o Exchange) y asignar una cuenta de correo electrónico para los informes de OnCommand Insight.

Pida al administrador de correo electrónico que cree una cuenta de correo electrónico para OnCommand Insight. Necesitará la siguiente información:

- El nombre de host o la dirección IP para identificar el servidor de correo (SMTP o Exchange) que utiliza la organización. Puede encontrar esta información a través de la aplicación que utiliza para leer su correo electrónico. En Microsoft Outlook, por ejemplo, puede buscar el nombre del servidor visualizando la configuración de su cuenta: Herramientas - Cuentas de correo electrónico - Ver o cambiar la cuenta de correo existente.
- Nombre de la cuenta de correo electrónico a través de la cual OnCommand Insight enviará informes regulares. La cuenta debe ser una dirección de correo electrónico válida en su empresa. (La mayoría de los sistemas de correo no enviarán mensajes a menos que se envíen desde un usuario válido.) Si el servidor de correo electrónico requiere un nombre de usuario y una contraseña para enviar correo, obtenga esta información del administrador del sistema.

## Configuración de su correo electrónico para Insight

Si sus usuarios desean recibir informes de Insight en sus cuentas de correo electrónico, debe configurar su servidor de correo electrónico para habilitar esta función.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **correo electrónico** de la página.
3. En el cuadro **servidor**, escriba el nombre del servidor SMTP de su organización, que se identifica mediante un nombre de host o una dirección IP (*nnn.nnn.nnn.nnn* formato).

Si especifica un nombre de host, asegúrese de que el nombre se puede resolver mediante DNS.

4. En el cuadro **Nombre de usuario**, introduzca su nombre de usuario.
5. En el cuadro **Contraseña**, introduzca la contraseña para acceder al servidor de correo electrónico, que sólo es necesaria si el servidor SMTP está protegido mediante contraseña. Esta es la misma contraseña que utiliza para iniciar sesión en la aplicación que le permite leer su correo electrónico. Si se requiere una contraseña, debe introducirla por segunda vez para la verificación.
6. En el cuadro **correo electrónico del remitente**, introduzca la cuenta de correo electrónico del remitente que se identificará como remitente en todos los informes de OnCommand Insight.

Esta cuenta debe ser una cuenta de correo electrónico válida dentro de su empresa.

7. En el cuadro **firma de correo electrónico**, introduzca el texto que desea insertar en cada correo electrónico que se envíe.
8. En el cuadro destinatarios, haga clic en **+**, Introduzca una dirección de correo electrónico y haga clic en **Aceptar**.

Para editar una dirección de correo electrónico, seleccione la dirección y haga clic en . Para eliminar

una dirección de correo electrónico, seleccione la dirección y haga clic en .

9. Para enviar un correo electrónico de prueba a los destinatarios especificados, haga clic en .

10. Haga clic en **Guardar**.

## Configuración de notificaciones SNMP

OnCommand Insight admite notificaciones SNMP para cambios en la configuración y la política de ruta global, así como incumplimientos. Por ejemplo, las notificaciones SNMP se envían cuando se superan los umbrales del origen de datos.

### Antes de empezar

Deben haberse completado los siguientes pasos:

- Identificación de la dirección IP del servidor que consolida capturas para cada tipo de evento.

Es posible que tenga que consultar con el administrador del sistema para obtener esta información.

- Identificación del número de puerto mediante el cual la máquina designada obtiene capturas SNMP, para cada tipo de evento.

El puerto predeterminado para las capturas SNMP es 162.

- Compilando la MIB en su sitio.

La MIB propiedad incluye el software de instalación para admitir las capturas OnCommand Insight. El MIB de NetApp es compatible con todo el software de gestión SNMP estándar y se puede encontrar en el servidor Insight de `<install_dir>\SANscreen\MIBS\sanscreen.mib`.

### Pasos

1. Haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **SNMP** de la página.
3. Haga clic en **acciones** y seleccione **Agregar fuente de captura**.
4. En el cuadro de diálogo **Agregar destinatarios de capturas SNMP**, introduzca estos valores:

- **IP**

La dirección IP a la que OnCommand Insight envía mensajes de captura SNMP.

- **Puerto**

El número de puerto al que OnCommand Insight envía mensajes de captura SNMP.

- **Cadena comunitaria**

Utilice «'public'» para los mensajes de captura SNMP.

5. Haga clic en **Guardar**.

## Activación de la instalación de syslog

Puede identificar una ubicación para el registro de los incumplimientos y las alertas de rendimiento de OnCommand Insight, así como mensajes de auditoría, y activar el proceso de registro.

### Antes de empezar

- Debe tener la dirección IP del servidor en el que almacenar el registro del sistema.
- Debe conocer el nivel de instalación que corresponde al tipo de programa que está registrando el mensaje, como LOCAL1 o USUARIO.

### Acerca de esta tarea

Syslog incluye los siguientes tipos de información:

- Mensajes de infracción
- Alertas de rendimiento
- De manera opcional, los mensajes del registro de auditoría

Las siguientes unidades se usan en el syslog:

- Métricas de utilización: Porcentaje
- Métricas de tráfico: MB
- Velocidad de tráfico: MB/s

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **Notificaciones**.
2. Desplácese hasta la sección **Syslog** de la página.
3. Active la casilla de verificación **Activar syslog**.
4. Si lo desea, active la casilla de verificación **Enviar auditoría**. Se enviarán nuevos mensajes de registro de auditoría a syslog además de mostrarse en la página de auditoría. Tenga en cuenta que los mensajes de registro de auditoría que ya son existentes no se enviarán a syslog; solo se enviarán los mensajes de registro recién generados.
5. En el campo **servidor**, introduzca la dirección IP del servidor de registro.  
  
Puede especificar un puerto personalizado anexándolo después de dos puntos al final de la IP del servidor (por ejemplo, Server:Port). Si no se especifica el puerto, se utiliza el puerto de syslog predeterminado de 514.
6. En el campo **Facility**, seleccione el nivel de instalación que corresponda al tipo de programa que está registrando el mensaje.
7. Haga clic en **Guardar**.

### Contenido de syslog de Insight

Puede habilitar un syslog en un servidor para recopilar mensajes de alerta de rendimiento y violación de Insight que incluyan datos de utilización y tráfico.

## Tipos de mensaje

Insight syslog enumera tres tipos de mensajes:

- Infracciones de la ruta DE SAN
- Violaciones generales
- Alertas de rendimiento

## Datos proporcionados

Las descripciones de infracción incluyen los elementos implicados, el tiempo del evento y la gravedad o prioridad relativa de la infracción.

Las alertas de rendimiento incluyen los siguientes datos:

- Porcentajes de utilización
- Tipos de tráfico
- Velocidad de tráfico medida en MB

## Configurar el rendimiento y garantizar notificaciones de infracciones

OnCommand Insight admite notificaciones para incumplimientos de rendimiento y garantiza los incumplimientos. De manera predeterminada, Insight no envía notificaciones de estos incumplimientos; debe configurar Insight para que envíe correo electrónico, para enviar mensajes de syslog al servidor de syslog o para enviar notificaciones SNMP cuando se produce una infracción.

## Antes de empezar

Debe haber configurado métodos de envío de correo electrónico, syslog y SNMP para infracciones.

## Pasos

1. Haga clic en **Admin > Notificaciones**.
2. Haga clic en **Eventos**.
3. En la sección **Eventos de infracciones de rendimiento** o **Eventos de infracciones de seguridad**, haga clic en la lista del método de notificación (**correo electrónico**, **Syslog** o **SNMP**) que desee y seleccione el nivel de gravedad (**Advertencia y superior** o **crítico**) para la violación.
4. Haga clic en **Guardar**.

## Configurar notificaciones de eventos en el nivel del sistema

OnCommand Insight admite notificaciones sobre eventos de nivel de sistema, como fallos de unidad de adquisición o errores de origen de datos. Para recibir notificaciones, debe configurar Insight para que envíe mensajes de correo electrónico cuando se produzca uno o varios de estos eventos.

## Antes de empezar

Debe haber configurado los destinatarios de correo electrónico para recibir notificaciones en **Admin > Notificaciones > métodos de envío**.

### Pasos

1. Haga clic en **Admin > Notificaciones**.
2. Haga clic en **Eventos**.
3. En la sección **Eventos de alerta del sistema** correo electrónico, seleccione el nivel de gravedad (**Advertencia y superior** o **crítico**) para la notificación o seleccione **no enviar** si no desea recibir notificaciones de eventos de nivel de sistema.
4. Haga clic en **Guardar**.
5. Haga clic en **Admin > Alertas del sistema** para configurar las alertas.
6. Para agregar una nueva alerta, haga clic en **+Agregar** y asigne a la alerta un nombre \* único. También puede hacer clic en el icono del lado derecho para **Editar** una alerta existente.
7. Seleccione el **Tipo de evento** en el que desea alertar, por ejemplo *error de unidad de adquisición*.
8. Seleccione un intervalo **Snooze** para suprimir notificaciones en eventos duplicados del tipo seleccionado para el intervalo de tiempo seleccionado. Si selecciona *Never*, recibirá notificaciones repetidas una vez por minuto hasta que el evento ya no se produzca.
9. Elija una **gravedad** (Advertencia o crítica) para la notificación de eventos.
10. De forma predeterminada, las notificaciones por correo electrónico se enviarán a la lista global de destinatarios o bien puede hacer clic en el enlace proporcionado para anular la lista global y enviar notificaciones a destinatarios específicos.
11. Haga clic en **Guardar** para añadir la alerta.

## Configurar el procesamiento de ASUP

Todos los productos de NetApp están equipados con funcionalidades automatizadas para ofrecer el mejor soporte posible a los clientes. El soporte automatizado (ASUP) envía periódicamente información predefinida y específica al soporte del cliente. Puede controlar la información que se va a reenviar a NetApp y con qué frecuencia se envía.

## Antes de empezar

Es necesario configurar OnCommand Insight para reenviar los datos antes de enviarlos.

## Acerca de esta tarea

Los datos de ASUP se reenvían mediante el protocolo HTTPS.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **Configuración**.
3. Haga clic en la ficha **ASUP y proxy**.
4. En la sección **ASUP**, seleccione **Activar ASUP** para activar la instalación de ASUP.

5. Si desea cambiar la información corporativa, actualice los siguientes campos:
  - **Nombre de la compañía**
  - **Nombre del sitio**
  - **Qué enviar:** Registros, datos de configuración, datos de rendimiento
6. Haga clic en **probar conexión** para asegurarse de que la conexión especificada funciona.
7. Haga clic en **Guardar**.
8. En la sección **Proxy**, elija si desea **Activar proxy** y especifique su información de proxy **host**, **puerto** y **usuario**.
9. Haga clic en **probar conexión** para asegurarse de que el proxy especificado funciona.
10. Haga clic en **Guardar**.

### Lo que se incluye en el paquete AutoSupport (ASUP)

El paquete AutoSupport contiene la copia de seguridad de la base de datos, así como información ampliada.

El paquete AutoSupport incluye lo siguiente:

- Datos de inventario
- Datos de rendimiento (si se seleccionan para incluir en ASUP)
- Orígenes de datos y configuración de orígenes de datos
- Paquetes de integración
- Unidades de adquisición remota
- Configuración de ASUP/proxy
- Configuración de ubicación de copia de seguridad
- Configuración de ubicación de archivo
- Configuración de notificaciones
- Usuarios
- Políticas de rendimiento
- Entidades y aplicaciones empresariales
- Reglas y configuración de resolución del dispositivo
- Paneles y widgets
- Widgets y paneles de páginas de activos personalizados
- Consultas
- Anotaciones y reglas de anotación
- Registros
- Licencias
- Estado de adquisición/origen de datos
- Estado de MySQL
- Información del sistema

El paquete AutoSupport no incluye:

- Configuración de herramientas de seguridad / información del almacén (copia de seguridad mediante un proceso CLI independiente)
- Datos de rendimiento (si no se seleccionan para incluir en ASUP)



Si decide incluir datos de rendimiento en el ASUP, se incluyen los siete días más recientes de datos. Los datos restantes estarán en el archivo si tiene activada esa función. Los datos de archivado no se incluyen en ASUP.

## Definición de aplicaciones

Si desea realizar un seguimiento de los datos asociados con aplicaciones específicas que se ejecutan en su entorno, debe definir dichas aplicaciones.

### Antes de empezar

Si desea asociar la aplicación a una entidad de negocio, debe haber creado ya la entidad de negocio.

### Acerca de esta tarea

Puede asociar las aplicaciones con los siguientes activos: Hosts, máquinas virtuales, volúmenes, volúmenes internos, qtrees, recursos compartidos e hipervisores.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.

Después de definir una aplicación, la página aplicaciones muestra el nombre de la aplicación, su prioridad y, si corresponde, la entidad de negocio asociada a la aplicación.

3. Haga clic en **Agregar**.

Aparece el cuadro de diálogo Agregar aplicación.

4. Introduzca un nombre único para la aplicación en el cuadro **Nombre**.
5. Haga clic en **prioridad** y seleccione la prioridad (crítica, alta, media o baja) de la aplicación en su entorno.
6. Si planea utilizar esta aplicación con una entidad de negocio, haga clic en **entidad de negocio** y seleccione la entidad de la lista.
7. **Opcional:** Si no utiliza el uso compartido de volúmenes, haga clic para desactivar el cuadro **Validar uso compartido de volúmenes**.

Esto requiere la licencia Assure. Configure esto cuando desee garantizar que cada host tenga acceso a los mismos volúmenes en un clúster. Por ejemplo, los hosts de clústeres de alta disponibilidad suelen tener que enmascarar a los mismos volúmenes para permitir la recuperación tras fallos; sin embargo, los hosts de aplicaciones que no estén relacionados suelen tener acceso a los mismos volúmenes físicos. Además, es posible que las políticas normativas exijan que se deniega explícitamente el acceso de aplicaciones no relacionadas a los mismos volúmenes físicos por motivos de seguridad.

8. Haga clic en **Guardar**.



La aplicación aparece en la página aplicaciones. Si hace clic en el nombre de la aplicación, Insight muestra la página de activos de la aplicación.



## Después de terminar

Después de definir una aplicación, puede ir a una página de activos para host, máquina virtual, volumen, volumen interno o hipervisor a fin de asignar una aplicación a un activo.

## Asignar aplicaciones a activos

Después de definir aplicaciones con o sin entidades de negocio, puede asociar las aplicaciones con activos.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo (host, máquina virtual, volumen o volumen interno) al que desea aplicar la aplicación. Para ello, siga uno de estos pasos:
  - Haga clic en **Panel**, seleccione **Panel de activos** y haga clic en el activo.
  - Haga clic en  En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, coloque el cursor sobre el nombre de la aplicación actualmente asignada al activo (si no hay ninguna aplicación asignada, aparece **Ninguno** en su lugar) y, a continuación, haga clic en  (Editar aplicación).

Lista de aplicaciones disponibles para la visualización de activos seleccionados. Las aplicaciones que están actualmente asociadas con el activo van precedidas de una Marca de verificación.

4. Puede escribir en el cuadro Buscar para filtrar los nombres de las aplicaciones o desplazarse por la lista.
5. Seleccione las aplicaciones que desea asociar al activo.

Es posible asignar varias aplicaciones a un host, una máquina virtual y un volumen interno; no obstante, solo se puede asignar una aplicación al volumen.


6. Haga clic en  para asignar la aplicación o aplicaciones seleccionadas al activo.

Los nombres de las aplicaciones aparecen en la sección datos de usuario; si la aplicación está asociada a una entidad de negocio, el nombre de la entidad de negocio también aparece en esta sección.

## Editar aplicaciones

Se recomienda cambiar la prioridad de una aplicación, la entidad empresarial asociada con una aplicación o el estado de uso compartido de un volumen.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.
3. Coloque el cursor sobre la aplicación que desea editar y haga clic en .

Aparece el cuadro de diálogo Editar aplicación.

4. Realice alguna de las siguientes acciones:

- Haga clic en **prioridad** y seleccione una prioridad diferente.



No se puede cambiar el nombre de la aplicación.

- Haga clic en **entidad de negocio** y seleccione una entidad de negocio diferente con la que asociar la aplicación o seleccione **ninguna** para eliminar la asociación de la aplicación con la entidad de negocio.
- Haga clic para desactivar o seleccionar **Validar el uso compartido de volúmenes**.




Esta opción solo está disponible si tiene la licencia Assure.

5. Haga clic en **Guardar**.

## Eliminar aplicaciones

Es posible que desee eliminar una aplicación cuando ya no satisfaga una necesidad en el entorno.

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **aplicaciones**.
3. Coloque el cursor sobre la aplicación que desea eliminar y haga clic en .

Aparecerá un cuadro de diálogo de confirmación en el que se le preguntará si desea eliminar la aplicación.

4. Haga clic en **Aceptar**.

## La jerarquía de entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular.

En OnCommand Insight, la jerarquía de entidades de negocio contiene estos niveles:

- **El cliente** se utiliza principalmente por los proveedores de servicios para asociar recursos con un cliente, por ejemplo, NetApp.
- **Línea de negocio (LOB)** es una línea de negocio o línea de producto dentro de una compañía, por ejemplo, almacenamiento de datos.
- **Unidad de Negocio** representa una unidad de negocio tradicional como Legal o Marketing.
- **El proyecto** se utiliza a menudo para identificar un proyecto específico dentro de una unidad de negocio para la cual usted desea el pago por uso de capacidad. Por ejemplo, "Patentes" puede ser un nombre de proyecto para la unidad de negocio Legal y "Eventos de ventas" puede ser un nombre de proyecto para la unidad de negocio de marketing. Tenga en cuenta que los nombres de nivel pueden incluir espacios.

No es necesario que utilice todos los niveles en el diseño de la jerarquía corporativa.

## Diseño de la jerarquía de entidades de negocio

Debe comprender los elementos de la estructura corporativa y lo que debe representar en las entidades de negocio porque se convierten en una estructura fija en su base de datos de OnCommand Insight. Puede utilizar la siguiente información para configurar las entidades de negocio. Recuerde que no es necesario utilizar todos los niveles de jerarquía para recopilar datos en estas categorías.

### Pasos

1. Examine cada nivel de la jerarquía de entidades de negocio para determinar si ese nivel debe incluirse en la jerarquía de entidades de negocio de su empresa:
  - **El nivel de inquilino** es necesario si su empresa es un ISP y desea hacer un seguimiento del uso de los recursos por parte del cliente.
  - **La línea de negocio (LOB)** es necesaria en la jerarquía si es necesario hacer un seguimiento de los datos de las diferentes líneas de producto.
  - **La unidad de negocio** es necesaria si necesita realizar un seguimiento de los datos de diferentes departamentos. Este nivel de la jerarquía suele ser valioso para separar un recurso que un departamento utiliza que otros departamentos no.
  - **El nivel de proyecto** se puede utilizar para trabajos especializados dentro de un departamento. Estos datos pueden ser útiles para determinar, definir y supervisar las necesidades tecnológicas de un proyecto independiente en comparación con otros proyectos de una empresa o departamento.
2. Cree un gráfico que muestre cada entidad de negocio con los nombres de todos los niveles dentro de la entidad.
3. Compruebe los nombres en la jerarquía para estar seguros de que serán explicativos en las vistas e informes de OnCommand Insight.
4. Identificar todas las aplicaciones que están asociadas con cada entidad de negocio.

## Creación de entidades de negocio

Después de diseñar la jerarquía de entidades de negocio para la empresa, puede configurar aplicaciones y, a continuación, asociar las entidades de negocio con las aplicaciones. Este proceso crea la estructura de entidades de negocio en la base de datos de OnCommand Insight.

### Acerca de esta tarea

Asociar aplicaciones con entidades de negocio es opcional; sin embargo, es una práctica recomendada.

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **entidades empresariales**.

Aparece la página entidades de negocio.

3. Haga clic en  **Add** para empezar a construir una nueva entidad.

Aparece el cuadro de diálogo **Agregar entidad de negocio**.

4. Para cada nivel de entidad (inquilino, línea de negocio, Unidad de negocio y proyecto), puede realizar cualquiera de las siguientes acciones:
  - Haga clic en la lista nivel de entidad y seleccione un valor.
  - Escriba un nuevo valor y pulse Intro.
  - Deje el valor de nivel de entidad como N/A si no desea utilizar el nivel de entidad para la entidad de negocio.
5. Haga clic en **Guardar**.

### Asignar entidades de negocio a activos

Es posible asignar una entidad de negocio a un activo (host, puerto, almacenamiento, switch, máquina virtual, qtree, share, volume o internal volume) sin haber asociado la entidad comercial a una aplicación; sin embargo, las entidades comerciales se asignan automáticamente a un activo si dicho activo está asociado con una aplicación relacionada con una entidad empresarial.



#### Antes de empezar

Debe haber creado ya una entidad de negocio.

#### Acerca de esta tarea

Si bien puede asignar entidades de negocio directamente a activos, se recomienda asignar aplicaciones a activos y, a continuación, asignar entidades de negocio a activos.


#### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la entidad de negocio realizando una de las siguientes acciones:
  - Haga clic en el activo en el panel de activos.
  - Haga clic en  En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, sitúe el cursor sobre **Ninguno** junto a **entidades de negocio** y, a continuación, haga clic en .

Se muestra la lista de entidades de negocio disponibles.

4. Escriba el cuadro **Buscar** para filtrar la lista de una entidad específica o desplácese hacia abajo por la lista; seleccione una entidad comercial de la lista.

Si la entidad de negocio que elija está asociada a una aplicación, se mostrará el nombre de la aplicación. En este caso, aparece la palabra "derived" junto al nombre de la entidad de negocio. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

5. Para reemplazar una aplicación derivada de una entidad de negocio, coloque el cursor sobre el nombre de la aplicación y haga clic en , seleccione otra entidad de negocio y seleccione otra aplicación de la lista.

## Asignar entidades de negocio a o eliminar entidades de negocio de varios activos

Puede asignar entidades de negocio a o quitar entidades de negocio de varios activos utilizando una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

### Antes de empezar

Debe haber creado ya las entidades de negocio que desea agregar a los activos deseados.

### Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Si lo desea, puede filtrar los activos a los que desea agregar entidades de negocio.
3. Seleccione los activos deseados en la lista o haga clic en ☐ ▼ Para seleccionar **todo**.

Aparece el botón **acciones**.

4. Para agregar una entidad de negocio a los activos seleccionados, haga clic en . Si el tipo de activo seleccionado puede tener entidades de negocio asignadas a él, verá la opción de menú a **Agregar entidad de negocio**. Seleccione esto.
5. Seleccione la entidad comercial deseada de la lista y haga clic en **Guardar**.

Cualquier nueva entidad de negocio que asigne reemplazará a cualquier entidad de negocio que ya se haya asignado al activo. La asignación de aplicaciones a activos también anulará las entidades de negocio asignadas de la misma manera. La asignación de entidades de negocio a como activo también puede reemplazar cualquier aplicación asignada a ese activo.

6. Para eliminar una entidad de negocio asignada a los activos, haga clic en  Y seleccione **Quitar entidad de negocio**.
7. Seleccione la entidad de negocio deseada de la lista y haga clic en **Eliminar**.

## Definición de anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos según sus requisitos corporativos, puede definir las anotaciones especializadas que necesite para tener una imagen completa de sus datos, como, por ejemplo, el fin de vida de los activos, el centro de datos, la creación de ubicaciones, el nivel de almacenamiento o el volumen, y el nivel de servicio del volumen interno.

### Pasos

1. Enumere cualquier terminología del sector a la que deben asociarse los datos del entorno.
2. Enumere la terminología corporativa a la que deben asociarse los datos de entorno, que no se está realizando un seguimiento utilizando las entidades de negocio.
3. Identifique los tipos de anotaciones predeterminados que pueda utilizar.
4. Identifique qué anotaciones personalizadas debe crear.

## Uso de anotaciones para supervisar su entorno

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. Por ejemplo, puede anotar los activos con información como finalización de la vida útil de los activos, centro de datos, ubicación del edificio, nivel de almacenamiento o nivel de servicio de volumen.

El uso de anotaciones para supervisar su entorno incluye las siguientes tareas de alto nivel:

- Crear o editar definiciones para todos los tipos de anotaciones.
- Mostrar páginas de activos y asociar cada activo con una o varias anotaciones.

Por ejemplo, si un activo se está arrendando y el arrendamiento caduca dentro de dos meses, puede que desee aplicar una anotación de fin de vida al activo. Esto ayuda a evitar que otros utilicen ese activo durante un tiempo prolongado.

- Crear reglas para aplicar anotaciones automáticamente a varios activos del mismo tipo.
- Utilizar la utilidad de importación de anotaciones para importar anotaciones.
- Filtrar activos por sus anotaciones.
- Agrupación de datos en informes basada en anotaciones y generación de dichos informes.

Consulte la *Guía de informes de OnCommand Insight* para obtener más información acerca de los informes.

## Gestión de tipos de anotaciones

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados, como el ciclo de vida de los activos (cumpleaños o fin de vida), la ubicación del centro de datos o edificio y la capa, que puede personalizar para que aparezcan en los informes. Puede definir valores para tipos de anotaciones predeterminados o crear sus propios tipos de anotaciones personalizadas. Posteriormente, puede editar esos valores.

### Tipos de anotaciones predeterminados

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados. Estas anotaciones se pueden utilizar para filtrar o agrupar datos y filtrar los informes de datos.

Puede asociar activos con tipos de anotación predeterminados como los siguientes:

- Ciclo de vida de los activos, como cumpleaños, puesta de sol o fin de vida
- Información sobre la ubicación de un dispositivo, como un centro de datos, un edificio o un piso
- Clasificación de activos, como por calidad (niveles), por dispositivos conectados (nivel de switch) o por nivel de servicio
- Estado, como caliente (alta utilización)

En la siguiente tabla se enumeran los tipos de anotaciones predeterminados. Puede editar cualquiera de estos nombres de anotaciones según sus necesidades.

Tipos de anotaciones	Descripción	Tipo
Alias	Nombre sencillo para un recurso.	Texto
Cumpleaños	Fecha en la que el dispositivo estaba o se pondrá en línea.	Fecha
Edificio	Ubicación física de recursos de host, almacenamiento, switch y cinta.	Lista
Ciudad	Ubicación municipal de recursos de host, almacenamiento, switch y cinta.	Lista
Grupo de recursos informáticos	Asignación de grupos utilizada por el origen de datos de sistemas de archivos del host y del equipo virtual.	Lista
Continente	Ubicación geográfica de recursos de host, almacenamiento, switch y cinta.	Lista
País	Ubicación nacional de recursos de host, almacenamiento, switch y cinta.	Lista
Centro de datos	La ubicación física del recurso y está disponible para hosts, cabinas de almacenamiento, switches y cintas.	Lista
Conexión directa	Indica (Sí o no) si un recurso de almacenamiento está conectado directamente a los hosts.	Booleano
Fin de la vida	Fecha en la que se desconecta un dispositivo, por ejemplo, si el arrendamiento ha caducado o se está retirando el hardware.	Fecha
Alias de estructura	Nombre sencillo para un tejido.	Texto
Piso	Ubicación de un dispositivo en la planta de un edificio. Se pueden definir para hosts, cabinas de almacenamiento, switches y cintas.	Lista

Caliente	Dispositivos que ya están en uso pesado regularmente o en el umbral de capacidad.	Booleano
Nota	Comentarios que desea asociar a un recurso.	Texto
Rack	Rack en el que reside el recurso.	Texto
Habitación	Sala en un edificio u otra ubicación de recursos de host, almacenamiento, switch y cinta.	Lista
SAN	Partición lógica de la red. Disponible en hosts, cabinas de almacenamiento, cintas, switches y aplicaciones.	Lista
Nivel de servicio	Un conjunto de niveles de servicio compatibles que puede asignar a recursos. Proporciona una lista de opciones ordenadas para volúmenes internos, qtrees y volúmenes. Editar niveles de servicio para establecer políticas de rendimiento para diferentes niveles.	Lista
Estado/provincia	Estado o provincia en la que se encuentra el recurso.	Lista
Puesta de sol	Límite establecido después del cual no se puede realizar ninguna asignación nueva a ese dispositivo. Útil para migraciones planificadas y otros cambios de red pendientes.	Fecha
Cambiar el nivel	Incluye opciones predefinidas para configurar categorías de conmutadores. Normalmente, estas designaciones permanecen durante toda la vida útil del dispositivo, aunque puede modificarlas, si es necesario. Sólo disponible para interruptores.	Lista



Nivel	Puede utilizarse para definir distintos niveles de servicio dentro de su entorno. Los niveles pueden definir el tipo de nivel, como la velocidad necesaria (por ejemplo, oro o plata). Esta función solo está disponible en volúmenes internos, qtrees, cabinas de almacenamiento, pools de almacenamiento y volúmenes.	Lista
Gravedad de la infracción	Clasificación (por ejemplo, mayor) de una infracción (por ejemplo, falta de puertos de host o falta de redundancia), en una jerarquía de mayor a menor importancia.	Lista



Alias, centro de datos, caliente, nivel de servicio, puesta de sol, El nivel de conmutador, el nivel de servicio, el nivel y la gravedad de la infracción son anotaciones a nivel de sistema, que no puede eliminar ni cambiar de nombre; sólo puede cambiar sus valores asignados.

### Cómo se asignan las anotaciones

Puede asignar anotaciones de forma manual o automática mediante reglas de anotación. OnCommand Insight también asigna automáticamente algunas anotaciones sobre la adquisición de activos y por herencia. Las anotaciones que asigne a un activo aparecerán en la sección datos de usuario de la página activo.

Las anotaciones se asignan de las siguientes formas:

- Puede asignar una anotación manualmente a un activo.

Si una anotación se asigna directamente a un activo, la anotación aparece como texto normal en una página de activos. Las anotaciones que se asignan manualmente siempre tienen prioridad sobre las anotaciones que son heredadas o asignadas por reglas de anotación.

- Puede crear una regla de anotación para asignar anotaciones automáticamente a activos del mismo tipo.

Si la anotación está asignada por regla, Insight muestra el nombre de la regla junto al nombre de la anotación en una página de activos.

- Insight asocia automáticamente un nivel con un modelo de niveles de almacenamiento para acelerar la asignación de anotaciones de almacenamiento a sus recursos sobre la adquisición de activos.

Ciertos recursos de almacenamiento se asocian automáticamente con un nivel predefinido (nivel 1 y nivel 2). Por ejemplo, el nivel de almacenamiento Symmetrix se basa en la familia Symmetrix y VMAX y está asociado con el nivel 1. Puede cambiar los valores predeterminados para que coincidan con sus requisitos de nivel. Si Insight asigna la anotación (por ejemplo, Tier), verá "System-defined" cuando sitúe el cursor sobre el nombre de la anotación en una página de activos.

- Unos pocos recursos (hijos de un activo) pueden derivar la anotación predefinida de nivel de su activo (principal).

Por ejemplo, si se asigna una anotación a un almacenamiento, la anotación de nivel se obtiene de todos los pools de almacenamiento, los volúmenes internos, los volúmenes, los qtrees y los recursos compartidos que pertenecen al almacenamiento. Si se aplica una anotación diferente a un volumen interno del almacenamiento, la anotación se deriva posteriormente de todos los volúmenes, qtrees y recursos compartidos. Aparece "derived" junto al nombre de la anotación en una página de activos.

## Asociación de costes con anotaciones

Antes de ejecutar informes relacionados con costes, debe asociar los costes con las anotaciones a nivel de sistema de nivel de servicio, nivel de switch y nivel, que permiten cobrar a los usuarios de almacenamiento en función del uso que hagan realmente de la producción y la capacidad replicada. Por ejemplo, para el nivel, puede tener valores de nivel Gold y Silver y asignar un coste más alto al nivel Gold que al nivel Silver.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en Administrar y seleccione **Anotaciones**.


Aparece la página anotación.

3. Coloque el cursor sobre la anotación nivel de servicio, nivel de conmutación o nivel y haga clic en .

Aparece el cuadro de diálogo Editar anotación.

4. Introduzca los valores para cualquier nivel existente en el campo **coste**.

Las anotaciones Tier y Service Level tienen los valores de Auto Tier y Object Storage, respectivamente, que no se pueden quitar.

5. Haga clic en  para agregar niveles adicionales.
6. Haga clic en **Guardar** cuando termine.

### Creación de anotaciones personalizadas

Con las anotaciones, puede agregar datos personalizados específicos del negocio que se ajusten a los activos de las necesidades del negocio. Aunque OnCommand Insight proporciona un conjunto de anotaciones predeterminadas, es posible que desee ver datos de otras maneras. Los datos de anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del switch, el número de puertos y las estadísticas de rendimiento. Insight no detecta los datos que se agregan con anotaciones.

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

La página Anotaciones muestra la lista de anotaciones.

3. Haga clic en .

Aparece el cuadro de diálogo **Agregar anotación**.

4. Introduzca un nombre y una descripción en los campos **Nombre** y **Descripción**.

Es posible introducir hasta 255 caracteres en estos campos.



Nombres de anotaciones que empiezan o terminan con un punto "." no son compatibles.

5. Haga clic en **Tipo** y, a continuación, seleccione una de las siguientes opciones que representa el tipo de datos permitidos en esta anotación:

- **Booleano**

Esto crea una lista desplegable con las opciones de yes y no. Por ejemplo, la anotación "Ditret adjuntado" es booleana.

- **Fecha**

Esto crea un campo que contiene una fecha. Por ejemplo, si la anotación será una fecha, selecciónela.

- **Lista**

Esto puede crear uno de los siguientes:

- **Una lista desplegable fija**

Cuando otros están asignando este tipo de anotación en un dispositivo, no pueden agregar más valores a la lista.

- **Una lista desplegable flexible**

Si selecciona la opción **Agregar nuevos valores sobre la marcha** al crear esta lista, cuando otros asignan este tipo de anotación en un dispositivo, pueden agregar más valores a la lista.

- **Número**

Esto crea un campo en el que el usuario que asigna la anotación puede introducir un número. Por ejemplo, si el tipo de anotación es "Piso", el usuario puede seleccionar el tipo de valor "número" e introducir el número de piso.

- **Texto**

Esto crea un campo que permite texto de forma libre. Por ejemplo, puede escribir «'Idioma'» como tipo de anotación, seleccionar «'texto'» como tipo de valor e introducir un idioma como valor.




Después de establecer el tipo y guardar los cambios, no puede cambiar el tipo de anotación. Si necesita cambiar el tipo, debe eliminar la anotación y crear una nueva.

6. Si selecciona **List** como tipo de anotación, haga lo siguiente:

- Selecione **Agregar nuevos valores sobre la marcha** si desea la capacidad de agregar más valores a la anotación cuando se encuentra en una página de activos, que crea una lista flexible.

Por ejemplo, supongamos que se encuentra en una página de activos y que el activo tiene la anotación Ciudad con los valores Detroit, Tampa y Boston. Si ha seleccionado la opción **Agregar nuevos valores sobre la marcha**, puede agregar valores adicionales a Ciudad como San Francisco y Chicago directamente en la página de activos en lugar de tener que ir a la página Anotaciones para agregarlos. Si no selecciona esta opción, no podrá agregar nuevos valores de anotación al aplicar la anotación; esto creará una lista fija.

b. Introduzca un valor y un nombre en los campos **valor** y **Descripción**.

c. Haga clic en  para añadir valores adicionales.

d. Haga clic en  para eliminar un valor.

7. Haga clic en **Guardar**.

Las anotaciones aparecen en la lista de la página Anotaciones.

## Información relacionada

["Importar y exportar datos de usuario"](#)


## Asignación manual de anotaciones a activos

La asignación de anotaciones a activos ayuda a ordenar, agrupar e informar sobre los activos de forma que sean relevantes para su negocio. Aunque puede asignar anotaciones a activos de un tipo concreto automáticamente, mediante reglas de anotación, puede asignar anotaciones a un activo individual mediante su página de activos.

## Antes de empezar

Debe haber creado la anotación que desea asignar.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la anotación realizando una de las siguientes acciones:
  - Haga clic en el activo en el panel de activos.
  - Haga clic en  En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el tipo o el nombre del activo y, a continuación, seleccione el activo de la lista que aparece.

Aparece la página Asset.


3. En la sección **datos de usuario** de la página de activos, haga clic en .

Aparece el cuadro de diálogo Agregar anotación.

4. Haga clic en **anotación** y seleccione una anotación de la lista.
5. Haga clic en **valor** y realice una de las siguientes acciones, según el tipo de anotación que haya seleccionado:
  - Si el tipo de anotación es lista, fecha o booleano, seleccione un valor de la lista.

- Si el tipo de anotación es texto, escriba un valor.

6. Haga clic en **Guardar**.

7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en  y seleccione un valor diferente.

Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

## Modificación de anotaciones

Es posible que desee cambiar el nombre, la descripción o los valores de una anotación o eliminar una anotación que ya no desee utilizar.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desee editar y haga clic en .

Aparece el cuadro de diálogo **Editar anotación**.



4. Puede realizar las siguientes modificaciones en una anotación:

- a. Cambie el nombre, la descripción o ambos.

Sin embargo, tenga en cuenta que puede introducir un máximo de 255 caracteres tanto para el nombre como para la descripción, y no puede cambiar el tipo de anotación. Además, para las anotaciones a nivel de sistema, no se puede cambiar el nombre ni la descripción; sin embargo, se pueden agregar o quitar valores si la anotación es un tipo de lista.



Si se publica una anotación personalizada en el almacén de datos y se le cambia el nombre, se perderán los datos históricos.

- a. Para agregar otro valor a una anotación de tipo de lista, haga clic en .
- b. Para eliminar un valor de una anotación de un tipo de lista, haga clic en .

No se puede eliminar un valor de anotación si dicho valor está asociado a una anotación incluida en una regla de anotación, una consulta o una política de rendimiento.

5. Haga clic en **Guardar** cuando termine.

### Después de terminar

Si va a utilizar anotaciones en el almacén de datos, debe forzar una actualización de las anotaciones en el almacén de datos. Consulte la *OnCommand Insight Guía de administración de almacenes de datos*.

## Eliminar anotaciones

Es posible que desee eliminar una anotación que ya no desee utilizar. No puede eliminar una anotación a nivel de sistema ni una anotación que se utilice en una regla de anotación, una consulta o una política de rendimiento.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desea eliminar y haga clic en  .

Se muestra un cuadro de diálogo de confirmación.

4. Haga clic en **Aceptar**.

### Asignación de anotaciones a activos mediante reglas de anotación

Para asignar anotaciones automáticamente a activos basándose en los criterios definidos, configure reglas de anotación. OnCommand Insight asigna las anotaciones a los activos basándose en estas reglas. Insight también proporciona dos reglas de anotación predeterminadas, que se pueden modificar para ajustarse a sus necesidades o quitar si no desea utilizarlas.

### Reglas de anotación de almacenamiento predeterminadas

Para acelerar la asignación de anotaciones de almacenamiento a los recursos, OnCommand Insight incluye 21 reglas de anotación predeterminadas, que asocian un nivel a un modelo de niveles de almacenamiento. Todos los recursos de almacenamiento están asociados automáticamente con un nivel tras la adquisición de los activos de su entorno.

Las reglas de anotación predeterminadas aplican anotaciones de nivel de la siguiente manera:

- Nivel 1, nivel de calidad del almacenamiento

La anotación de nivel 1 se aplica a los siguientes proveedores y a sus familias específicas: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 o FAS6200) y Violin (memoria).

- Nivel 2, nivel de calidad del almacenamiento

La anotación del nivel 2 se aplica a los siguientes proveedores y a sus familias específicas: HP (3PAR StoreServ o EVA), EMC (CLARiiON), HDS (AMS o D800), IBM (XIV) y NetApp (FAS3000, FAS3100 y FAS3200).

Puede editar la configuración predeterminada de estas reglas para que se ajuste a sus requisitos de nivel o puede eliminarlas si no las necesita.

## Creación de reglas de anotación

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a varios activos mediante reglas de anotación. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

### Antes de empezar

Debe haber creado una consulta para la regla de anotación.

### Acerca de esta tarea

Aunque puede editar los tipos de anotaciones mientras crea las reglas, debe haber definido los tipos con anticipación.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Haga clic en  **Add**.

Aparece el cuadro de diálogo Agregar regla.

4. Haga lo siguiente:
  - a. En el cuadro **Nombre**, escriba un nombre único que describa la regla.  
  
Este nombre aparecerá en la página Reglas de anotación.
  - b. Haga clic en **Consulta** y seleccione la consulta que OnCommand Insight debe utilizar para aplicar la anotación a los activos.
  - c. Haga clic en **anotación** y seleccione la anotación que desea aplicar.
  - d. Haga clic en **valor** y seleccione un valor para la anotación.

Por ejemplo, si selecciona Cumpleaños como anotación, especifique una fecha para el valor.

5. Haga clic en **Guardar**.
6. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán a un intervalo programado regularmente.

### Establecimiento de la precedencia de regla de anotación

De forma predeterminada, OnCommand Insight evalúa las reglas de anotación secuencialmente; sin embargo, puede configurar el orden en el que OnCommand Insight evalúa las reglas de anotación si desea que Insight evalúe las reglas en un orden específico.

## Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Coloque el cursor sobre una regla de anotación.

Las flechas de precedencia aparecen a la derecha de la regla.

4. Para mover una regla hacia arriba o hacia abajo en la lista, haga clic en la flecha hacia arriba o hacia abajo.

De forma predeterminada, las nuevas reglas se agregan secuencialmente a la lista de reglas. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.


## Modificación de reglas de anotación

Puede modificar una regla de anotación para cambiar el nombre de la regla, su anotación, el valor de la anotación o la consulta asociada con la regla.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea modificar:
  - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
  - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una página.
4. Realice una de las siguientes acciones para visualizar el cuadro de diálogo **Editar regla**:
  - Si se encuentra en la página Reglas de anotación, coloque el cursor sobre la regla de anotación y haga clic en .
  - Si se encuentra en una página de activos, coloque el cursor sobre la anotación asociada con la regla, coloque el cursor sobre el nombre de la regla cuando aparezca y, a continuación, haga clic en el nombre de la regla.
5. Realice los cambios necesarios y haga clic en **Guardar**.

## Eliminación de reglas de anotación


Puede eliminar una regla de anotación cuando la regla ya no sea necesaria para supervisar los objetos de la red.



## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea eliminar:
  - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
  - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una sola página.
4. Coloque el cursor sobre la regla que desea eliminar y, a continuación, haga clic en .

Aparecerá un mensaje de confirmación en el que se le preguntará si desea eliminar la regla.

5. Haga clic en **Aceptar**.

## Importando valores de anotación

Si mantiene anotaciones en objetos SAN (como almacenamiento, hosts y máquinas virtuales) en un archivo CSV, puede importar esa información a OnCommand Insight. Puede importar aplicaciones, entidades de negocio o anotaciones como Tier y Building.

## Acerca de esta tarea

Se aplican las siguientes reglas:

- Si un valor de anotación está vacío, esa anotación se elimina del objeto.
- Al anotar volúmenes o volúmenes internos, el nombre del objeto es una combinación de nombre de almacenamiento y nombre de volumen utilizando el guión y el separador de flecha (->):

```
<storage_name>-><volume_name>
```

- Cuando se anota el almacenamiento, los conmutadores o los puertos, se omite la columna aplicación.
- Las columnas de inquilino, línea\_de\_negocio, Unidad\_Negocio y proyecto conforman una entidad de negocio.

Cualquiera de los valores puede dejarse en blanco. Si una aplicación ya está relacionada con una entidad de negocio distinta de los valores de entrada, la aplicación se asigna a la nueva entidad de negocio.

La utilidad de importación admite los siguientes tipos de objeto y claves:

Tipo	Clave
Host	id-><id> o. <Name> o. <IP>
MÁQUINA VIRTUAL	id-><id> o. <Name>

Del banco de almacenamiento	id-><id> 0. <Storage_name>-><Storage_Pool_name>
Volumen interno	id-><id> 0. <Storage_name>-><Internal_volume_name>
Volumen	id-><id> 0. <Storage_name>-><Volume_name>
Reducida	id-><id> 0. <Name> 0. <IP>
Conmutador	id-><id> 0. <Name> 0. <IP>
Puerto	id-><id> 0. <WWN>
Share	id-><id> 0. <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> es opcional si hay un qtree predeterminado.
Qtree	id-><id> 0. <Storage Name>-><Internal Volume Name>-><Qtree Name>

El archivo CSV debe utilizar el formato siguiente:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Admin** y seleccione **solución de problemas**.

Aparece la página solución de problemas.

3. En la sección **otras tareas** de la página, haga clic en el vínculo **Portal OnCommand Insight**.
4. Haga clic en **Insight Connect API**.
5. Inicie sesión en el portal.
6. Haga clic en **Utilidad de importación de anotación**.
7. Guarde la `.zip` descomprimirlo, descomprimirlo y leer el `readme.txt` archivo para obtener información adicional y muestras.
8. Coloque el archivo CSV en la misma carpeta que `.zip` archivo.
9. En la ventana de línea de comandos de, introduzca lo siguiente:

```
java -jar rest-import-utility.jar [-username] [-password]  
[-server name or IP address] [-batch size] [-ccase  
sensitive:true/false]  
[-extra logging:true/false] csv filename
```

La opción `-l`, que activa el registro adicional, y la opción `-c`, que habilita la sensibilidad del caso, se establecen en `FALSE` de forma predeterminada. Por lo tanto, sólo debe especificarlos cuando desee utilizar las operaciones.



No hay espacios entre las opciones y sus valores.



Las siguientes palabras clave están reservadas e impiden que los usuarios las especifiquen como nombres de anotación: `- Aplicación` - `prioridad_de_aplicación` - `arrendatario` - `línea_de_negocio` - `Unidad_de_negocio` - se generan errores de proyecto si intenta importar un tipo de anotación utilizando una de las palabras clave reservadas. Si ha creado nombres de anotación con estas palabras clave, debe modificarlas para que la herramienta de utilidad de importación pueda funcionar correctamente.



La utilidad de importación de anotaciones requiere Java 8 o Java 11. Asegúrese de que uno de ellos está instalado antes de ejecutar la utilidad de importación. Se recomienda utilizar la última versión de OpenJDK 11.

### Asignar anotaciones a varios activos mediante una consulta

La asignación de una anotación a un grupo de activos ayuda a identificar o utilizar más fácilmente los activos relacionados en consultas o paneles.

#### Antes de empezar

Las anotaciones que desea asignar a los activos deben haberse creado previamente.

#### Acerca de esta tarea

Puede simplificar la tarea de asignar una anotación a varios activos mediante una consulta. Por ejemplo, si desea asignar una anotación de dirección personalizada a todas las matrices en una ubicación específica del centro de datos.

## Pasos

1. Cree una nueva consulta para identificar los activos en los que desea asignar una anotación. Haga clic en **consultas > +Nueva consulta**.
2. En el menú desplegable **Buscar...**, elija **almacenamiento**. Puede establecer filtros para delimitar aún más la lista de almacenamientos mostrados.
3. En la lista de almacenamientos que se muestra, seleccione uno o varios haciendo clic en la casilla de comprobación situada junto al nombre del almacenamiento. También puede seleccionar todos los almacenamientos mostrados haciendo clic en la casilla de verificación principal de la parte superior de la lista.
4. Cuando haya seleccionado todos los almacenamientos deseados, haga clic en **acciones > Editar anotación**.

El sistema muestra el cuadro de diálogo Agregar anotación.

5. Seleccione **Annotation** y **Value** que desea asignar a los almacenamientos y haga clic en **Save**.

Si está mostrando la columna para esa anotación, aparecerá en todos los almacenamientos seleccionados.

6. Ahora puede utilizar la anotación para filtrar los almacenamientos en un widget o consulta. En un widget, puede hacer lo siguiente:
  - a. Cree un panel o abra uno existente. Añada una **variable** y elija la anotación que haya establecido en los almacenamientos anteriores. La variable se agrega al panel.
  - b. En el campo de variable que acaba de agregar, haga clic en **any** e introduzca el valor adecuado para filtrar. Haga clic en la Marca de verificación para guardar el valor de variable.
  - c. Agregar un widget. En la consulta del widget, haga clic en el botón **Filter by+** y seleccione la anotación correspondiente de la lista.
  - d. Haga clic en **Any** y seleccione la variable de anotación que agregó anteriormente. Las variables creadas empiezan por "\$" y se muestran en la lista desplegable.
  - e. Configure los otros filtros o campos que desee y, a continuación, haga clic en **Guardar** cuando el widget se personalice según sus preferencias.

El widget del panel de control muestra los datos sólo de los almacenamientos a los que se ha asignado la anotación.

## Consulta de activos

Las consultas permiten supervisar y solucionar problemas en la red mediante la búsqueda de activos en el entorno a un nivel granular en función de los criterios seleccionados por el usuario (anotaciones y métricas de rendimiento). Además, las reglas de anotación, que asignan anotaciones automáticamente a los activos, requieren una consulta.

### Activos utilizados en consultas y paneles

Las consultas de Insight y los widgets de panel pueden utilizarse con una amplia gama de tipos de activos

Los siguientes tipos de activos se pueden utilizar en consultas, widgets de panel y páginas de activos personalizados. Los campos y contadores disponibles para filtros, expresiones y visualización variarán entre los tipos de activos. No todos los activos se pueden utilizar en todos los tipos de widgets.

- Cliente más
- Almacén de datos
- Disco
- Estructura
- Dispositivo genérico
- Host
- Volumen interno
- Sesión iSCSI
- Portal de red de iSCSI
- Ruta
- Puerto
- Qtree
- Cuota
- Share
- Reducida
- Nodo de almacenamiento
- Pool de almacenamiento
- Conmutador
- Cinta
- VMDK
- Máquina virtual
- Volumen
- Zona
- Miembro de la zona

### **Crear una consulta**

Puede crear una consulta para poder buscar los activos de su entorno a un nivel granular. Las consultas permiten cortar los datos agregando filtros y, a continuación, ordenando los resultados para ver los datos de inventario y rendimiento en una sola vista.

#### **Acerca de esta tarea**

Por ejemplo, puede crear una consulta para los volúmenes, agregar un filtro para buscar determinados almacenamientos asociados al volumen seleccionado, agregar un filtro para buscar una anotación determinada, como el nivel 1, en los almacenamientos seleccionados, Y añada otro filtro para encontrar todos los almacenamientos con IOPS - Leer (IO/s) más de 25. Cuando se muestran los resultados, puede ordenar las columnas de información asociadas a la consulta en orden ascendente o descendente.

Cuando se agrega un nuevo origen de datos que adquiere activos o se realiza cualquier anotación o asignación de aplicaciones, puede consultar esos activos, anotaciones o aplicaciones después de indizar las consultas, lo que ocurre a intervalos regulares programados.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **+ Nueva consulta**.
3. Haga clic en **Seleccionar tipo de recurso** y seleccione un tipo de activo.

Cuando se selecciona un recurso para una consulta, se muestran automáticamente un número de columnas predeterminadas; puede eliminar estas columnas o agregar nuevas en cualquier momento.


4. En el cuadro de texto **Nombre**, escriba el nombre del activo o escriba una parte del texto para filtrar a través de los nombres de los activos.

Puede utilizar cualquiera de las opciones siguientes, solo o combinadas, para refinar la búsqueda en cualquier cuadro de texto de la página Nueva consulta:


- Un asterisco le permite buscar todo. Por ejemplo: `vol*rhel` muestra todos los recursos que empiezan con «'vol'» y terminan con «'rhel'».
- El signo de interrogación le permite buscar un número específico de caracteres. Por ejemplo: `BOS-PRD??-S12` Muestra BOS-PRD12-S12, BOS-PRD13-S12, etc.
- El operador OR permite especificar varias entidades. Por ejemplo: `FAS2240 OR CX600 OR FAS3270` busca varios modelos de almacenamiento.
- El operador NOT permite excluir el texto de los resultados de búsqueda. Por ejemplo: `NOT EMC*` Encuentra todo lo que no empieza con «'EMC'». Puede utilizar `NOT *` para mostrar campos que no contienen ningún valor.

5. Haga clic en  para mostrar los activos.

6. Para agregar un criterio, haga clic en , y realice una de las siguientes acciones:

- Escriba para buscar un criterio específico y, a continuación, selecciónelo.
- Desplácese hacia abajo por la lista y seleccione un criterio.
- Introduzca un rango de valores si selecciona una métrica de rendimiento, como IOPS - Read (IO/s). Las anotaciones predeterminadas proporcionadas por Insight se indican mediante ; es posible tener anotaciones con nombres duplicados.

Se agrega una columna a la lista resultados de la consulta para los criterios y los resultados de la consulta en la lista se actualizan.

7. De manera opcional, puede hacer clic en  para eliminar una métrica de rendimiento o anotación de los resultados de la consulta.

Por ejemplo, si la consulta muestra la latencia máxima y el rendimiento máximo de los almacenes de datos y desea mostrar sólo la latencia máxima en la lista de resultados de la consulta, haga clic en este botón y desactive la casilla de verificación **rendimiento - Máx**. La columna Throughput - Max (MB/s) se elimina de la lista resultados de la consulta.



Dependiendo del número de columnas que se muestran en la tabla de resultados de la consulta, es posible que no pueda ver columnas adicionales agregadas. Puede eliminar una o más columnas hasta que las columnas que desee se vean.

8. Haga clic en **Guardar**, escriba un nombre para la consulta y vuelva a hacer clic en **Guardar**.

Si tiene una cuenta con una función de administrador, puede crear paneles personalizados. Un panel personalizado puede incluir cualquiera de los widgets de la Biblioteca de widgets, algunos de los cuales permiten representar los resultados de las consultas en un panel personalizado. Para obtener más información acerca de los paneles personalizados, consulte la *Guía de introducción de OnCommand Insight*.

## Información relacionada

["Importar y exportar datos de usuario"](#)

## Ver consultas

Puede ver sus consultas para supervisar sus activos y cambiar el modo en que sus consultas muestran los datos relacionados con sus activos.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.
3. Puede cambiar el modo en que se muestran las consultas realizando cualquiera de las siguientes acciones:
  - Puede introducir texto en el cuadro **filtro** para buscar y mostrar consultas específicas.
  - Puede cambiar el orden de las columnas de la tabla de consultas a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
  - Para cambiar el tamaño de una columna, coloque el ratón sobre el encabezado de la columna hasta que aparezca una barra azul. Coloque el ratón sobre la barra y arrástrelo hacia la derecha o la izquierda.
  - Para mover una columna, haga clic en el encabezado de la columna y arrástrela hacia la derecha o hacia la izquierda.
  - Al desplazarse por los resultados de la consulta, tenga en cuenta que los resultados pueden cambiar a medida que Insight sondea automáticamente sus orígenes de datos. Esto puede resultar en que faltan algunos elementos o que algunos elementos aparezcan fuera de servicio en función de cómo se ordenen.


## Exportando resultados de consulta a un archivo .CSV

Es posible que desee exportar los resultados de una consulta a un archivo .CSV para importar los datos a otra aplicación.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Se muestra la página consultas.

3. Haga clic en una consulta.
4. Haga clic en  para exportar los resultados de la consulta a un .CSV archivo.
5. Debe realizar una de las siguientes acciones:
  - Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardar el archivo en una ubicación específica.
  - Haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas. Sólo se exportarán los atributos de las columnas mostradas. Algunas columnas mostradas, en particular las que forman parte de relaciones anidadas complejas, no se exportan.



Cuando aparece una coma en un nombre de activo, la exportación incluye el nombre entre comillas, conservando el nombre del activo y el formato .csv adecuado.

+ cuando exporte los resultados de la consulta, tenga en cuenta que **todas las filas** de la tabla de resultados se exportarán, no sólo las seleccionadas o mostradas en la pantalla, hasta un máximo de 10,000 filas.

Al abrir un archivo .CSV exportado con Excel, si tiene un nombre de objeto u otro campo con el formato NN:NN (dos dígitos seguidos de dos puntos seguidos de dos dígitos más), Excel interpretará a veces ese nombre como un formato de hora, en lugar de texto. Esto puede resultar en que Excel muestre valores incorrectos en esas columnas. Por ejemplo, un objeto llamado "81:45" se mostraría en Excel como "81:45:00". Para evitar esto, importe .CSV en Excel utilizando los pasos siguientes:

+

- Open a new sheet in Excel.
  - On the "Data" tab, choose "From Text".
  - Locate the desired .CSV file and click "Import".
  - In the Import wizard, choose "Delimited" and click Next.
  - Choose "Comma" for the delimiter and click Next.
  - Select the desired columns and choose "Text" for the column data format.
  - Click Finish.
- Your objects should show in Excel in the proper format.

+

## Modificar consultas

Puede cambiar los criterios asociados a una consulta cuando desee cambiar los criterios de búsqueda de los activos que esté consultando.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.

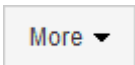


2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Se muestra la página consultas.

3. Haga clic en el nombre de la consulta.

4. Para eliminar un criterio de la consulta, haga clic en .

5. Para agregar un criterio a la consulta, haga clic en  y seleccione un criterio de la lista.

6. Debe realizar una de las siguientes acciones:

- Haga clic en **Guardar** para guardar la consulta con el nombre que se utilizó inicialmente.
- Haga clic en **Guardar como** para guardar la consulta con otro nombre.
- Haga clic en **Cambiar nombre** para cambiar el nombre de la consulta que ha utilizado inicialmente.
- Haga clic en **revertir** para volver a cambiar el nombre de la consulta al que había utilizado inicialmente.

## Eliminación de consultas

Puede eliminar consultas cuando ya no reúnan información útil sobre sus activos. No se puede eliminar una consulta si se utiliza en una regla de anotación.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Aparece la página consultas.

3. Coloque el cursor sobre la consulta que desea eliminar y haga clic en .

Aparece un mensaje de confirmación en el que se pregunta si desea eliminar la consulta.

4. Haga clic en **Aceptar**.

## Asignar múltiples aplicaciones a o quitar varias aplicaciones de activos

Puede asignar varias aplicaciones a o eliminar varias aplicaciones de activos mediante una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

### Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

### Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en ☐ ▼ Para seleccionar **todo**.

Aparece el botón **acciones**.

4. Para agregar una aplicación a los activos seleccionados, haga clic en  Y seleccione **Editar aplicación**.

- a. Haga clic en **aplicación** y seleccione una o más aplicaciones.

Es posible seleccionar varias aplicaciones para hosts, volúmenes internos y máquinas virtuales; sin embargo, solo puede seleccionar una aplicación para un volumen.

- b. Haga clic en **Guardar**.

5. Para eliminar una aplicación asignada a los activos, haga clic en  Y seleccione **Eliminar aplicación**.

- a. Seleccione la aplicación o aplicaciones que desea eliminar.

- b. Haga clic en **Eliminar**.

Las aplicaciones nuevas que asigne anulan las aplicaciones del activo que se derivaron de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de hosts y cuando se asignan aplicaciones nuevas a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

## Edición o eliminación de varias anotaciones de activos

Puede editar varias anotaciones para activos o eliminar varias anotaciones de activos mediante una consulta en lugar de tener que editarlas o eliminarlas manualmente.

### Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

### Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en ☐ ▼ Para seleccionar **todo**.


Aparece el botón **acciones**.

4. Para agregar una anotación a los activos o editar el valor de una anotación asignada a los activos, haga clic en  Y seleccione **Editar anotación**.

- a. Haga clic en **anotación** y seleccione una anotación para la que desee cambiar el valor, o seleccione una nueva anotación para asignarla a todos los activos.

- b. Haga clic en **valor** y seleccione un valor para la anotación.

c. Haga clic en **Guardar**.

5. Para eliminar una anotación asignada a los activos, haga clic en  Y seleccione **Quitar anotación**.

a. Haga clic en **anotación** y seleccione la anotación que desea eliminar de los activos.

b. Haga clic en **Eliminar**.

## Copiando valores de tabla

Puede copiar valores en tablas para utilizarlos en cuadros de búsqueda u otras aplicaciones.

### Acerca de esta tarea

Existen dos métodos que se pueden utilizar para copiar valores de tablas o resultados de consultas.

### Pasos

1. Método 1: Resalte el texto deseado con el ratón, cópielo y péguelo en campos de búsqueda u otras aplicaciones.
2. Método 2: Para campos de un solo valor cuya longitud supere el ancho de la columna de tabla, indicado por elipses (...), pase el cursor sobre el campo y haga clic en el icono del portapapeles. El valor se copia en el portapapeles para utilizarlo en campos de búsqueda u otras aplicaciones.

Tenga en cuenta que sólo se pueden copiar los valores que son vínculos a activos. Tenga en cuenta también que sólo los campos que incluyen valores únicos (es decir, no listas) tienen el icono de copia.

## Gestionar políticas de rendimiento

OnCommand Insight le permite crear políticas de rendimiento para supervisar la red de diversos umbrales y generar alertas cuando se superen esos umbrales. Mediante políticas de rendimiento, puede detectar una infracción de un umbral inmediatamente, identificar la implicación y analizar el impacto y la causa raíz del problema de forma que permita una corrección rápida y efectiva.

Una política de rendimiento permite establecer umbrales en cualquier objeto (almacén de datos, disco, hipervisor, volumen interno, puerto, Almacenamiento, nodo de almacenamiento, pool de almacenamiento, VMDK, máquina virtual, Y volumen) con contadores de rendimiento reportados (por ejemplo, un total de IOPS). Cuando se produce una infracción de un umbral, Insight lo detecta y lo notifica en la página de activos asociados, mostrando un círculo sólido rojo; por alerta de correo electrónico, si se configura; y en el panel de infracciones o en cualquier panel personalizado que informe de infracciones.

Insight proporciona algunas políticas de rendimiento predeterminadas, que se pueden modificar o eliminar si no son aplicables al entorno, para los siguientes objetos:

- Hipervisor

Existen políticas de intercambio de ESX y uso de ESX.

- Volumen y volumen internos

Hay dos políticas de latencia para cada recurso, una anotada para el nivel 1 y la otra anotada para el nivel 2.

- Puerto

Existe una política para el crédito de BB cero.

- Nodo de almacenamiento

Existe una política de uso de nodos.

- Máquina virtual

Se intercambian las VM y las políticas de CPU y memoria de ESX.

- Volumen

Existen normativas de volumen mal alineadas y de nivel de latencia.

### Crear políticas de rendimiento

Se crean políticas de rendimiento para establecer umbrales que activen alertas para notificarle acerca de los problemas relacionados con los recursos de la red. Por ejemplo, puede crear una política de rendimiento para alertarle cuando el uso total de los pools de almacenamiento es superior al 60 %.

#### Pasos

1. Abra OnCommand Insight en el explorador.
2. Seleccione **gestionar > políticas de rendimiento**.

Se muestra la página Performance

Insight Demo

Search

Alerts

Reports

Users

Dashboard

Queries

Manage

Admin 26

Performance Policies

Add new policy

Dataverse policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Latency	Warning		First occurrence	'Latency - Total' > 200 ms
Dataverse_0	Warning		First occurrence	'IOPS - Total' > 0 I/Os or 'Latency - Total' > 0 ms

Showing 1 to 2 of 2 entries

Internal volume policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Atmos Service Level	Critical	Service_Level = Atmos	First occurrence	'Latency - Total' > 100 ms or 'IOPS - Total' > 100 I/Os or 'Throughput - Total' > 200 MB/s
Global	Critical		First occurrence	'Latency - Total' > 200 ms or 'IOPS - Total' > 1 I/Os or 'Throughput - Total' > 300 MB/s

Showing 1 to 2 of 2 entries

Storage policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Storage_Storage	Warning		First occurrence	'IOPS - Read' > 10 I/Os
Storage_0	Warning		First occurrence	'Throughput - Total' > 0 MB/s or 'IOPS - Total' > 0 I/Os

Showing 1 to 2 of 2 entries

Policies.

Las directivas se organizan por objeto y se evalúan en el orden en el que aparecen en la lista de ese objeto.

3. Haga clic en **Agregar nueva directiva**.

Aparecerá el cuadro de diálogo Add Policy.

4. En el campo **Nombre de directiva**, escriba un nombre para la directiva.

Debe usar un nombre diferente de los demás nombres de políticas del objeto. Por ejemplo, no se pueden tener dos políticas denominadas «'latencia'» para un volumen interno; sin embargo, se puede tener una política de «'latencia'» para un volumen interno y otra política de «'latencia'» para un volumen diferente. La práctica recomendada es utilizar siempre un nombre único para cualquier política, independientemente del tipo de objeto.

5. En la lista **aplicar a objetos de tipo**, seleccione el tipo de objeto al que se aplica la directiva.

6. En la lista **con anotación**, seleccione un tipo de anotación, si corresponde, e introduzca un valor para la anotación en el cuadro **valor** para aplicar la directiva sólo a los objetos que tienen definida esta anotación en particular.

7. Si ha seleccionado **Puerto** como tipo de objeto, en la lista **conectado a**, seleccione a qué puerto está conectado.

8. En la lista **aplicar después de una ventana de**, seleccione cuando se cree una alerta para indicar una infracción de umbral.

La primera opción de ocurrencia activa una alerta cuando se supera un umbral en la primera muestra de datos. Todas las demás opciones activan una alerta cuando el umbral se cruza una vez y se cruza de forma continua durante al menos el tiempo especificado.

9. En la lista **with severity**, seleccione la gravedad de la infracción.

10. De forma predeterminada, las alertas por correo electrónico sobre infracciones de directivas se enviarán a los destinatarios de la lista global de correo electrónico. Puede anular esta configuración para que se envíen alertas de una directiva concreta a destinatarios específicos.

- Haga clic en el vínculo para abrir la lista de destinatarios y, a continuación, haga clic en el botón **+** para agregar destinatarios. Las alertas de infracción de esa directiva se enviarán a todos los destinatarios de la lista.

11. Haga clic en el enlace **Any** de la sección **Crear alerta si cualquiera de las siguientes opciones son verdaderas** para controlar cómo se activan las alertas:

- **cualquiera**

Esta es la configuración predeterminada, que crea alertas cuando se cruza cualquiera de los umbrales relacionados con una política.

- **todo**

Este ajuste crea una alerta cuando se cruzan todos los umbrales de una política. Al seleccionar **all**, el primer umbral que se crea para una política de rendimiento se denomina regla principal. Debe asegurarse de que el umbral de regla principal sea la infracción de la que le preocupa más la política de rendimiento.

12. En la sección **Crear alerta si**, seleccione un contador de rendimiento y un operador y, a continuación, introduzca un valor para crear un umbral.

13. Haga clic en **Agregar umbral** para agregar más umbrales.
14. Para eliminar un umbral, haga clic en el icono de papelera.
15. Active la casilla de verificación **Detener el procesamiento de directivas adicionales si se genera una alerta** si desea que la directiva deje de procesarse cuando se produzca una alerta.

Por ejemplo, si tiene cuatro políticas para almacenes de datos y la segunda política se configura para detener el procesamiento cuando se produce una alerta, las tercera y cuarta políticas no se procesan mientras que la violación de la segunda política está activa.

16. Haga clic en **Guardar**.

Se muestra la página Performance Policies y la política de rendimiento se muestra en la lista de políticas para el tipo de objeto.

### Prioridad de evaluación de políticas de rendimiento

La página Performance Policies agrupa las políticas por tipo de objeto y Insight evalúa las políticas en el orden en que aparecen en la lista de políticas de rendimiento del objeto. Puede cambiar el orden en el que Insight evalúa las políticas para mostrar la información más importante para usted en su red.

Insight evalúa todas las políticas que se aplican a un objeto secuencialmente cuando se toman muestras de datos de rendimiento en el sistema para ese objeto; sin embargo, dependiendo de las anotaciones, no todas las políticas se aplican a un grupo de objetos. Por ejemplo, supongamos que el volumen interno tiene las siguientes políticas:

- Política 1 (la directiva predeterminada proporcionada por Insight)
- Política 2 (con una anotación de "nivel de servicio = Plata" con la opción **Detener el procesamiento de directivas adicionales si se genera una alerta**)
- Política 3 (con una anotación de "nivel de servicio = oro")
- Política 4

Para un nivel de volumen interno con una anotación Gold, Insight evalúa la política 1, ignora la política 2 y, a continuación, evalúa la política 3 y la política 4. Para un nivel sin anotar, Insight evalúa según el orden de las políticas; por lo tanto, Insight evalúa únicamente la Política 1 y la Política 4. Para un nivel de volumen interno con una anotación Silver, Insight evalúa las políticas 1 y 2; Sin embargo, si una alerta se activa cuando el umbral de la política se cruza una vez y se cruza continuamente para la ventana de tiempo especificada en la política, Insight ya no evalúa las demás políticas de la lista mientras evalúa los contadores actuales del objeto. Cuando Insight captura el siguiente conjunto de muestras de rendimiento para el objeto, de nuevo comienza a evaluar las políticas de rendimiento para el objeto por filtro y luego por orden.

### Cambiar la prioridad de una política de rendimiento

De forma predeterminada, Insight evalúa las políticas de un objeto de forma secuencial. Puede configurar el orden en el que Insight evalúa las políticas de rendimiento. Por ejemplo, si tiene una política configurada para detener el procesamiento cuando se produce una infracción en el almacenamiento de nivel Gold, puede colocar esa política primero en la lista y evitar que se produzcan más infracciones genéricas del mismo activo de almacenamiento.

## Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

Se muestra la página Performance Policies.

3. Pase el cursor por el nombre de una política de la lista de políticas de rendimiento de un tipo de objeto.

Las flechas de precedencia aparecen a la derecha de la directiva.

4. Para mover una política hacia arriba en la lista, haga clic en la flecha hacia arriba; para mover una política hacia abajo en la lista, haga clic en la flecha hacia abajo.

De forma predeterminada, las nuevas directivas se agregan secuencialmente a la lista de directivas de un objeto.


## Editar políticas de rendimiento

Puede editar las políticas de rendimiento existentes y predeterminadas para cambiar la forma en que Insight supervisa las condiciones que le interesan en la red. Por ejemplo, se recomienda cambiar el umbral de una política.

## Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

Se muestra la página Performance Policies.

3. Pase el cursor sobre el nombre de una política de la lista de políticas de rendimiento de un objeto.
4. Haga clic en .

Se muestra el cuadro de diálogo Edit Policy.

5. Realice los cambios necesarios.

Si cambia alguna opción que no sea el nombre de la política, Insight elimina todos los incumplimientos existentes de esa política.

6. Haga clic en **Guardar**.


## Eliminar políticas de rendimiento

Puede eliminar una política de rendimiento si cree que ya no es aplicable a la supervisión de los objetos de la red.

## Pasos

1. Abra Insight en su navegador.
2. En el menú **gestionar**, seleccione **políticas de rendimiento**.

Se muestra la página Performance Policies.

3. Pase el cursor sobre el nombre de una política de la lista de políticas de rendimiento de un objeto.
4. Haga clic en .

Aparece un mensaje en el que se pregunta si desea eliminar la directiva.

5. Haga clic en **Aceptar**.

## Importar y exportar datos de usuario

Las funciones de importación y exportación permiten exportar anotaciones, reglas de anotación, consultas, políticas de rendimiento y paneles personalizados a un archivo. Este archivo se puede importar posteriormente a diferentes servidores OnCommand Insight.

Las funciones de exportación e importación sólo se admiten entre servidores que ejecutan la misma versión de OnCommand Insight.

Para exportar o importar datos de usuario, haga clic en **Admin** y seleccione **Configuración**; a continuación, seleccione la ficha **Importar/Exportar datos de usuario**.

Durante la operación de importación, los datos se agregan, combinan o reemplazan, dependiendo de los objetos y tipos de objeto que se importan.

- Tipos de anotaciones
  - Agrega una anotación si no existe ninguna anotación con el mismo nombre en el sistema de destino.
  - Combina una anotación si el tipo de anotación es una lista y existe una anotación con el mismo nombre en el sistema de destino.
  - Reemplaza una anotación si el tipo de anotación no es una lista y existe una anotación con el mismo nombre en el sistema de destino.



Si existe una anotación con el mismo nombre pero con un tipo diferente en el sistema de destino, la importación falla. Si los objetos dependen de la anotación fallida, dichos objetos pueden mostrar información incorrecta o no deseada. Debe comprobar todas las dependencias de anotación una vez completada la operación de importación.

- Reglas de anotación
  - Agrega una regla de anotación si no existe ninguna regla de anotación con el mismo nombre en el sistema de destino.
  - Reemplaza una regla de anotación si existe una regla de anotación con el mismo nombre en el sistema de destino.



Las reglas de anotación dependen tanto de las consultas como de las anotaciones. Debe comprobar la precisión de todas las reglas de anotación una vez completada la operación de importación.

- Normativas
  - Agrega una directiva si no existe ninguna directiva con el mismo nombre en el sistema de destino.



- Reemplaza una directiva si existe una directiva con el mismo nombre en el sistema de destino.



Las políticas pueden estar fuera de servicio una vez completada la operación de importación. Debe comprobar el orden de las directivas después de la importación. Las directivas que dependen de anotaciones pueden fallar si las anotaciones son incorrectas. Debe comprobar todas las dependencias de anotación después de la importación.

+

#### • Consultas

- Agrega una consulta si no existe ninguna consulta con el mismo nombre en el sistema de destino.
- Reemplaza una consulta si existe una consulta con el mismo nombre en el sistema de destino, incluso si el tipo de recurso de la consulta es diferente.



Si el tipo de recurso de una consulta es diferente, después de la importación, cualquier widget de panel que utilice esa consulta puede mostrar resultados no deseados o incorrectos. Debe comprobar la precisión de todos los widgets basados en consultas después de la importación. Las consultas que dependen de anotaciones pueden fallar si las anotaciones son incorrectas. Debe comprobar todas las dependencias de anotación después de la importación.

+

#### • Consolas

- Agrega un panel si no existe ningún panel con el mismo nombre en el sistema de destino.
- Reemplaza un panel si existe un panel con el mismo nombre en el sistema de destino, incluso si el tipo de recurso de la consulta es diferente.



Debe comprobar la precisión de todos los widgets basados en consultas en los paneles después de la importación. Si el servidor de origen tiene varios paneles con el mismo nombre, se exportarán todos. Sin embargo, sólo se importará el primero al servidor de destino. Para evitar errores durante la importación, debe asegurarse de que los paneles tienen nombres únicos antes de exportarlos.

+

## 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.

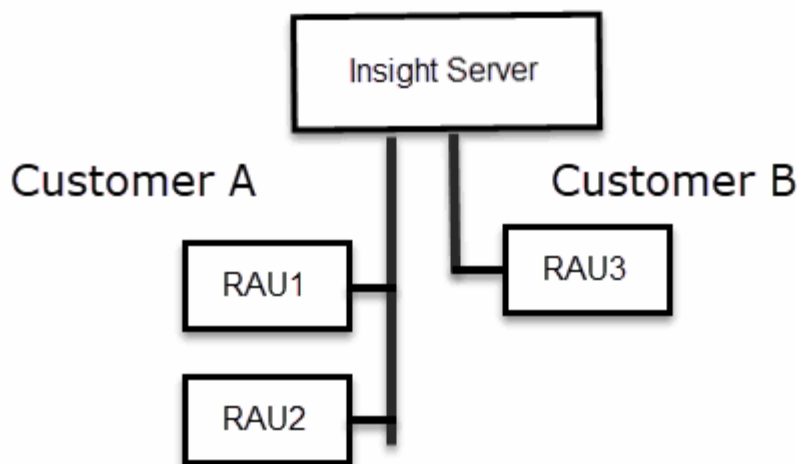
## **Consideraciones sobre la actualización y la instalación**

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
- dwuser
- hosts
- inventario
- raíz



Al cambiar las contraseñas de dwuser, 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
dwuser	
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**.

**Edit Connector**

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="••••••••"/>

**Advanced** ▼

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.

#### Edit Connector

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

Basic ^

6. 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.

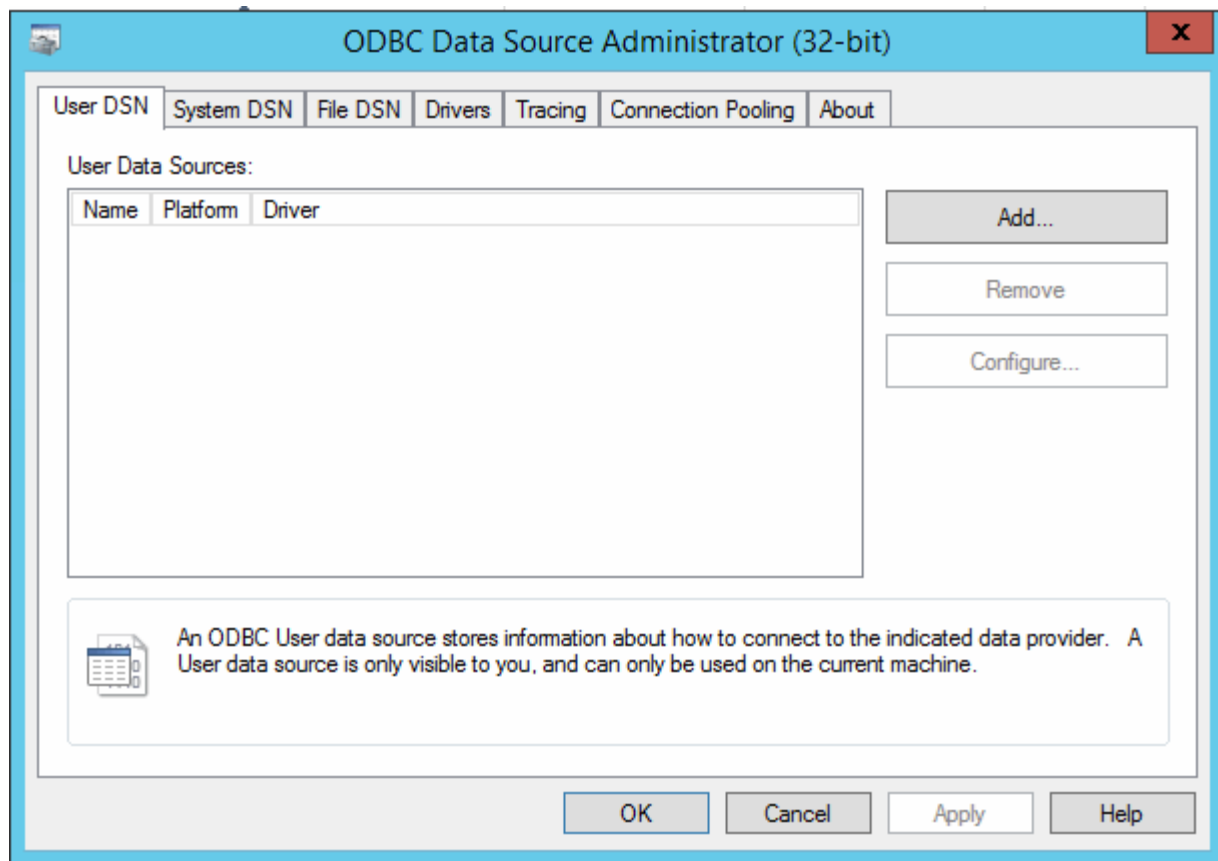
##### Antes de empezar

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

##### Pasos

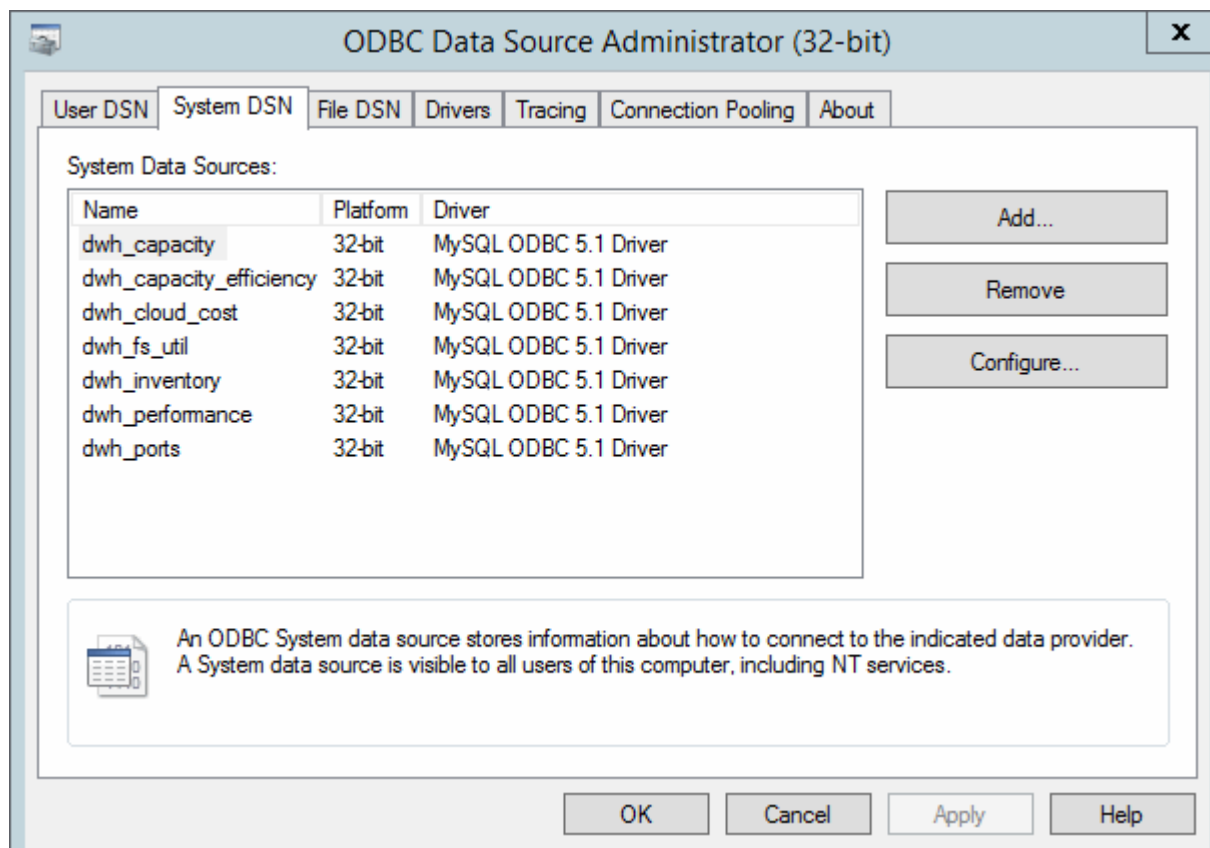
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

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



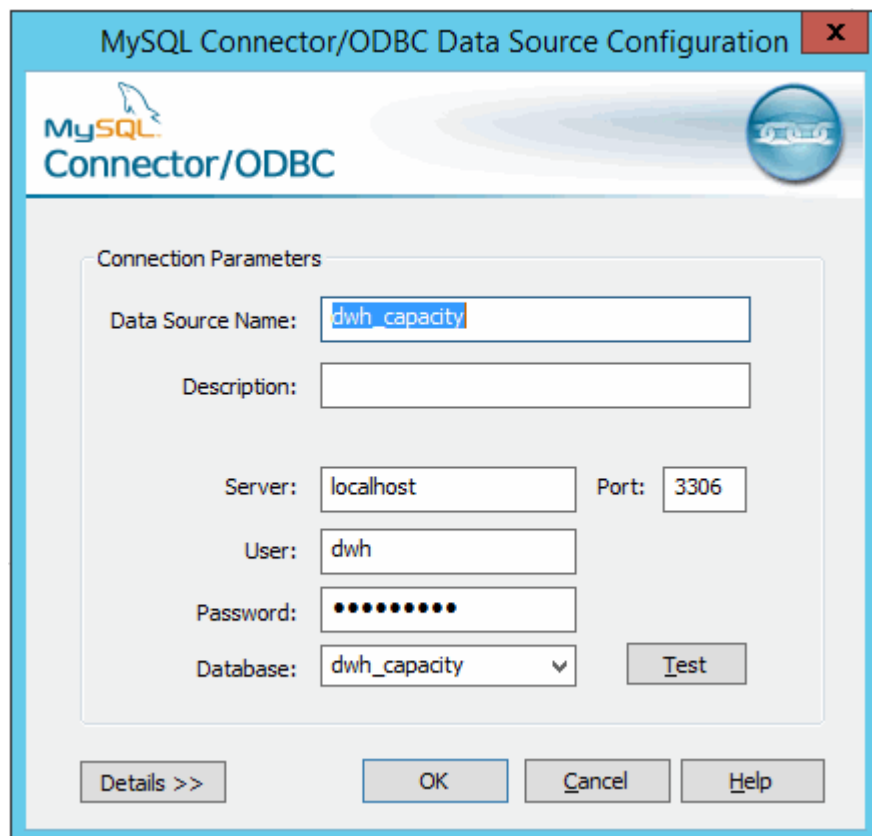
### 3. Haga clic en **DSN de sistema**

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**.

## Compatibilidad con el inicio de sesión de la tarjeta inteligente y el certificado

OnCommand Insight admite el uso de tarjetas inteligentes (CAC) y certificados para autenticar a los usuarios que inician sesión en los servidores de Insight. Debe configurar el sistema para habilitar estas funciones.

Después de configurar el sistema para que admita CAC y certificados, desplazarse a una nueva sesión de OnCommand Insight da como resultado que el explorador muestre un cuadro de diálogo nativo, proporcionando al usuario una lista de certificados personales entre los que elegir. Estos certificados se filtran en función del conjunto de certificados personales emitidos por entidades emisoras de certificados de confianza del servidor OnCommand Insight. La mayoría de las veces, existe una única opción. De forma predeterminada, Internet Explorer omite este cuadro de diálogo si sólo hay una opción.



Para los usuarios de CAC, las tarjetas inteligentes contienen varios certificados, sólo uno de los cuales puede coincidir con la CA de confianza. El certificado CAC para *identification* debe utilizarse.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Configuración de hosts para el inicio de sesión de tarjeta inteligente y certificado

Debe realizar modificaciones en la configuración del host de OnCommand Insight para admitir la tarjeta inteligente (CAC) y los inicios de sesión de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el ID de un usuario.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Pasos

1. Utilice la regedit utilidad para modificar los valores del registro en  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java:
  - a. Cambie la JVM\_OPTION DclientAuth=false para DclientAuth=true.



2. Realice una copia de seguridad del archivo keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Abra un símbolo del sistema especificando Run as administrator
4. Elimine el certificado autofirmado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Genere un nuevo certificado: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Genere una solicitud de firma de certificación (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Una vez que se devuelva la CSR en el paso 6, importe el certificado y exporte el certificado en formato base-64 y colóquelo "C:\temp" named servername.cer.
8. Extraiga el certificado del almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extraiga una clave privada del archivo p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Fusione el certificado base-64 exportado en el paso 7 con la clave privada: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importe el certificado combinado al almacén de claves: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importe el certificado raíz: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importe el certificado raíz al servidor.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Importe el certificado intermedio: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

Repita este paso con todos los certificados intermedios.

15. Especifique el dominio en LDAP para que coincida con este ejemplo.

16. Reinicie el servidor.

## Configuración de un cliente para que admita el inicio de sesión de tarjeta inteligente y certificado

Las máquinas cliente requieren middleware y modificaciones a los exploradores para permitir el uso de tarjetas inteligentes y para el inicio de sesión de certificados. Los clientes que ya utilizan tarjetas inteligentes no deben requerir modificaciones adicionales en sus equipos cliente.

### Antes de empezar



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Acerca de esta tarea

A continuación se enumeran los requisitos comunes de configuración del cliente:

- Instalación de Smart Card middleware, como ActivClient (consulte
- Modificación del explorador de IE (consulte
- Modificación del navegador Firefox (consulte

## Activación de CAC en un servidor Linux

Se necesitan algunas modificaciones para habilitar CAC en un servidor OnCommand Insight de Linux.

### Pasos

1. Vaya a. `/opt/netapp/oci/conf/`
2. Editar `wildfly.properties` y cambie el valor de `CLIENT_AUTH_ENABLED` A "Verdadero"
3. Importe el «'certificado raíz» que existe en  
`/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`

#### 4. Reinicie el servidor

## Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.
- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)



### Pasos

#### 1. Utilice regedit para modificar los valores del Registro en

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. Cambie la JVM\_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

#### 2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

- a. En una ventana de comandos, vaya a `..\SANscreen\wildfly\standalone\configuration`.
- b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

La primera palabra de cada línea indica el alias de CA.

- c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un .pem archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a.
- ```
..\SANscreen\wildfly\standalone\configuration y utilice la keytool comando de importación: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
```

Mi\_alias es normalmente un alias que fácilmente identificaría la CA enkeytool -list funcionamiento.

3. En el servidor OnCommand Insight, el wildfly/standalone/configuration/standalone-full.xml El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en /subsystem=undertow/server=default-server/https-listener=default-httpsPara activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

| SO      | Guión                                                               |
|---------|---------------------------------------------------------------------|
| Windows | <install<br>dir>\SANscreen\wilfly\bin\enableCACforRemoteEJB<br>.bat |
| Linux   | /Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB.sh                 |

Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecuten OnCommand Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\jre\bin\keytool.exe`

```
-list -keystore CAMKeystore.jks -storepass NoPassWordSet
```

La primera palabra de cada línea indica el alias de CA.

c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.

d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\.
```

e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\jre\bin\keytool.exe`

```
-importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem'  
-v -trustcacerts
```

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

g. Responda `yes` cuando se le solicite que confíe en el certificado.

2. Para activar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. Para desactivar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para

el servidor Cognos.

## Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass`

```
NoPassWordSet
```

La primera palabra de cada línea indica el alias de CA.

c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.

d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\.
```

e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

g. Responda `yes` cuando se le solicite que confíe en el certificado.

2. Para activar el modo CAC, realizar lo siguiente:

a. Configure la página salir de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos\_admin)
- (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
- (Sólo para 7.3.10 y 7.3.11) Introduzca cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

3. Para desactivar el modo CAC, realizar lo siguiente:

a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.

c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos\_admin)
- Haga clic en Administrar -> Configuración -> sistema -> Seguridad
- Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
- Cierre el navegador.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

### Antes de empezar

Este procedimiento se aplica a sistemas que ejecutan OnCommand Insight 7.3.5 a 7.3.9.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

### Pasos

1. Cree un backup de `..\SANSscreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANSscreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Envíe el `encryptRequest.csr` a la entidad de certificación (CA) para obtener un certificado SSL.

Asegúrese de agregar atributos adicionales como "TAN:dns=FQDN (por ejemplo, hostname.netapp.com)" para agregar SubjectAltName. Google Chrome versión 58 y posteriores se queja si falta SubjectAltName en el certificado.

6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 al 8 c para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `Intermediate.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `root.cer` con el Bloc de notas y guarde el contenido de 9a.
  - c. Guarde el archivo como `CA.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer`



Esto establecerá CA.cer como entidad emisora de certificados raíz.

c. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

Esto establecerá Cognos.cer como certificado de cifrado firmado por CA.cer.

11. Abra la configuración de IBM Cognos.
  - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
  - b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -exportcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\cognos\analítica\Configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoWordSet -alias cifrado
13. Importe "c:\temp\cognos.crt" en dwh truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -importcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\wiland\autónoma\Configuration\Server.trustore" -storeprechrit -alias cognoscert
14. Reinicie el servicio SANscreen.
15. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

## Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANSscreen\cognos\analytics\configuration y..`  
`..\SANSscreen\cognos\analytics\temp\cam\freshness` carpetas.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress".` Nota: Aquí -H y -i van a agregar `subjectAltNames` como `dns` e `ipaddress`.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido `encryptRequest.csr` y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7  
  
Esto descargará el archivo `fqdn.p7b`
7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en `"Extensiones de shell de cifrado"`.
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `root.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `Intermediate.cer` con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
  - c. Guarde el archivo como `chain.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer`
  - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer`

- d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Abra la configuración de IBM Cognos.
    - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
    - b. Cambiar «¿utilizar CA de terceros?» Para True.
    - c. Guarde la configuración.
    - d. Reinicie Cognos
  12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    - a. cd "C:\Archivos de programa\SANscreen"
    - b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analítica\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias cifrado
  13. Haga una copia de seguridad del servidor de seguridad DWH  
en. .\SANscreen\wildfly\standalone\configuration\server.trustore
  14. Importe "c:\temp\cognos.crt" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    - a. cd "C:\Archivos de programa\SANscreen"
    - b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore willose\reasons\configuration\server.trustore -storepass chretosca -alias cognos3rdca
  15. Reinicie el servicio SANscreen.
  16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
  17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.
    - a. cd "%SANSSCREEN\_HOME%cognos\analytics\bin\"
    - b. "%SANSSCREEN\_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN\_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"
    - c. ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"

Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Configuración del almacén de datos para el inicio de sesión de la tarjeta inteligente y el certificado

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con las conexiones de tarjeta inteligente (CAC) y de certificados.

### Antes de empezar

- LDAP debe estar habilitado en el sistema.

- El LDAP User principal account name El atributo debe coincidir con el campo LDAP que contiene el número de ID de gobierno de un usuario.

El nombre común (CN) almacenado en los CAC emitidos por el gobierno suele estar en el siguiente formato: `first.last.ID`. Para algunos campos LDAP, como `sAMAccountName`, este formato es demasiado largo. En estos campos, OnCommand Insight extrae sólo el número de ID del sistema nervioso central.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Utilice regedit para modificar los valores del Registro en

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. Cambie la JVM\_OPTION `-DclientAuth=false` para `-DclientAuth=true`.

Para Linux, modifique el `clientAuth` parámetro in `/opt/netapp/oci/scripts/wildfly.server`

2. Agregue las entidades emisoras de certificados (CA) al almacén de datos de trueque:

- a. En una ventana de comandos, vaya a `..\SANscreen\wildfly\standalone\configuration`.

- b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

La primera palabra de cada línea indica el alias de CA.

- c. Si es necesario, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo. Para incluir las CA del cliente con las CA de confianza de Data Warehouse vaya a

```
..\SANscreen\wildfly\standalone\configuration y utilice la keytool comando de
importación: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert
-keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v
-trustcacerts
```

Mi\_alias es normalmente un alias que fácilmente identificaría la CA en `keytool -list` funcionamiento.

3. En el servidor OnCommand Insight, el `wildfly/standalone/configuration/standalone-full.xml` El archivo debe modificarse actualizando el cliente de verificación a "SOLICITADO" en `/subsystem=undertow/server=default-server/https-listener=default-https` Para activar CAC. Inicie sesión en el servidor de Insight y ejecute el comando adecuado:

| SO      | Guión                                                                                    |
|---------|------------------------------------------------------------------------------------------|
| Windows | <code>&lt;install<br/>dir&gt;\SANscreen\wilfly\bin\enableCACforRemoteEJB<br/>.bat</code> |
| Linux   | <code>/Opt/netapp/oci/wiland/bin/enableCACforRemoteEJB<br/>.sh</code>                    |

Después de ejecutar la secuencia de comandos, espere hasta que se complete la recarga del servidor de wilfly antes de continuar con el siguiente paso.

4. Reinicie el servidor OnCommand Insight.

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.5 a 7.3.9)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecuten OnCommand Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

1. Agregue las autoridades de certificación (CA) al almacén de Cognos.
  - a. En una ventana de comandos, vaya a.  
`..\SANscreen\cognos\analytics\configuration\certs\`
  - b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`  
  
La primera palabra de cada línea indica el alias de CA.
  - c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.
  - d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.  
`..\SANscreen\cognos\analytics\configuration\certs\`
  - e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`  
  
`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.
  - f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.
  - g. Responda `yes` cuando se le solicite que confíe en el certificado.
2. Para activar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Para desactivar el modo CAC, ejecute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

## Configuración de Cognos para el inicio de sesión con tarjeta inteligente y certificado (OnCommand Insight 7.3.10 y posterior)

Debe modificar la configuración del almacén de datos de OnCommand Insight para que sea compatible con la tarjeta inteligente (CAC) y los inicios de sesión del certificado para el servidor Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Pasos

### 1. Agregue las autoridades de certificación (CA) al almacén de Cognos.

#### a. En una ventana de comandos, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

#### b. Utilice la `keytool` Utilidad para enumerar las CA de confianza: `..\..\ibm-`

```
jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass  
NoPassWordSet
```

La primera palabra de cada línea indica el alias de CA.

#### c. Si no existen archivos adecuados, proporcione un archivo de certificado de CA, normalmente un `.pem` archivo.

#### d. Para incluir las CA del cliente con CA de confianza OnCommand Insight, vaya a.

```
..\SANscreen\cognos\analytics\configuration\certs\
```

#### e. Utilice la `keytool` utilidad para importar `.pem` archivo: `..\..\ibm-jre\jre\bin\keytool.exe` `-importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem'` `-v -trustcacerts`

`my_alias` Normalmente es un alias que identificaría fácilmente la CA en `keytool -list` funcionamiento.

#### f. Cuando se le pida una contraseña, introduzca `NoPassWordSet`.

#### g. Responda `yes` cuando se le solicite que confíe en el certificado.

### 2. Para activar el modo CAC, realizar lo siguiente:

#### a. Configure la página salir de CAC siguiendo los pasos siguientes:

- Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, `cognos_admin`)
- (Sólo para 7.3.10 y 7.3.11) haga clic en Administrar -> Configuración -> sistema -> Seguridad
- (Sólo para 7.3.10 y 7.3.11) Introduzca `cacLogout.html` con la URL de redireccionamiento de cierre de sesión -> aplicar

- Cierre el navegador.
  - b. Ejecución `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
  - c. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
3. Para desactivar el modo CAC, realizar lo siguiente:
- a. Ejecución `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
  - b. Inicie el servicio IBM Cognos. Espere a que se inicie el servicio Cognos.
  - c. (Sólo para 7.3.10 y 7.3.11) desconfigure la página de cierre de sesión de CAC siguiendo los pasos siguientes:
    - Iniciar sesión en el portal de Cognos (el usuario debe formar parte del grupo de administradores del sistema, es decir, cognos\_admin)
    - Haga clic en Administrar -> Configuración -> sistema -> Seguridad
    - Escriba cacLogout.html con la URL de redireccionamiento de cierre de sesión -> aplicar
    - Cierre el navegador.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.5 a 7.3.9)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

### Antes de empezar

Este procedimiento se aplica a sistemas que ejecutan OnCommny Insight 7.3.5 a 7.3.9.

Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):



- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnComand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

### Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.



## Pasos

1. Cree un backup de `..\SANSscreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANSscreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Envíe el `encryptRequest.csr` a la entidad de certificación (CA) para obtener un certificado SSL.

Asegúrese de agregar atributos adicionales como "TAN:dns=FQDN (por ejemplo, hostname.netapp.com)" para agregar SubjectAltName. Google Chrome versión 58 y posteriores se queja si falta SubjectAltName en el certificado.

6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7

Esto descargará el archivo `fqdn.p7b`

7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 al 8 c para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `Intermediate.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `root.cer` con el Bloc de notas y guarde el contenido de 9a.
  - c. Guarde el archivo como `CA.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer`  
  
Esto establecerá `CA.cer` como entidad emisora de certificados raíz.
  - c. `ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`

Esto establecerá Cognos.cer como certificado de cifrado firmado por CA.cer.

11. Abra la configuración de IBM Cognos.
  - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
  - b. Cambiar «¿utilizar CA de terceros?» Para True.
  - c. Guarde la configuración.
  - d. Reinicie Cognos
12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -exportcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\cognos\analítica\Configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoWordSet -alias cifrado
13. Importe "c:\temp\cognos.crt" en dwh truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
  - a. "D:\Archivos de programa\SANscreen\java\bin\keytool.exe" -importcert -file "c:\temp\cognos.crt" -keystore "D:\Archivos de programa\SANscreen\wiland\autónoma\Configuration\Server.trustore" -storeprechrit -alias cognoscrt
14. Reinicie el servicio SANscreen.
15. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.

## Importación de certificados SSL firmados por CA para Cognos y DWH (Insight 7.3.10 y posterior)

Puede agregar certificados SSL para habilitar la autenticación y el cifrado mejorados para su entorno de Data Warehouse y Cognos.

### Antes de empezar

Este procedimiento es para sistemas que ejecutan OnCommand Insight 7.3.10 y versiones posteriores.



Para obtener las instrucciones más actualizadas del CAC y del certificado, consulte los siguientes artículos de la base de conocimientos (se requiere inicio de sesión de asistencia técnica):

- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para OnCommand Insight"](#)
- ["Cómo configurar la autenticación de la tarjeta de acceso común \(CAC\) para el almacén de datos de OnCommand Insight"](#)
- ["Cómo crear e importar un certificado firmado de entidad de certificación \(CA\) en OnCommand Insight y almacén de datos OnCommand Insight 7.3.x."](#)
- ["Cómo crear un certificado autofirmado en OnCommand Insight 7.3.X instalado en un host de Windows"](#)
- ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Acerca de esta tarea

Debe tener privilegios de administrador para realizar este procedimiento.

## Pasos

1. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANSscreen\cognos\analytics\configuration y..`  
`..\SANSscreen\cognos\analytics\temp\cam\freshness carpetas.`
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
  - a. `cd "\Program Files\sansscreen\cognos\analytics\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress".` Nota: Aquí -H y -i van a agregar `subjectAltNames` como `dns` e `ipaddress`.
4. Abra el `c:\temp\encryptRequest.csr` archiva y copia el contenido generado.
5. Introduzca el contenido `encryptRequest.csr` y genere un certificado mediante el portal de firma de CA.
6. Descargue los certificados de cadena incluyendo el certificado raíz utilizando el formato PKCS7  
  
Esto descargará el archivo `fqdn.p7b`
7. Obtenga un certificado en formato `.p7b` de la CA. Utilice un nombre que lo marque como el certificado del servidor web Cognos.
8. `ThirdPartyCertificateTool.bat` no puede importar la cadena completa, de modo que se necesitan varios pasos para exportar todos los certificados. Divida la cadena exportándolos individualmente de la siguiente manera:
  - a. Abra el certificado `.p7b` en "Extensiones de shell de cifrado".
  - b. Navegue en el panel izquierdo hasta «'certificados'».
  - c. Haga clic con el botón derecho del ratón en la CA raíz > todas las tareas > Exportar.
  - d. Seleccione salida Base64.
  - e. Introduzca un nombre de archivo que lo identifique como certificado raíz.
  - f. Repita los pasos del 8 a al 8 e para exportar todos los certificados por separado en archivos `.cer`.
  - g. Asigne un nombre a los archivos `intermediateX.cer` y `cognos.cer`.
9. Ignore este paso si sólo tiene un certificado de CA, de lo contrario, combine `root.cer` y `intermediateX.cer` en un archivo.
  - a. Abra `root.cer` con el Bloc de notas y copie el contenido.
  - b. Abra `Intermediate.cer` con el Bloc de notas y anexe el contenido de 9a (primero intermedio y raíz siguiente).
  - c. Guarde el archivo como `chain.cer`.
10. Importe los certificados al almacén de claves de Cognos mediante el símbolo del sistema Admin CMD:
  - a. `cd "Archivos de programa\sansscreen\cognos\analítica\bin"`
  - b. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer`
  - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer`

- d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Abra la configuración de IBM Cognos.
    - a. Seleccione Configuración local → Seguridad → Criptografía → Cognos
    - b. Cambiar «¿utilizar CA de terceros?» Para True.
    - c. Guarde la configuración.
    - d. Reinicie Cognos
  12. Exporte el último certificado Cognos a cognos.crt utilizando el indicador de administración CMD:
    - a. cd "C:\Archivos de programa\SANscreen"
    - b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analítica\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias cifrado
  13. Haga una copia de seguridad del servidor de seguridad DWH  
en. .\SANscreen\wildfly\standalone\configuration\server.trustore
  14. Importe "c:\temp\cognos.crt" en DWH truStore para establecer la comunicación SSL entre Cognos y DWH, mediante la ventana de indicación Admin CMD.
    - a. cd "C:\Archivos de programa\SANscreen"
    - b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore willose\reasons\configuration\server.trustore -storepass chretosca -alias cognos3rdca
  15. Reinicie el servicio SANscreen.
  16. Realice una copia de seguridad de DWH para asegurarse de que DWH se comunica con Cognos.
  17. Los siguientes pasos deben realizarse incluso cuando sólo se cambia el "certificado de I" y los certificados de Cognos predeterminados no se modifican. De lo contrario, Cognos puede quejarse del nuevo certificado SANscreen o no puede crear una copia de seguridad DWH.
    - a. cd "%SANSSCREEN\_HOME%cognos\analytics\bin\"
    - b. "%SANSSCREEN\_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN\_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"
    - c. ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"

Por lo general, estos pasos se realizan como parte del proceso de importación de certificados Cognos descrito en ["Cómo importar un certificado firmado por Cognos Certificate Authority \(CA\) en OnCommand DataWarehouse 7.3.3 y posterior"](#)

## Importación de certificados SSL

Puede añadir certificados SSL para habilitar la autenticación y el cifrado mejorados a fin de mejorar la seguridad del entorno de OnCommand Insight.

### Antes de empezar

Debe asegurarse de que el sistema cumple el nivel de bit mínimo requerido (1024 bits).

## Acerca de esta tarea



Antes de intentar realizar este procedimiento, debe realizar una copia de seguridad de la existente `server.keystore` y asigne un nombre a la copia de seguridad `server.keystore.old`. Corromper o dañar el `server.keystore` El archivo puede resultar en un servidor Insight inoperable después de reiniciar el servidor Insight. Si crea una copia de seguridad, puede revertir al archivo antiguo si se producen problemas.

## Pasos

1. Cree una copia del archivo original del almacén de claves: 

```
cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old"
```
2. Enumere el contenido del almacén de claves: 

```
C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"
```

  - a. Cuando se le pida una contraseña, introduzca `changeit`.

El sistema muestra el contenido del almacén de claves. Debe haber al menos un certificado en el almacén de claves, `"ssl certificate"`.
3. Elimine el `"ssl certificate"`: 

```
keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
```
4. Genere una nueva clave: 

```
C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"
```

  - a. Cuando se le soliciten los nombres y apellidos, introduzca el nombre de dominio completo (FQDN) que desee utilizar.
  - b. Proporcione la siguiente información acerca de la organización y la estructura de su organización:
    - País: Abreviatura ISO de dos letras para su país (por ejemplo, US)
    - Estado o provincia: Nombre del estado o provincia donde está ubicada la oficina central de su organización (por ejemplo, Massachusetts)
    - Localidad: Nombre de la ciudad donde está ubicada la oficina central de su organización (por ejemplo, Waltham)
    - Nombre organizativo: Nombre de la organización a la que se pertenece el nombre de dominio (por ejemplo, NetApp).
    - Nombre de la unidad organizativa: Nombre del departamento o grupo que utilizará el certificado (por ejemplo, Soporte)
    - Nombre de dominio/ Nombre común: El FQDN que se utiliza para las búsquedas DNS de su servidor (por ejemplo, `www.example.com`) el sistema responde con información similar a la siguiente: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
  - c. Introduzca `Yes` Cuando el nombre común (CN) es igual al FQDN.
  - d. Al solicitar la contraseña clave, introduzca la contraseña o pulse la tecla `Intro` para usar la contraseña del almacén de claves existente.

5. Generar un archivo de solicitud de certificado: C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr

La c:\localhost.csr archivo es el archivo de solicitud de certificado que se acaba de generar.

6. Envíe el c:\localhost.csr Archivar a la entidad emisora de certificados (CA) para su aprobación.

Una vez aprobado el archivo de solicitud de certificado, desea que se le devuelva el certificado .der formato. Es posible que el archivo no se devuelva como a. .der archivo. El formato de archivo predeterminado es .cer Para los servicios de CA de Microsoft.

Las CA de la mayoría de las organizaciones utilizan una cadena de modelo de confianza, incluida una CA raíz, que a menudo se encuentra sin conexión. Ha firmado los certificados para sólo algunas CA secundarias, conocidas como CA intermedias.

Debe obtener la clave pública (certificados) para toda la cadena de confianza: El certificado de la CA que firmó el certificado para el servidor OnCommand Insight, y todos los certificados entre esa CA firmada hasta la CA raíz de la organización y hasta ella.

En algunas organizaciones, al enviar una solicitud de firma, es posible que reciba una de las siguientes opciones:

- Archivo PKCS12 que contiene el certificado firmado y todos los certificados públicos de la cadena de confianza
- A. .zip archivo que contiene archivos individuales (incluido el certificado firmado) y todos los certificados públicos de la cadena de confianza
- Solo el certificado firmado

Debe obtener los certificados públicos.

7. Importe el certificado aprobado para Server.keystore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"

- a. Al solicitar, introduzca la contraseña del almacén de claves.

Se muestra el siguiente mensaje: Certificate reply was installed in keystore

8. Importe el certificado aprobado para Server.trustore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"

- a. Cuando se le solicite, introduzca la contraseña de trusted.

Se muestra el siguiente mensaje: Certificate reply was installed in trustore

9. Edite el SANscreen\wildfly\standalone\configuration\standalone-full.xml archivo:

Sustituya la siguiente cadena de alias: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Por ejemplo:

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"
keystore-password="{VAULT::HttpsRealm::keystore_password:1}" alias="cbc-oci-
02.muccbc.hq.netapp.com" key-
password="{VAULT::HttpsRealm::key_password:1}"/>
```

#### 10. Reinicie el servicio del servidor SANscreen.

Una vez que Insight esté en funcionamiento, puede hacer clic en el icono de candado para ver los certificados instalados en el sistema.

Si ve un certificado que contiene información "emitida a" que coincide con la información "emitida por", todavía tiene instalado un certificado autofirmado. Los certificados autofirmados generados por el instalador de Insight tienen un vencimiento de 100 años.

NetApp no puede garantizar que este procedimiento elimine las advertencias de certificado digitales. NetApp no puede controlar el modo en que se han configurado las estaciones de trabajo de los usuarios finales. Considere los siguientes casos:

- Microsoft Internet Explorer y Google Chrome utilizan las funciones de certificado nativo de Microsoft en Windows.

Esto significa que si los administradores de Active Directory presionan los certificados de CA de su empresa en los almacenes de certificados del usuario final, los usuarios de estos exploradores verán que desaparecen las advertencias de certificado cuando los certificados autofirmados de OnCommand Insight se han reemplazado por los firmados por la infraestructura de CA interna.

- Java y Mozilla Firefox tienen sus propios almacenes de certificados.

Si los administradores del sistema no automatizan la ingestión de certificados de CA en los almacenes de certificados de confianza de estas aplicaciones, el uso del navegador Firefox puede continuar generando advertencias de certificados debido a un certificado que no es de confianza, incluso cuando el certificado autofirmado se haya reemplazado. Conseguir que la cadena de certificados de su empresa esté instalada en el almacén de verdad es un requisito adicional.

## La jerarquía de entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular.

En OnCommand Insight, la jerarquía de entidades de negocio contiene estos niveles:

- **El cliente** se utiliza principalmente por los proveedores de servicios para asociar recursos con un cliente, por ejemplo, NetApp.
- **Línea de negocio (LOB)** es una línea de negocio o línea de producto dentro de una compañía, por ejemplo, almacenamiento de datos.
- **Unidad de Negocio** representa una unidad de negocio tradicional como Legal o Marketing.
- **El proyecto** se utiliza a menudo para identificar un proyecto específico dentro de una unidad de negocio para la cual usted desea el pago por uso de capacidad. Por ejemplo, "Patentes" puede ser un nombre de proyecto para la unidad de negocio Legal y "Eventos de ventas" puede ser un nombre de proyecto para la unidad de negocio de marketing. Tenga en cuenta que los nombres de nivel pueden incluir espacios.

No es necesario que utilice todos los niveles en el diseño de la jerarquía corporativa.

## Diseño de la jerarquía de entidades de negocio

Debe comprender los elementos de la estructura corporativa y lo que debe representar en las entidades de negocio porque se convierten en una estructura fija en su base de datos de OnCommand Insight. Puede utilizar la siguiente información para configurar las entidades de negocio. Recuerde que no es necesario utilizar todos los niveles de jerarquía para recopilar datos en estas categorías.

### Pasos

1. Examine cada nivel de la jerarquía de entidades de negocio para determinar si ese nivel debe incluirse en la jerarquía de entidades de negocio de su empresa:
  - **El nivel de inquilino** es necesario si su empresa es un ISP y desea hacer un seguimiento del uso de los recursos por parte del cliente.
  - **La línea de negocio (LOB)** es necesaria en la jerarquía si es necesario hacer un seguimiento de los datos de las diferentes líneas de producto.
  - **La unidad de negocio** es necesaria si necesita realizar un seguimiento de los datos de diferentes departamentos. Este nivel de la jerarquía suele ser valioso para separar un recurso que un departamento utiliza que otros departamentos no.
  - **El nivel de proyecto** se puede utilizar para trabajos especializados dentro de un departamento. Estos datos pueden ser útiles para determinar, definir y supervisar las necesidades tecnológicas de un proyecto independiente en comparación con otros proyectos de una empresa o departamento.
2. Cree un gráfico que muestre cada entidad de negocio con los nombres de todos los niveles dentro de la entidad.
3. Compruebe los nombres en la jerarquía para estar seguros de que serán explicativos en las vistas e informes de OnCommand Insight.
4. Identificar todas las aplicaciones que están asociadas con cada entidad de negocio.

## Creación de entidades de negocio

Después de diseñar la jerarquía de entidades de negocio para la empresa, puede configurar aplicaciones y, a continuación, asociar las entidades de negocio con las aplicaciones. Este proceso crea la estructura de entidades de negocio en la base de datos de OnCommand Insight.

### Acerca de esta tarea

Asociar aplicaciones con entidades de negocio es opcional; sin embargo, es una práctica recomendada.

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **entidades empresariales**.

Aparece la página entidades de negocio.



3. Haga clic en  para empezar a construir una nueva entidad.

Aparece el cuadro de diálogo **Agregar entidad de negocio**.

4. Para cada nivel de entidad (inquilino, línea de negocio, Unidad de negocio y proyecto), puede realizar cualquiera de las siguientes acciones:
  - Haga clic en la lista nivel de entidad y seleccione un valor.
  - Escriba un nuevo valor y pulse Intro.
  - Deje el valor de nivel de entidad como N/A si no desea utilizar el nivel de entidad para la entidad de negocio.
5. Haga clic en **Guardar**.

## Asignar entidades de negocio a activos

Es posible asignar una entidad de negocio a un activo (host, puerto, almacenamiento, switch, máquina virtual, qtree, share, volume o internal volume) sin haber asociado la entidad comercial a una aplicación; sin embargo, las entidades comerciales se asignan automáticamente a un activo si dicho activo está asociado con una aplicación relacionada con una entidad empresarial.



### Antes de empezar

Debe haber creado ya una entidad de negocio.

### Acerca de esta tarea

Si bien puede asignar entidades de negocio directamente a activos, se recomienda asignar aplicaciones a activos y, a continuación, asignar entidades de negocio a activos.


### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la entidad de negocio realizando una de las siguientes acciones:
  - Haga clic en el activo en el panel de activos.
  - Haga clic en  En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
3. En la sección **datos de usuario** de la página de activos, sitúe el cursor sobre **Ninguno** junto a **entidades de negocio** y, a continuación, haga clic en .

Se muestra la lista de entidades de negocio disponibles.

4. Escriba el cuadro **Buscar** para filtrar la lista de una entidad específica o desplácese hacia abajo por la lista; seleccione una entidad comercial de la lista.

Si la entidad de negocio que elija está asociada a una aplicación, se mostrará el nombre de la aplicación. En este caso, aparece la palabra "derived" junto al nombre de la entidad de negocio. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

5. Para reemplazar una aplicación derivada de una entidad de negocio, coloque el cursor sobre el nombre de la aplicación y haga clic en  , seleccione otra entidad de negocio y seleccione otra aplicación de la lista.


## Asignar entidades de negocio a o eliminar entidades de negocio de varios activos

Puede asignar entidades de negocio a o quitar entidades de negocio de varios activos utilizando una consulta en lugar de tener que asignarlas o eliminarlas manualmente.


### Antes de empezar

Debe haber creado ya las entidades de negocio que desea agregar a los activos deseados.


### Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Si lo desea, puede filtrar los activos a los que desea agregar entidades de negocio.
3. Seleccione los activos deseados en la lista o haga clic en  ▼ Para seleccionar **todo**.

Aparece el botón **acciones**.

4. Para agregar una entidad de negocio a los activos seleccionados, haga clic en  . Si el tipo de activo seleccionado puede tener entidades de negocio asignadas a él, verá la opción de menú a **Agregar entidad de negocio**. Seleccione esto.
5. Seleccione la entidad comercial deseada de la lista y haga clic en **Guardar**.

Cualquier nueva entidad de negocio que asigne reemplazará a cualquier entidad de negocio que ya se haya asignado al activo. La asignación de aplicaciones a activos también anulará las entidades de negocio asignadas de la misma manera. La asignación de entidades de negocio a como activo también puede reemplazar cualquier aplicación asignada a ese activo.

6. Para eliminar una entidad de negocio asignada a los activos, haga clic en  Y seleccione **Quitar entidad de negocio**.
7. Seleccione la entidad de negocio deseada de la lista y haga clic en **Eliminar**.

## Definición de anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos según sus requisitos corporativos, puede definir las anotaciones especializadas que necesite para tener una imagen completa de sus datos, como, por ejemplo, el fin de vida de los activos, el centro de datos, la creación de ubicaciones, el nivel de almacenamiento o el volumen. y el nivel de servicio del volumen interno.

### Pasos

1. Enumere cualquier terminología del sector a la que deben asociarse los datos del entorno.
2. Enumere la terminología corporativa a la que deben asociarse los datos de entorno, que no se está realizando un seguimiento utilizando las entidades de negocio.

3. Identifique los tipos de anotaciones predeterminados que pueda utilizar.
4. Identifique qué anotaciones personalizadas debe crear.

## Uso de anotaciones para supervisar su entorno

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. Por ejemplo, puede anotar los activos con información como finalización de la vida útil de los activos, centro de datos, ubicación del edificio, nivel de almacenamiento o nivel de servicio de volumen.

El uso de anotaciones para supervisar su entorno incluye las siguientes tareas de alto nivel:

- Crear o editar definiciones para todos los tipos de anotaciones.
- Mostrar páginas de activos y asociar cada activo con una o varias anotaciones.

Por ejemplo, si un activo se está arrendando y el arrendamiento caduca dentro de dos meses, puede que desee aplicar una anotación de fin de vida al activo. Esto ayuda a evitar que otros utilicen ese activo durante un tiempo prolongado.

- Crear reglas para aplicar anotaciones automáticamente a varios activos del mismo tipo.
- Utilizar la utilidad de importación de anotaciones para importar anotaciones.
- Filtrar activos por sus anotaciones.
- Agrupación de datos en informes basada en anotaciones y generación de dichos informes.

Consulte la *Guía de informes de OnCommand Insight* para obtener más información acerca de los informes.

## Gestión de tipos de anotaciones

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados, como el ciclo de vida de los activos (cumpleaños o fin de vida), la ubicación del centro de datos o edificio y la capa, que puede personalizar para que aparezcan en los informes. Puede definir valores para tipos de anotaciones predeterminados o crear sus propios tipos de anotaciones personalizadas. Posteriormente, puede editar esos valores.

### Tipos de anotaciones predeterminados

OnCommand Insight proporciona algunos tipos de anotaciones predeterminados. Estas anotaciones se pueden utilizar para filtrar o agrupar datos y filtrar los informes de datos.

Puede asociar activos con tipos de anotación predeterminados como los siguientes:

- Ciclo de vida de los activos, como cumpleaños, puesta de sol o fin de vida
- Información sobre la ubicación de un dispositivo, como un centro de datos, un edificio o un piso
- Clasificación de activos, como por calidad (niveles), por dispositivos conectados (nivel de switch) o por nivel de servicio

- Estado, como caliente (alta utilización)

En la siguiente tabla se enumeran los tipos de anotaciones predeterminados. Puede editar cualquiera de estos nombres de anotaciones según sus necesidades.

| Tipos de anotaciones           | Descripción                                                                                                                 | Tipo     |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------|
| Alias                          | Nombre sencillo para un recurso.                                                                                            | Texto    |
| Cumpleaños                     | Fecha en la que el dispositivo estaba o se pondrá en línea.                                                                 | Fecha    |
| Edificio                       | Ubicación física de recursos de host, almacenamiento, switch y cinta.                                                       | Lista    |
| Ciudad                         | Ubicación municipal de recursos de host, almacenamiento, switch y cinta.                                                    | Lista    |
| Grupo de recursos informáticos | Asignación de grupos utilizada por el origen de datos de sistemas de archivos del host y del equipo virtual.                | Lista    |
| Continente                     | Ubicación geográfica de recursos de host, almacenamiento, switch y cinta.                                                   | Lista    |
| País                           | Ubicación nacional de recursos de host, almacenamiento, switch y cinta.                                                     | Lista    |
| Centro de datos                | La ubicación física del recurso y está disponible para hosts, cabinas de almacenamiento, switches y cintas.                 | Lista    |
| Conexión directa               | Indica (Sí o no) si un recurso de almacenamiento está conectado directamente a los hosts.                                   | Booleano |
| Fin de la vida                 | Fecha en la que se desconecta un dispositivo, por ejemplo, si el arrendamiento ha caducado o se está retirando el hardware. | Fecha    |
| Alias de estructura            | Nombre sencillo para un tejido.                                                                                             | Texto    |

|                   |                                                                                                                                                                                                                                                                    |          |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| Piso              | Ubicación de un dispositivo en la planta de un edificio. Se pueden definir para hosts, cabinas de almacenamiento, switches y cintas.                                                                                                                               | Lista    |
| Caliente          | Dispositivos que ya están en uso pesado regularmente o en el umbral de capacidad.                                                                                                                                                                                  | Booleano |
| Nota              | Comentarios que desea asociar a un recurso.                                                                                                                                                                                                                        | Texto    |
| Rack              | Rack en el que reside el recurso.                                                                                                                                                                                                                                  | Texto    |
| Habitación        | Sala en un edificio u otra ubicación de recursos de host, almacenamiento, switch y cinta.                                                                                                                                                                          | Lista    |
| SAN               | Partición lógica de la red. Disponible en hosts, cabinas de almacenamiento, cintas, switches y aplicaciones.                                                                                                                                                       | Lista    |
| Nivel de servicio | Un conjunto de niveles de servicio compatibles que puede asignar a recursos. Proporciona una lista de opciones ordenadas para volúmenes internos, qtrees y volúmenes. Editar niveles de servicio para establecer políticas de rendimiento para diferentes niveles. | Lista    |
| Estado/provincia  | Estado o provincia en la que se encuentra el recurso.                                                                                                                                                                                                              | Lista    |
| Puesta de sol     | Límite establecido después del cual no se puede realizar ninguna asignación nueva a ese dispositivo. Útil para migraciones planificadas y otros cambios de red pendientes.                                                                                         | Fecha    |

|                           |                                                                                                                                                                                                                                                                                                                         |       |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Cambiar el nivel          | Incluye opciones predefinidas para configurar categorías de conmutadores. Normalmente, estas designaciones permanecen durante toda la vida útil del dispositivo, aunque puede modificarlas, si es necesario. Sólo disponible para interruptores.                                                                        | Lista |
| Nivel                     | Puede utilizarse para definir distintos niveles de servicio dentro de su entorno. Los niveles pueden definir el tipo de nivel, como la velocidad necesaria (por ejemplo, oro o plata). Esta función solo está disponible en volúmenes internos, qtrees, cabinas de almacenamiento, pools de almacenamiento y volúmenes. | Lista |
| Gravedad de la infracción | Clasificación (por ejemplo, mayor) de una infracción (por ejemplo, falta de puertos de host o falta de redundancia), en una jerarquía de mayor a menor importancia.                                                                                                                                                     | Lista |



Alias, centro de datos, caliente, nivel de servicio, puesta de sol, El nivel de conmutador, el nivel de servicio, el nivel y la gravedad de la infracción son anotaciones a nivel de sistema, que no puede eliminar ni cambiar de nombre; sólo puede cambiar sus valores asignados.

### Cómo se asignan las anotaciones

Puede asignar anotaciones de forma manual o automática mediante reglas de anotación. OnCommand Insight también asigna automáticamente algunas anotaciones sobre la adquisición de activos y por herencia. Las anotaciones que asigne a un activo aparecerán en la sección datos de usuario de la página activo.

Las anotaciones se asignan de las siguientes formas:

- Puede asignar una anotación manualmente a un activo.

Si una anotación se asigna directamente a un activo, la anotación aparece como texto normal en una página de activos. Las anotaciones que se asignan manualmente siempre tienen prioridad sobre las anotaciones que son heredadas o asignadas por reglas de anotación.

- Puede crear una regla de anotación para asignar anotaciones automáticamente a activos del mismo tipo.

Si la anotación está asignada por regla, Insight muestra el nombre de la regla junto al nombre de la anotación en una página de activos.

- Insight asocia automáticamente un nivel con un modelo de niveles de almacenamiento para acelerar la

asignación de anotaciones de almacenamiento a sus recursos sobre la adquisición de activos.

Ciertos recursos de almacenamiento se asocian automáticamente con un nivel predefinido (nivel 1 y nivel 2). Por ejemplo, el nivel de almacenamiento Symmetrix se basa en la familia Symmetrix y VMAX y está asociado con el nivel 1. Puede cambiar los valores predeterminados para que coincidan con sus requisitos de nivel. Si Insight asigna la anotación (por ejemplo, Tier), verá "System-defined" cuando sitúe el cursor sobre el nombre de la anotación en una página de activos.

- Unos pocos recursos (hijos de un activo) pueden derivar la anotación predefinida de nivel de su activo (principal).

Por ejemplo, si se asigna una anotación a un almacenamiento, la anotación de nivel se obtiene de todos los pools de almacenamiento, los volúmenes internos, los volúmenes, los qtrees y los recursos compartidos que pertenecen al almacenamiento. Si se aplica una anotación diferente a un volumen interno del almacenamiento, la anotación se deriva posteriormente de todos los volúmenes, qtrees y recursos compartidos. Aparece "derived" junto al nombre de la anotación en una página de activos.


### Asociación de costes con anotaciones

Antes de ejecutar informes relacionados con costes, debe asociar los costes con las anotaciones a nivel de sistema de nivel de servicio, nivel de switch y nivel, que permiten cobrar a los usuarios de almacenamiento en función del uso que hagan realmente de la producción y la capacidad replicada. Por ejemplo, para el nivel, puede tener valores de nivel Gold y Silver y asignar un coste más alto al nivel Gold que al nivel Silver.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en Administrar y seleccione **Anotaciones**.


Aparece la página anotación.

3. Coloque el cursor sobre la anotación nivel de servicio, nivel de conmutación o nivel y haga clic en .

Aparece el cuadro de diálogo Editar anotación.

4. Introduzca los valores para cualquier nivel existente en el campo **coste**.

Las anotaciones Tier y Service Level tienen los valores de Auto Tier y Object Storage, respectivamente, que no se pueden quitar.

5. Haga clic en  para agregar niveles adicionales.

6. Haga clic en **Guardar** cuando termine.

### Creación de anotaciones personalizadas

Con las anotaciones, puede agregar datos personalizados específicos del negocio que se ajusten a los activos de las necesidades del negocio. Aunque OnCommand Insight proporciona un conjunto de anotaciones predeterminadas, es posible que desee ver datos de otras maneras. Los datos de anotaciones personalizadas complementan los datos del dispositivo ya recopilados, como el fabricante del switch, el número de puertos

y las estadísticas de rendimiento. Insight no detecta los datos que se agregan con anotaciones.

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

La página Anotaciones muestra la lista de anotaciones.

3. Haga clic en .

Aparece el cuadro de diálogo **Agregar anotación**.

4. Introduzca un nombre y una descripción en los campos **Nombre** y **Descripción**.

Es posible introducir hasta 255 caracteres en estos campos.



Nombres de anotaciones que empiezan o terminan con un punto "." no son compatibles.

5. Haga clic en **Tipo** y, a continuación, seleccione una de las siguientes opciones que representa el tipo de datos permitidos en esta anotación:

- **Booleano**

Esto crea una lista desplegable con las opciones de yes y no. Por ejemplo, la anotación "Ditret adjuntado" es booleana.

- **Fecha**

Esto crea un campo que contiene una fecha. Por ejemplo, si la anotación será una fecha, selecciónela.

- **Lista**

Esto puede crear uno de los siguientes:

- **Una lista desplegable fija**

Cuando otros están asignando este tipo de anotación en un dispositivo, no pueden agregar más valores a la lista.

- **Una lista desplegable flexible**

Si selecciona la opción **Agregar nuevos valores sobre la marcha** al crear esta lista, cuando otros asignan este tipo de anotación en un dispositivo, pueden agregar más valores a la lista.

- **Número**

Esto crea un campo en el que el usuario que asigna la anotación puede introducir un número. Por ejemplo, si el tipo de anotación es "Piso", el usuario puede seleccionar el tipo de valor "número" e introducir el número de piso.

- **Texto**

Esto crea un campo que permite texto de forma libre. Por ejemplo, puede escribir «'Idioma'» como tipo



de anotación, seleccionar «'texto'» como tipo de valor e introducir un idioma como valor.




Después de establecer el tipo y guardar los cambios, no puede cambiar el tipo de anotación. Si necesita cambiar el tipo, debe eliminar la anotación y crear una nueva.

6. Si selecciona **List** como tipo de anotación, haga lo siguiente:

- a. Seleccione **Agregar nuevos valores sobre la marcha** si desea la capacidad de agregar más valores a la anotación cuando se encuentra en una página de activos, que crea una lista flexible.

Por ejemplo, supongamos que se encuentra en una página de activos y que el activo tiene la anotación Ciudad con los valores Detroit, Tampa y Boston. Si ha seleccionado la opción **Agregar nuevos valores sobre la marcha**, puede agregar valores adicionales a Ciudad como San Francisco y Chicago directamente en la página de activos en lugar de tener que ir a la página Anotaciones para agregarlos. Si no selecciona esta opción, no podrá agregar nuevos valores de anotación al aplicar la anotación; esto creará una lista fija.

- b. Introduzca un valor y un nombre en los campos **valor** y **Descripción**.

- c. Haga clic en  para añadir valores adicionales.

- d. Haga clic en  para eliminar un valor.

7. Haga clic en **Guardar**.

Las anotaciones aparecen en la lista de la página Anotaciones.

## Información relacionada

["Importar y exportar datos de usuario"](#)


### Asignación manual de anotaciones a activos

La asignación de anotaciones a activos ayuda a ordenar, agrupar e informar sobre los activos de forma que sean relevantes para su negocio. Aunque puede asignar anotaciones a activos de un tipo concreto automáticamente, mediante reglas de anotación, puede asignar anotaciones a un activo individual mediante su página de activos.


### Antes de empezar

Debe haber creado la anotación que desea asignar.


### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Busque el activo al que desea aplicar la anotación realizando una de las siguientes acciones:
  - Haga clic en el activo en el panel de activos.
  - Haga clic en  En la barra de herramientas para mostrar el cuadro **Buscar activos**, escriba el tipo o el nombre del activo y, a continuación, seleccione el activo de la lista que aparece.

Aparece la página Asset.

3. En la sección **datos de usuario** de la página de activos, haga clic en .

Aparece el cuadro de diálogo Agregar anotación.

4. Haga clic en **anotación** y seleccione una anotación de la lista.
5. Haga clic en **valor** y realice una de las siguientes acciones, según el tipo de anotación que haya seleccionado:
  - Si el tipo de anotación es lista, fecha o booleano, seleccione un valor de la lista.
  - Si el tipo de anotación es texto, escriba un valor.
6. Haga clic en **Guardar**.
7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en  y seleccione un valor diferente.

Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

### Modificación de anotaciones

Es posible que desee cambiar el nombre, la descripción o los valores de una anotación o eliminar una anotación que ya no desee utilizar.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desee editar y haga clic en .

Aparece el cuadro de diálogo **Editar anotación**.



4. Puede realizar las siguientes modificaciones en una anotación:

- a. Cambie el nombre, la descripción o ambos.

Sin embargo, tenga en cuenta que puede introducir un máximo de 255 caracteres tanto para el nombre como para la descripción, y no puede cambiar el tipo de anotación. Además, para las anotaciones a nivel de sistema, no se puede cambiar el nombre ni la descripción; sin embargo, se pueden agregar o quitar valores si la anotación es un tipo de lista.



Si se publica una anotación personalizada en el almacén de datos y se le cambia el nombre, se perderán los datos históricos.

- a. Para agregar otro valor a una anotación de tipo de lista, haga clic en .
- b. Para eliminar un valor de una anotación de un tipo de lista, haga clic en .

No se puede eliminar un valor de anotación si dicho valor está asociado a una anotación incluida en una regla de anotación, una consulta o una política de rendimiento.

5. Haga clic en **Guardar** cuando termine.

## Después de terminar

Si va a utilizar anotaciones en el almacén de datos, debe forzar una actualización de las anotaciones en el almacén de datos. Consulte la *OnCommand Insight Guía de administración de almacenes de datos*.

### Eliminar anotaciones

Es posible que desee eliminar una anotación que ya no desee utilizar. No puede eliminar una anotación a nivel de sistema ni una anotación que se utilice en una regla de anotación, una consulta o una política de rendimiento.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Anotaciones**.

Aparece la página Anotaciones.

3. Coloque el cursor sobre la anotación que desea eliminar y haga clic en .

Se muestra un cuadro de diálogo de confirmación.

4. Haga clic en **Aceptar**.

## Asignación de anotaciones a activos mediante reglas de anotación

Para asignar anotaciones automáticamente a activos basándose en los criterios definidos, configure reglas de anotación. OnCommand Insight asigna las anotaciones a los activos basándose en estas reglas. Insight también proporciona dos reglas de anotación predeterminadas, que se pueden modificar para ajustarse a sus necesidades o quitar si no desea utilizarlas.

### Reglas de anotación de almacenamiento predeterminadas

Para acelerar la asignación de anotaciones de almacenamiento a los recursos, OnCommand Insight incluye 21 reglas de anotación predeterminadas, que asocian un nivel a un modelo de niveles de almacenamiento. Todos los recursos de almacenamiento están asociados automáticamente con un nivel tras la adquisición de los activos de su entorno.

Las reglas de anotación predeterminadas aplican anotaciones de nivel de la siguiente manera:

- Nivel 1, nivel de calidad del almacenamiento

La anotación de nivel 1 se aplica a los siguientes proveedores y a sus familias específicas: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 o FAS6200) y Violin (memoria).

- Nivel 2, nivel de calidad del almacenamiento

La anotación del nivel 2 se aplica a los siguientes proveedores y a sus familias específicas: HP (3PAR StoreServ o EVA), EMC (CLARiiON), HDS (AMS o D800), IBM (XIV) y NetApp (FAS3000, FAS3100 y FAS3200).

Puede editar la configuración predeterminada de estas reglas para que se ajuste a sus requisitos de nivel o puede eliminarlas si no las necesita.

### Creación de reglas de anotación

Como alternativa a la aplicación manual de anotaciones a activos individuales, puede aplicar anotaciones automáticamente a varios activos mediante reglas de anotación. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

### Antes de empezar

Debe haber creado una consulta para la regla de anotación.

### Acerca de esta tarea

Aunque puede editar los tipos de anotaciones mientras crea las reglas, debe haber definido los tipos con anticipación.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Haga clic en  **Add**.

Aparece el cuadro de diálogo Agregar regla.

4. Haga lo siguiente:
  - a. En el cuadro **Nombre**, escriba un nombre único que describa la regla.  
  
Este nombre aparecerá en la página Reglas de anotación.
  - b. Haga clic en **Consulta** y seleccione la consulta que OnCommand Insight debe utilizar para aplicar la anotación a los activos.
  - c. Haga clic en **anotación** y seleccione la anotación que desea aplicar.
  - d. Haga clic en **valor** y seleccione un valor para la anotación.

Por ejemplo, si selecciona Cumpleaños como anotación, especifique una fecha para el valor.

5. Haga clic en **Guardar**.
6. Haga clic en **Ejecutar todas las reglas** si desea ejecutar todas las reglas inmediatamente; de lo contrario, las reglas se ejecutarán a un intervalo programado regularmente.

## Establecimiento de la precedencia de regla de anotación

De forma predeterminada, OnCommand Insight evalúa las reglas de anotación secuencialmente; sin embargo, puede configurar el orden en el que OnCommand Insight evalúa las reglas de anotación si desea que Insight evalúe las reglas en un orden específico.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Coloque el cursor sobre una regla de anotación.

Las flechas de precedencia aparecen a la derecha de la regla.

4. Para mover una regla hacia arriba o hacia abajo en la lista, haga clic en la flecha hacia arriba o hacia abajo.

De forma predeterminada, las nuevas reglas se agregan secuencialmente a la lista de reglas. Las anotaciones definidas manualmente en una página de activos individual tienen prioridad sobre las anotaciones basadas en reglas cuando Insight evalúa las reglas de anotación.

## Modificación de reglas de anotación

Puede modificar una regla de anotación para cambiar el nombre de la regla, su anotación, el valor de la anotación o la consulta asociada con la regla.

### Pasos


1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea modificar:

- En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
- Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una página.

4. Realice una de las siguientes acciones para visualizar el cuadro de diálogo **Editar regla**:

- Si se encuentra en la página Reglas de anotación, coloque el cursor sobre la regla de anotación y haga clic en .
- Si se encuentra en una página de activos, coloque el cursor sobre la anotación asociada con la regla, coloque el cursor sobre el nombre de la regla cuando aparezca y, a continuación, haga clic en el nombre de la regla.

5. Realice los cambios necesarios y haga clic en **Guardar**.


## Eliminación de reglas de anotación

Puede eliminar una regla de anotación cuando la regla ya no sea necesaria para supervisar los objetos de la red.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar** y seleccione **Reglas de anotación**.

La página Reglas de anotación muestra la lista de reglas de anotación existentes.

3. Busque la regla que desea eliminar:
  - En la página Reglas de anotación, puede filtrar las reglas de anotación introduciendo un valor en el cuadro de filtro.
  - Haga clic en un número de página para examinar las reglas de anotación por página si hay más reglas que ajustar en una sola página.
4. Coloque el cursor sobre la regla que desea eliminar y, a continuación, haga clic en  .

Aparecerá un mensaje de confirmación en el que se le preguntará si desea eliminar la regla.

5. Haga clic en **Aceptar**.

### Importando valores de anotación

Si mantiene anotaciones en objetos SAN (como almacenamiento, hosts y máquinas virtuales) en un archivo CSV, puede importar esa información a OnCommand Insight. Puede importar aplicaciones, entidades de negocio o anotaciones como Tier y Building.

#### Acerca de esta tarea

Se aplican las siguientes reglas:

- Si un valor de anotación está vacío, esa anotación se elimina del objeto.
- Al anotar volúmenes o volúmenes internos, el nombre del objeto es una combinación de nombre de almacenamiento y nombre de volumen utilizando el guión y el separador de flecha (->):

```
<storage_name>-><volume_name>
```

- Cuando se anota el almacenamiento, los conmutadores o los puertos, se omite la columna aplicación.
- Las columnas de inquilino, línea\_de\_negocio, Unidad\_Negocio y proyecto conforman una entidad de negocio.

Cualquiera de los valores puede dejarse en blanco. Si una aplicación ya está relacionada con una entidad de negocio distinta de los valores de entrada, la aplicación se asigna a la nueva entidad de negocio.

La utilidad de importación admite los siguientes tipos de objeto y claves:

| Tipo | Clave |
|------|-------|
|------|-------|

|                             |                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Host                        | id-><id> o. <Name> o. <IP>                                                                                                          |
| MÁQUINA VIRTUAL             | id-><id> o. <Name>                                                                                                                  |
| Del banco de almacenamiento | id-><id> o. <Storage_name>-><Storage_Pool_name>                                                                                     |
| Volumen interno             | id-><id> o. <Storage_name>-><Internal_volume_name>                                                                                  |
| Volumen                     | id-><id> o. <Storage_name>-><Volume_name>                                                                                           |
| Reducida                    | id-><id> o. <Name> o. <IP>                                                                                                          |
| Conmutador                  | id-><id> o. <Name> o. <IP>                                                                                                          |
| Puerto                      | id-><id> o. <WWN>                                                                                                                   |
| Share                       | id-><id> o. <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol><br><Qtree> es opcional si hay un qtree predeterminado. |
| Qtree                       | id-><id> o. <Storage Name>-><Internal Volume Name>-><Qtree Name>                                                                    |

El archivo CSV debe utilizar el formato siguiente:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.

2. Haga clic en **Admin** y seleccione **solución de problemas**.

Aparece la página solución de problemas.

3. En la sección **otras tareas** de la página, haga clic en el vínculo **Portal OnCommand Insight**.

4. Haga clic en **Insight Connect API**.

5. Inicie sesión en el portal.

6. Haga clic en **Utilidad de importación de anotación**.

7. Guarde la `.zip` descomprimirlo, descomprimirlo y leer el `readme.txt` archivo para obtener información adicional y muestras.

8. Coloque el archivo CSV en la misma carpeta que `.zip` archivo.

9. En la ventana de línea de comandos de, introduzca lo siguiente:

```
java -jar rest-import-utility.jar [-username] [-password]
[-server name or IP address] [-batch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

La opción `-l`, que activa el registro adicional, y la opción `-c`, que habilita la sensibilidad del caso, se establecen en `FALSE` de forma predeterminada. Por lo tanto, sólo debe especificarlos cuando desee utilizar las operaciones.



No hay espacios entre las opciones y sus valores.



Las siguientes palabras clave están reservadas e impiden que los usuarios las especifiquen como nombres de anotación: `- Aplicación` - `prioridad_de_aplicación` - `arrendatario` - `línea_de_negocio` - `Unidad_de_negocio` - se generan errores de proyecto si intenta importar un tipo de anotación utilizando una de las palabras clave reservadas. Si ha creado nombres de anotación con estas palabras clave, debe modificarlas para que la herramienta de utilidad de importación pueda funcionar correctamente.



La utilidad de importación de anotaciones requiere Java 8 o Java 11. Asegúrese de que uno de ellos está instalado antes de ejecutar la utilidad de importación. Se recomienda utilizar la última versión de OpenJDK 11.

## Asignar anotaciones a varios activos mediante una consulta

La asignación de una anotación a un grupo de activos ayuda a identificar o utilizar más fácilmente los activos relacionados en consultas o paneles.

### Antes de empezar

Las anotaciones que desea asignar a los activos deben haberse creado previamente.



## Acerca de esta tarea

Puede simplificar la tarea de asignar una anotación a varios activos mediante una consulta. Por ejemplo, si desea asignar una anotación de dirección personalizada a todas las matrices en una ubicación específica del centro de datos.

### Pasos

1. Cree una nueva consulta para identificar los activos en los que desea asignar una anotación. Haga clic en **consultas > +Nueva consulta**.
2. En el menú desplegable **Buscar...**, elija **almacenamiento**. Puede establecer filtros para delimitar aún más la lista de almacenamientos mostrados.
3. En la lista de almacenamientos que se muestra, seleccione uno o varios haciendo clic en la casilla de comprobación situada junto al nombre del almacenamiento. También puede seleccionar todos los almacenamientos mostrados haciendo clic en la casilla de verificación principal de la parte superior de la lista.
4. Cuando haya seleccionado todos los almacenamientos deseados, haga clic en **acciones > Editar anotación**.

El sistema muestra el cuadro de diálogo Agregar anotación.

5. Seleccione **Annotation** y **Value** que desea asignar a los almacenamientos y haga clic en **Save**.

Si está mostrando la columna para esa anotación, aparecerá en todos los almacenamientos seleccionados.

6. Ahora puede utilizar la anotación para filtrar los almacenamientos en un widget o consulta. En un widget, puede hacer lo siguiente:
  - a. Cree un panel o abra uno existente. Añada una **variable** y elija la anotación que haya establecido en los almacenamientos anteriores. La variable se agrega al panel.
  - b. En el campo de variable que acaba de agregar, haga clic en **any** e introduzca el valor adecuado para filtrar. Haga clic en la Marca de verificación para guardar el valor de variable.
  - c. Agregar un widget. En la consulta del widget, haga clic en el botón **Filter by+** y seleccione la anotación correspondiente de la lista.
  - d. Haga clic en **Any** y seleccione la variable de anotación que agregó anteriormente. Las variables creadas empiezan por "\$" y se muestran en la lista desplegable.
  - e. Configure los otros filtros o campos que desee y, a continuación, haga clic en **Guardar** cuando el widget se personalice según sus preferencias.

El widget del panel de control muestra los datos sólo de los almacenamientos a los que se ha asignado la anotación.

## Consulta de activos

Las consultas permiten supervisar y solucionar problemas en la red mediante la búsqueda de activos en el entorno a un nivel granular en función de los criterios seleccionados por el usuario (anotaciones y métricas de rendimiento). Además, las reglas de anotación, que asignan anotaciones automáticamente a los activos, requieren una consulta.

## Activos utilizados en consultas y paneles

Las consultas de Insight y los widgets de panel pueden utilizarse con una amplia gama de tipos de activos

Los siguientes tipos de activos se pueden utilizar en consultas, widgets de panel y páginas de activos personalizados. Los campos y contadores disponibles para filtros, expresiones y visualización variarán entre los tipos de activos. No todos los activos se pueden utilizar en todos los tipos de widgets.

- Cliente más
- Almacén de datos
- Disco
- Estructura
- Dispositivo genérico
- Host
- Volumen interno
- Sesión iSCSI
- Portal de red de iSCSI
- Ruta
- Puerto
- Qtree
- Cuota
- Share
- Reducida
- Nodo de almacenamiento
- Pool de almacenamiento
- Conmutador
- Cinta
- VMDK
- Máquina virtual
- Volumen
- Zona
- Miembro de la zona

## Crear una consulta

Puede crear una consulta para poder buscar los activos de su entorno a un nivel granular. Las consultas permiten cortar los datos agregando filtros y, a continuación, ordenando los resultados para ver los datos de inventario y rendimiento en una sola vista.

## Acerca de esta tarea

Por ejemplo, puede crear una consulta para los volúmenes, agregar un filtro para buscar determinados almacenamientos asociados al volumen seleccionado, agregar un filtro para buscar una anotación determinada, como el nivel 1, en los almacenamientos seleccionados, Y añada otro filtro para encontrar todos los almacenamientos con IOPS - Leer (IO/s) más de 25. Cuando se muestran los resultados, puede ordenar las columnas de información asociadas a la consulta en orden ascendente o descendente.

Cuando se agrega un nuevo origen de datos que adquiere activos o se realiza cualquier anotación o asignación de aplicaciones, puede consultar esos activos, anotaciones o aplicaciones después de indizar las consultas, lo que ocurre a intervalos regulares programados.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **+ Nueva consulta**.
3. Haga clic en **Seleccionar tipo de recurso** y seleccione un tipo de activo.

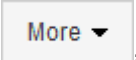
Cuando se selecciona un recurso para una consulta, se muestran automáticamente un número de columnas predeterminadas; puede eliminar estas columnas o agregar nuevas en cualquier momento.


4. En el cuadro de texto **Nombre**, escriba el nombre del activo o escriba una parte del texto para filtrar a través de los nombres de los activos.

Puede utilizar cualquiera de las opciones siguientes, solo o combinadas, para refinar la búsqueda en cualquier cuadro de texto de la página Nueva consulta:

- Un asterisco le permite buscar todo. Por ejemplo: `vol*rhel` muestra todos los recursos que empiezan con «'vol'» y terminan con «'rhel'».
- El signo de interrogación le permite buscar un número específico de caracteres. Por ejemplo: `BOS-PRD??-S12` Muestra BOS-PRD12-S12, BOS-PRD13-S12, etc.
- El operador OR permite especificar varias entidades. Por ejemplo: `FAS2240 OR CX600 OR FAS3270` busca varios modelos de almacenamiento.
- El operador NOT permite excluir el texto de los resultados de búsqueda. Por ejemplo: `NOT EMC*` Encuentra todo lo que no empieza con «'EMC'». Puede utilizar `NOT *` para mostrar campos que no contienen ningún valor.

5. Haga clic en  para mostrar los activos.

6. Para agregar un criterio, haga clic en , y realice una de las siguientes acciones:

- Escriba para buscar un criterio específico y, a continuación, selecciónelo.
- Desplácese hacia abajo por la lista y seleccione un criterio.
- Introduzca un rango de valores si selecciona una métrica de rendimiento, como IOPS - Read (IO/s). Las anotaciones predeterminadas proporcionadas por Insight se indican mediante ; es posible tener anotaciones con nombres duplicados.

Se agrega una columna a la lista resultados de la consulta para los criterios y los resultados de la consulta en la lista se actualizan.

7. De manera opcional, puede hacer clic en  para eliminar una métrica de rendimiento o anotación de los

resultados de la consulta.

Por ejemplo, si la consulta muestra la latencia máxima y el rendimiento máximo de los almacenes de datos y desea mostrar sólo la latencia máxima en la lista de resultados de la consulta, haga clic en este botón y desactive la casilla de verificación **rendimiento - Máx**. La columna Throughput - Max (MB/s) se elimina de la lista resultados de la consulta.



Dependiendo del número de columnas que se muestran en la tabla de resultados de la consulta, es posible que no pueda ver columnas adicionales agregadas. Puede eliminar una o más columnas hasta que las columnas que desee se vean.

8. Haga clic en **Guardar**, escriba un nombre para la consulta y vuelva a hacer clic en **Guardar**.

Si tiene una cuenta con una función de administrador, puede crear paneles personalizados. Un panel personalizado puede incluir cualquiera de los widgets de la Biblioteca de widgets, algunos de los cuales permiten representar los resultados de las consultas en un panel personalizado. Para obtener más información acerca de los paneles personalizados, consulte la *Guía de introducción de OnCommand Insight*.

## Información relacionada

["Importar y exportar datos de usuario"](#)

## Ver consultas

Puede ver sus consultas para supervisar sus activos y cambiar el modo en que sus consultas muestran los datos relacionados con sus activos.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.
3. Puede cambiar el modo en que se muestran las consultas realizando cualquiera de las siguientes acciones:
  - Puede introducir texto en el cuadro **filtro** para buscar y mostrar consultas específicas.
  - Puede cambiar el orden de las columnas de la tabla de consultas a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
  - Para cambiar el tamaño de una columna, coloque el ratón sobre el encabezado de la columna hasta que aparezca una barra azul. Coloque el ratón sobre la barra y arrástrelo hacia la derecha o la izquierda.
  - Para mover una columna, haga clic en el encabezado de la columna y arrástrela hacia la derecha o hacia la izquierda.
  - Al desplazarse por los resultados de la consulta, tenga en cuenta que los resultados pueden cambiar a medida que Insight sondea automáticamente sus orígenes de datos. Esto puede resultar en que faltan algunos elementos o que algunos elementos aparezcan fuera de servicio en función de cómo se ordenen.


## Exportando resultados de consulta a un archivo .CSV

Es posible que desee exportar los resultados de una consulta a un archivo .CSV para importar los datos a otra aplicación.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Se muestra la página consultas.

3. Haga clic en una consulta.
4. Haga clic en  para exportar los resultados de la consulta a un .CSV archivo.
5. Debe realizar una de las siguientes acciones:
  - Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardar el archivo en una ubicación específica.
  - Haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas. Sólo se exportarán los atributos de las columnas mostradas. Algunas columnas mostradas, en particular las que forman parte de relaciones anidadas complejas, no se exportan.



Cuando aparece una coma en un nombre de activo, la exportación incluye el nombre entre comillas, conservando el nombre del activo y el formato .csv adecuado.

+ cuando exporte los resultados de la consulta, tenga en cuenta que **todas las filas** de la tabla de resultados se exportarán, no sólo las seleccionadas o mostradas en la pantalla, hasta un máximo de 10,000 filas.

Al abrir un archivo .CSV exportado con Excel, si tiene un nombre de objeto u otro campo con el formato NN:NN (dos dígitos seguidos de dos puntos seguidos de dos dígitos más), Excel interpretará a veces ese nombre como un formato de hora, en lugar de texto. Esto puede resultar en que Excel muestre valores incorrectos en esas columnas. Por ejemplo, un objeto llamado "81:45" se mostraría en Excel como "81:45:00". Para evitar esto, importe .CSV en Excel utilizando los pasos siguientes:

+

- Open a new sheet in Excel.
  - On the "Data" tab, choose "From Text".
  - Locate the desired .CSV file and click "Import".
  - In the Import wizard, choose "Delimited" and click Next.
  - Choose "Comma" for the delimiter and click Next.
  - Select the desired columns and choose "Text" for the column data format.
  - Click Finish.
- Your objects should show in Excel in the proper format.

+


## Modificar consultas

Puede cambiar los criterios asociados a una consulta cuando desee cambiar los criterios de búsqueda de los activos que esté consultando.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Se muestra la página consultas.

3. Haga clic en el nombre de la consulta.
4. Para eliminar un criterio de la consulta, haga clic en .

5. Para agregar un criterio a la consulta, haga clic en  y seleccione un criterio de la lista.

6. Debe realizar una de las siguientes acciones:
  - Haga clic en **Guardar** para guardar la consulta con el nombre que se utilizó inicialmente.
  - Haga clic en **Guardar como** para guardar la consulta con otro nombre.
  - Haga clic en **Cambiar nombre** para cambiar el nombre de la consulta que ha utilizado inicialmente.
  - Haga clic en **revertir** para volver a cambiar el nombre de la consulta al que había utilizado inicialmente.

## Eliminación de consultas

Puede eliminar consultas cuando ya no reúnan información útil sobre sus activos. No se puede eliminar una consulta si se utiliza en una regla de anotación.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Aparece la página consultas.

3. Coloque el cursor sobre la consulta que desea eliminar y haga clic en .

Aparece un mensaje de confirmación en el que se pregunta si desea eliminar la consulta.

4. Haga clic en **Aceptar**.

## Asignar múltiples aplicaciones a o quitar varias aplicaciones de activos

Puede asignar varias aplicaciones a o eliminar varias aplicaciones de activos mediante una consulta en lugar de tener que asignarlas o eliminarlas manualmente.

### Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

### Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.


Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en  ▼ Para seleccionar **todo**.

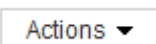
Aparece el botón **acciones**.

4. Para agregar una aplicación a los activos seleccionados, haga clic en  ▼ Y seleccione **Editar aplicación**.

- a. Haga clic en **aplicación** y seleccione una o más aplicaciones.

Es posible seleccionar varias aplicaciones para hosts, volúmenes internos y máquinas virtuales; sin embargo, solo puede seleccionar una aplicación para un volumen.

- b. Haga clic en **Guardar**.

5. Para eliminar una aplicación asignada a los activos, haga clic en  ▼ Y seleccione **Eliminar aplicación**.

- a. Seleccione la aplicación o aplicaciones que desea eliminar.
- b. Haga clic en **Eliminar**.

Las aplicaciones nuevas que asigne anulan las aplicaciones del activo que se derivaron de otro activo. Por ejemplo, los volúmenes heredan aplicaciones de hosts y cuando se asignan aplicaciones nuevas a un volumen, la nueva aplicación tiene prioridad sobre la aplicación derivada.

## Edición o eliminación de varias anotaciones de activos

Puede editar varias anotaciones para activos o eliminar varias anotaciones de activos mediante una consulta en lugar de tener que editarlas o eliminarlas manualmente.

### Antes de empezar

Debe haber creado una consulta que busque todos los activos que desea editar.

### Pasos

1. Haga clic en **consultas** y seleccione **Mostrar todas las consultas**.

Aparece la página consultas.

2. Haga clic en el nombre de la consulta que encuentra los activos.

Se muestra la lista de activos asociados a la consulta.

3. Seleccione los activos deseados en la lista o haga clic en ☐ ▼ Para seleccionar **todo**.

Aparece el botón **acciones**.

4. Para agregar una anotación a los activos o editar el valor de una anotación asignada a los activos, haga clic en **Actions ▼** Y seleccione **Editar anotación**.

- a. Haga clic en **anotación** y seleccione una anotación para la que desee cambiar el valor, o seleccione una nueva anotación para asignarla a todos los activos.
- b. Haga clic en **valor** y seleccione un valor para la anotación.
- c. Haga clic en **Guardar**.

5. Para eliminar una anotación asignada a los activos, haga clic en **Actions ▼** Y seleccione **Quitar anotación**.

- a. Haga clic en **anotación** y seleccione la anotación que desea eliminar de los activos.
- b. Haga clic en **Eliminar**.

## Copiando valores de tabla

Puede copiar valores en tablas para utilizarlos en cuadros de búsqueda u otras aplicaciones.

### Acerca de esta tarea

Existen dos métodos que se pueden utilizar para copiar valores de tablas o resultados de consultas.



## Pasos

1. Método 1: Resalte el texto deseado con el ratón, cópielo y péguelo en campos de búsqueda u otras aplicaciones.
2. Método 2: Para campos de un solo valor cuya longitud supere el ancho de la columna de tabla, indicado por elipses (...), pase el cursor sobre el campo y haga clic en el icono del portapapeles. El valor se copia en el portapapeles para utilizarlo en campos de búsqueda u otras aplicaciones.

Tenga en cuenta que sólo se pueden copiar los valores que son vínculos a activos. Tenga en cuenta también que sólo los campos que incluyen valores únicos (es decir, no listas) tienen el icono de copia.

## Gestión de fuentes de datos de Insight

Los orígenes de datos son el componente más importante que se utiliza para mantener un entorno OnCommand Insight. Dado que son la fuente principal de información de Insight, es imprescindible mantener los orígenes de datos en estado en ejecución.

Puede supervisar los orígenes de datos de la red seleccionando un origen de datos para comprobar los eventos relacionados con su estado y anotando cualquier cambio que pudiera haber causado problemas.

Además de examinar un origen de datos individual, puede realizar estas operaciones:

- Clone un origen de datos para crear muchos orígenes de datos similares en Insight
- Edite la información del origen de datos
- Cambiar credenciales
- Controlar sondeo
- Eliminar el origen de datos
- Instalar los parches de origen de datos
- Instale un nuevo origen de datos desde un parche
- Preparar un informe de error para el soporte al cliente de NetApp

## Configurar orígenes de datos en Insight

Los orígenes de datos son el componente más importante al intentar mantener un entorno Insight. Los orígenes de datos detectan la información de red que se utiliza para el análisis y la validación. Debe configurar sus orígenes de datos en Insight para poder supervisarlos dentro de su red.

Para cada origen de datos, los requisitos específicos para definir ese origen de datos dependen del proveedor y modelo de los dispositivos correspondientes. Antes de agregar los orígenes de datos, necesita direcciones de red, información de cuentas y contraseñas para todos los dispositivos y posiblemente estos detalles adicionales:

- Interruptores
- Estaciones de gestión de dispositivos
- Sistemas de almacenamiento que tienen conectividad IP
- Estaciones de gestión del almacenamiento

- Host de servidores que ejecutan software de gestión para dispositivos de almacenamiento que no tienen conectividad IP

Para obtener más información acerca de las definiciones de origen de datos, consulte la información de "referencia de origen de datos específico del proveedor" en esta sección.

## Información de soporte de fuentes de datos

Como parte de la planificación de la configuración, debe asegurarse de que Insight pueda supervisar los dispositivos del entorno. Para ello, puede consultar la matriz de compatibilidad del origen de datos para obtener información detallada sobre los sistemas operativos, dispositivos específicos y protocolos. Es posible que algunas fuentes de datos no estén disponibles en todos los sistemas operativos.

### Ubicación de la versión más actualizada de Data Source Support Matrix

La matriz de compatibilidad con orígenes de datos de OnCommand Insight se actualiza con cada versión de service pack. La versión más reciente del documento se encuentra en la ["Sitio de soporte de NetApp"](#). .

## Agregar orígenes de datos

Puede agregar rápidamente orígenes de datos mediante el cuadro de diálogo Agregar origen de datos.

### Pasos

1. Abra OnCommand Insight en el explorador e inicie sesión como usuario con permisos administrativos.
2. Seleccione **Admin** y elija **fuentes de datos**.
3. Haga clic en el botón **+Add**.

Se abrirá el asistente Agregar origen de datos.

4. En la sección **Configuración**, introduzca la siguiente información:

| Campo          | Descripción                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre         | Introduzca un nombre de red único para este origen de datos. NOTA: Sólo se permiten letras, números y el carácter de subrayado (_) en el nombre del origen de datos. |
| Proveedor      | Elija el proveedor del origen de datos en la lista desplegable.                                                                                                      |
| Modelo         | Elija el modelo del origen de datos en la lista desplegable.                                                                                                         |
| Dónde ejecutar | Elija local, o puede elegir una unidad de adquisición remota si las RAU están configuradas en su entorno.                                                            |

|             |                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Qué recoger | Para la mayoría de los orígenes de datos, estas opciones serán Inventario y rendimiento. El inventario se selecciona siempre de forma predeterminada y no se puede anular la selección. Tenga en cuenta que algunos orígenes de datos pueden tener opciones diferentes. Las opciones de recopilación que seleccione cambian los campos disponibles en las secciones Configuración y Configuración avanzada. |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Haga clic en el enlace **Configuración** e introduzca la información básica de configuración necesaria para el origen de datos con el tipo de recopilación de datos seleccionado.
- Si este tipo de origen de datos normalmente requiere información más detallada para configurarlo en la red, haga clic en el vínculo **Configuración avanzada** para introducir información adicional.
- Para obtener información detallada acerca de la configuración o la información de configuración avanzada necesaria o disponible para su origen de datos específico, consulte "[Referencia de origen de datos específica del proveedor](#)".
- Haga clic en el enlace **Prueba** para asegurarse de que el origen de datos está configurado correctamente.
- Haga clic en **Guardar**.

#### Importar orígenes de datos de una hoja de cálculo

Puede importar varios orígenes de datos en OnCommand Insight desde una hoja de cálculo. Esto puede ser útil si ya mantiene sus dispositivos de descubrimiento en una hoja de cálculo. Este proceso agrega nuevos orígenes de datos, pero no se puede utilizar para actualizar orígenes de datos existentes.

#### Acerca de esta tarea

OnCommand Insight incluye una hoja de cálculo que le ayuda a crear orígenes de datos. Esta hoja de cálculo tiene los siguientes atributos:

- La hoja de cálculo se puede utilizar con Microsoft Excel 2003 o posterior.
- Cada pestaña contiene un tipo de origen de datos, por ejemplo, Brocade SSH/CLI.
- Cada fila representa una instancia de un nuevo origen de datos que se va a crear.

La hoja de cálculo incluye una macro que crea un nuevo origen de datos en OnCommand Insight.

#### Pasos

- Busque la hoja de cálculo en  
`<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
- En la hoja de cálculo, introduzca la información del origen de datos en las celdas con color.
- Eliminar filas vacías.
- Desde la hoja de cálculo, ejecute la `CreateDataSources` macro para crear los orígenes de datos.
- Cuando se le soliciten las credenciales, especifique el nombre de usuario y la contraseña de

administración del servidor OnCommand Insight.

Los resultados se registran en el registro de adquisición.

6. Se le pregunta si el equipo que ejecuta actualmente la macro tiene OnCommand Insight instalado.

Seleccione una de las siguientes opciones:

- No: Seleccione "no" si se va a crear un archivo por lotes que se debe ejecutar en el equipo OnCommand Insight. Ejecute este archivo por lotes desde el directorio de instalación.
- Sí: Seleccione "Sí" si OnCommand Insight ya está instalado y no se requieren pasos adicionales para generar la información del origen de datos.

7. Para verificar la adición de los orígenes de datos, abra Insight en su navegador.

8. En la barra de herramientas Insight, haga clic en **Admin**.

9. Compruebe la lista orígenes de datos de los orígenes de datos importados.

#### Adición de un nuevo origen de datos por parche

Los nuevos orígenes de datos se publican como archivos de revisión que se pueden cargar en el sistema mediante el proceso de revisión. Con este proceso puede estar disponible nuevo origen de datos entre las versiones programadas de OnCommand Insight.

#### Antes de empezar

Debe haber cargado el archivo de revisión que desea instalar.

#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Seleccione **parches**.
3. Seleccione **acciones > instalar Service Pack o parche**.
4. En el cuadro de diálogo **instalar Service Pack o parche**, haga clic en **examinar** para buscar y seleccionar el archivo de revisión que cargó.
5. Haga clic en **Siguiente** en el cuadro de diálogo **Resumen de parches**.
6. Revise la información **Léame** y haga clic en **Siguiente** para continuar.
7. En el cuadro de diálogo **instalar**, haga clic en **Finalizar**.

#### Clonar un origen de datos

Con la instalación de clonado, puede agregar rápidamente un origen de datos con las mismas credenciales y atributos que otro origen de datos. La clonación le permite configurar fácilmente varias instancias del mismo tipo de dispositivo.

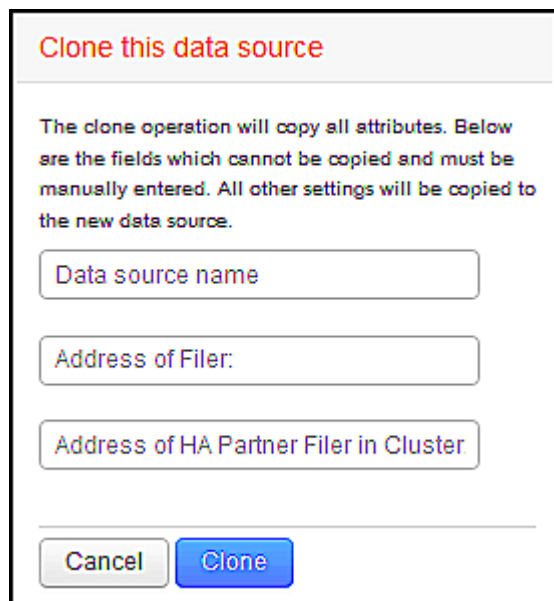
#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

Se abrirá la lista orígenes de datos.

2. Resalte el origen de datos que contiene la información de configuración que desea utilizar para el nuevo origen de datos.
3. A la derecha del origen de datos resaltado, haga clic en el icono **Clonar**.

En el cuadro de diálogo Clone this data source, se enumera la información que debe suministrar para el origen de datos seleccionado, como se muestra en el siguiente ejemplo de un origen de datos de NetApp:



4. Introduzca la información necesaria en los campos; esos detalles no se pueden copiar desde el origen de datos existente.
5. Haga clic en **Clonar**.

## Resultados

La operación de clonado copia todos los otros atributos y configuraciones para crear el nuevo origen de datos.

## Prueba de la configuración del origen de datos

Cuando se agrega un origen de datos, puede comprobar la corrección de la configuración para comunicarse con el dispositivo antes de guardar o actualizar ese origen de datos.

Al hacer clic en el botón **Prueba** del asistente de origen de datos, se comprueba la comunicación con el dispositivo especificado. La prueba produce uno de estos resultados:

- PASADO: El origen de datos está configurado correctamente.
- ADVERTENCIA: La prueba estaba incompleta, probablemente debido a que el tiempo de espera se agota durante el procesamiento o la adquisición no se estaba ejecutando.
- FAILED: El origen de datos, tal y como se ha configurado, no puede comunicarse con el dispositivo especificado. Compruebe los ajustes de configuración y vuelva a realizar una prueba.

## Referencia de origen de datos específica del proveedor

Los detalles de la configuración varían según el proveedor y modelo del origen de datos

que se agrega.

Si el origen de datos de un proveedor requiere instrucciones de configuración de Insight avanzadas, como requisitos especiales y comandos específicos, esa información se incluye en esta sección.

### Origen de datos de 3PAR InServ

OnCommand Insight usa el origen de datos InServ (firmware 2.2.2+, SSH) de 3PAR para descubrir el inventario de cabinas de almacenamiento StoreServ de HP 3PAR.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de 3PAR InServ. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                  |                        |
|----------------------------------|------------------------|
| Plazo del proveedor/modelo       | Insight plazo          |
| Disco físico                     | Disco                  |
| Sistema de almacenamiento        | Reducida               |
| Nodo de controladoras            | Nodo de almacenamiento |
| Grupo de aprovisionamiento común | Pool de almacenamiento |
| Volumen virtual                  | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

#### Requisitos

- La dirección IP o el FQDN del clúster InServ
- Para inventario, nombre de usuario y contraseña de sólo lectura para InServ Server.
- Para obtener rendimiento, nombre de usuario y contraseña de lectura y escritura en InServ Server.
- Requisitos de puerto: 22 (colección de inventario), 5988 o 5989 (recopilación de rendimiento) [Nota: El rendimiento de 3PAR es compatible con InServ OS 3.x+]
- Para la recogida del rendimiento, confirme que SMI-S está habilitado mediante el inicio de sesión en la cabina 3PAR por SSH.

#### Configuración

| Campo          | Descripción                                                  |
|----------------|--------------------------------------------------------------|
| IP del clúster | Dirección IP o nombre de dominio completo del clúster InServ |

|                             |                                                        |
|-----------------------------|--------------------------------------------------------|
| Nombre de usuario           | Nombre de usuario del servidor InServ                  |
| Contraseña                  | Contraseña utilizada para InServ Server                |
| IP DEL HOST DE SMI-S.       | Dirección IP del host del proveedor SMI-S.             |
| Nombre de usuario de SMI-S. | Nombre de usuario para el host del proveedor de SMI-S. |
| Contraseña SMI-S.           | Contraseña utilizada para el host del proveedor SMI-S. |

#### Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 40 minutos)    |
| Excluir dispositivos                     | Lista separada por comas de IP de dispositivo que se van a excluir   |
| Tiempo de espera del proceso SSH (s)     | Tiempo de espera del proceso SSH (60 segundos predeterminado)        |
| Número de reintentos SSH                 | Número de intentos de reintento de SSH                               |
| Tiempo de espera del banner SSH (s)      | Tiempo de espera del banner SSH (20 segundos predeterminado)         |
| Puerto SMI-S.                            | Puerto que utiliza el host del proveedor SMI-S.                      |
| Protocolo                                | Protocolo utilizado para conectar con el proveedor SMI-S.            |
| Espacio de nombres SMI-S.                | Espacio de nombres SMI-S.                                            |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |
| Número de reintentos de conexión SMI-S.  | Número de intentos de reintento de conexión SMI-S.                   |

#### Origen de datos de Amazon AWS EC2

OnCommand Insight utiliza este origen de datos para descubrir inventario y rendimiento de Amazon AWS EC2.

### Requisitos previos:

Para recopilar datos de los dispositivos Amazon EC2, debe disponer de la siguiente información:

- Debe tener el ID de clave de acceso IAM
- Debe tener la clave de acceso secreta de la cuenta de cloud de Amazon EC2
- Debe tener el privilegio "list organization"
- Puerto 433 HTTPS
- Las instancias EC2 se pueden notificar como una máquina virtual o (menos naturalmente) como un host. Los volúmenes de EBS se pueden notificar como un disco virtual usado por el equipo virtual, así como un almacén de datos que proporciona la capacidad para el disco virtual.

Las claves de acceso consisten en un ID de clave de acceso (por ejemplo, AKIAIOSFONDNN7EXAMPLE) y una clave de acceso secreta (por ejemplo, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Utilice las claves de acceso para firmar solicitudes de programación que realice a EC@ si utiliza los SDK, REST o operaciones de API de consulta de Amazon EC2. Estas claves se proporcionan con su contrato de Amazon.

### Cómo configurar este origen de datos

Para configurar el origen de datos de Amazon AWS EC2, necesitará el identificador de clave de acceso IAM de AWS y la clave de acceso secreta para su cuenta de AWS.

Rellene los campos de origen de datos según las tablas siguientes:

#### Configuración:

| Campo                                                | Descripción                                                                                                                                                      |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Región de AWS                                        | Seleccione la región de AWS                                                                                                                                      |
| Rol IAM                                              | Para su uso solo cuando se adquiere en una unidad de almacenamiento AU en AWS. Consulte a continuación para obtener más información sobre las funciones del IAM. |
| ID de clave de acceso IAM de AWS                     | Introduzca el ID de clave de acceso IAM de AWS. Se requiere si no utiliza el rol IAM.                                                                            |
| Clave de acceso secreta de AWS IAM                   | Introduzca la clave de acceso secreta del IAM de AWS. Se requiere si no utiliza el rol IAM.                                                                      |
| Entiendo que AWS me facturará las solicitudes de API | Compruebe esto para saber que AWS le da la razón de las solicitudes de API que ha realizado el sondeo de Insight                                                 |

#### Configuración avanzada:

| Campo | Descripción |
|-------|-------------|
|-------|-------------|



|                                                  |                                                                                                   |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Incluir regiones adicionales                     | Especifique las regiones adicionales que se incluirán en el sondeo.                               |
| Función de cuenta cruzada                        | Función para acceder a los recursos de diferentes cuentas de AWS.                                 |
| Intervalo de sondeo de inventario (mín.)         | Intervalo entre sondeos de inventario (predeterminado 60 minutos)                                 |
| Tiempo de espera de conexión HTTP y socket (seg) | Tiempo de espera de conexión HTTP (300 segundos predeterminado)                                   |
| Incluir etiquetas de AWS                         | Haga clic en esto para habilitar la compatibilidad con etiquetas de AWS en anotaciones de Insight |
| Intervalo de sondeo de rendimiento (s)           | Intervalo entre sondeos de rendimiento (predeterminado 1800 segundos)                             |

#### Asignación de etiquetas de AWS a anotaciones de Insight

El origen de datos de AWS EC2 incluye una opción que permite completar anotaciones de Insight con etiquetas configuradas en AWS. Las anotaciones deben denominarse exactamente como etiquetas de AWS. Insight rellenará siempre anotaciones con el mismo nombre de tipo de texto y hará un "mejor intento" para rellenar anotaciones de otros tipos (número, booleano, etc.). Si la anotación es de un tipo diferente y el origen de datos no la rellena, puede ser necesario eliminar la anotación y volver a crearla como un tipo de texto.

Tenga en cuenta que AWS distingue mayúsculas de minúsculas, mientras que Insight no distingue mayúsculas de minúsculas. De este modo, si se crea una anotación denominada «PROPIETARIO» en Insight y etiquetas denominadas «PROPIETARIO», «propietario» y «propietario» en AWS, todas las variaciones de AWS del «propietario» se asignarán a la anotación de «PROPIETARIO» de Insight.

Información relacionada:

["Administración de claves de acceso para usuarios de IAM"](#)

#### Incluir regiones adicionales

En la sección AWS Data Collector **Configuración avanzada**, puede configurar el campo **incluir regiones adicionales** para que incluya regiones adicionales separadas por coma o punto y coma. De forma predeterminada, este campo se establece en **US-.\***, que recoge todas las regiones de AWS de EE.UU.. Para recopilar en *All* regiones, establezca este campo en **.\***.

Si el campo **incluir regiones adicionales** está vacío, el recopilador de datos recopilará en los activos especificados en el campo **Región de AWS** según se especifica en la sección **Configuración**.

#### Recolección de cuentas secundarias de AWS

Insight admite la colección de cuentas secundarias para AWS en un único recopilador de datos de AWS. La configuración de esta colección se realiza en el entorno AWS:

- Debe configurar cada cuenta secundaria para que tenga una función de AWS que permita que el ID de cuenta principal tenga acceso a los detalles de EC2 desde la cuenta secundaria.

- Cada cuenta secundaria debe tener el nombre de función configurado como la misma cadena
- Introduzca esta cadena de nombre de rol en la sección Insight AWS Data Collector **Configuración avanzada**, en el campo **función de cuenta cruzada**.

Práctica recomendada: Es muy recomendable asignar la directiva AmazonEC2ReadOnlyAccess predefinida de AWS a la cuenta principal de ECS. Además, el usuario configurado en el origen de datos debe tener al menos la directiva predefinida *AWSOrganizationsReadOnlyAccessPolicy* asignada para consultar a AWS.

Consulte lo siguiente para obtener información sobre la configuración de su entorno para permitir que Insight recopile desde cuentas secundarias de AWS:

["Tutorial: Delege el acceso en las cuentas de AWS mediante roles IAM"](#)

["Configuración de AWS: Proporcionando acceso a un usuario IAM en otra cuenta de AWS que posee"](#)

["Creación de un rol para delegar permisos en un usuario de IAM"](#)

### Roles IAM

Al utilizar la seguridad *IAM Role*, debe asegurarse de que el rol que cree o especifique tenga los permisos necesarios para acceder a los recursos.

Por ejemplo, si crea un rol IAM denominado *InstanceEc2ReadOnly*, debe configurar la política para conceder permiso de acceso a la lista de EC2 de solo lectura a todos los recursos EC2 de este rol IAM. Además, debe otorgar acceso STS (Security Token Service) para que esta función pueda asumir funciones en cuentas cruzadas.

Después de crear un rol IAM, puede adjuntarlo cuando crea una instancia nueva de EC2 o cualquier instancia existente de EC2.

Después de asociar el rol IAM *Instance2ReadOnly* a una instancia de EC2, podrá recuperar la credencial temporal mediante metadatos de instancia mediante el nombre del rol IAM y utilizarla para acceder a los recursos de AWS mediante cualquier aplicación que se ejecute en esta instancia de EC2.



El rol IAM se puede utilizar sólo cuando la unidad de adquisición se está ejecutando en una instancia de AWS.

### Fuente de datos de Brocade Enterprise Fabric Connectivity Manager

OnCommand Insight utiliza la fuente de datos de Brocade Enterprise Fabric Connectivity Manager (EFCM) para descubrir el inventario de los switches Brocade EFCM. Insight es compatible con las versiones 9.5, 9.6 y 9.7 de EFCM.

### Requisitos



Este recopilador de datos no está disponible a partir de OnCommand Insight 7.3.11.

- Dirección de red o nombre de dominio completo para el servidor EFCM
- La versión de EFCM debe ser 9.5, 9.6 o 9.7
- Dirección IP del servidor EFCM
- Nombre de usuario y contraseña de sólo lectura para el servidor EFCM

- Acceso validado al conmutador Connectrix mediante Telnet desde el servidor Insight, utilizando el nombre de usuario y la contraseña de sólo lectura en el puerto 51512

#### Configuración

| Campo             | Descripción                                                |
|-------------------|------------------------------------------------------------|
| Servidor EFC      | Dirección IP o nombre de dominio completo del servidor EFC |
| Nombre de usuario | Nombre de usuario del conmutador                           |
| Contraseña        | Contraseña utilizada para el conmutador                    |

#### Configuración avanzada

| Campo                                    | Descripción                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 15 minutos)                                                                                                    |
| Nombre de la estructura                  | El nombre de la estructura que debe notificar el origen de datos de EFCM. Deje en blanco para informar el nombre de la estructura como WWN.                          |
| Puerto de comunicación                   | Puerto que se utiliza para la comunicación con el switch                                                                                                             |
| Habilite el solapamiento                 | Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP.       |
| Tiempo mínimo entre solapamientos (seg)  | Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 15 segundos)                                                                 |
| Zonesets inactivos                       | Lista separada por comas de los conjuntos de zonas inactivas en los que realizar la adquisición, además de realizar la adquisición en los conjuntos de zonas activas |
| NIC para utilizar                        | Especifique la interfaz de red que se debe utilizar en la RAU al informar sobre dispositivos SAN                                                                     |
| Excluir dispositivos                     | Lista de nombres de unidades separados por comas para incluir o excluir del sondeo                                                                                   |

|                                                                          |                                                                                                       |
|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Utilice el apodo del interruptor EFCM como nombre del conmutador Insight | Seleccione esta opción para utilizar el apodo del interruptor EFCM como nombre del conmutador Insight |
| Intervalo de sondeo de rendimiento (s)                                   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                  |

## Fuente de datos del switch FC Brocade

OnCommand Insight utiliza la fuente de datos de switch FC de Brocade (SSH) para descubrir el inventario de Brocade o dispositivos de switch nuevos que ejecutan el firmware 4.2 de sistema operativo (FOS) incluido en versiones posteriores. Son compatibles los dispositivos en los modos de switch FC y Access Gateway.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de switches FC Brocade. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                       |               |
|---------------------------------------|---------------|
| Plazo del proveedor/modelo            | Insight plazo |
| Conmutador                            | Conmutador    |
| Puerto                                | Puerto        |
| Estructura virtual, estructura física | Estructura    |
| Zona                                  | Zona          |
| Cambio lógico                         | Cambio lógico |
| Zona LSAN                             | Zona IVR      |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- La unidad de adquisición (local o remota) iniciará conexiones al puerto TCP 22 en los conmutadores Brocade para recopilar datos de inventario. El AU también iniciará conexiones al puerto UDP 161 para la recopilación de datos de rendimiento.
- Debe haber conectividad IP a todos los switches de la estructura. Si selecciona la casilla de comprobación detectar todos los switches en la estructura, OCI identifica todos los switches de la estructura; sin embargo, necesita conectividad IP a estos switches adicionales para detectarlos.
- La misma cuenta es necesaria globalmente en todos los switches del entramado. Puede utilizar PuTTY (emulador de terminal de código abierto) para confirmar el acceso.

- Si se ha instalado la licencia Perform, los puertos 161 y 162 deben estar abiertos para todos los switches de la estructura para realizar el sondeo de rendimiento de SNMP.
- Cadena de comunidad de sólo lectura SNMP

#### Configuración

| Campo                    | Descripción                                                                           |
|--------------------------|---------------------------------------------------------------------------------------|
| Cambie IP                | Dirección IP o nombre de dominio completo del switch                                  |
| Nombre de usuario        | Nombre de usuario del conmutador                                                      |
| Contraseña               | Contraseña utilizada para el conmutador                                               |
| Versión de SNMP          | Versión de SNMP                                                                       |
| Cadena de comunidad SNMP | Cadena de comunidad de sólo lectura de SNMP que se utiliza para acceder al conmutador |
| Nombre de usuario SNMP   | Nombre de usuario del protocolo de versión SNMP (sólo se aplica a SNMP v3)            |
| Contraseña SNMP          | Contraseña de protocolo de versión SNMP (sólo se aplica a SNMP v3)                    |

#### Configuración avanzada

| Campo                                    | Descripción                                                                                                                 |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Nombre de la estructura                  | El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN. |
| Excluir dispositivos                     | Lista separada por comas de ID de dispositivo que se van a excluir del sondeo                                               |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 15 minutos)                                                           |
| Tiempo de espera (s)                     | Tiempo de espera de conexión (30 segundos predeterminado)                                                                   |
| Tiempo de espera del banner (s)          | Tiempo de espera del banner SSH (5 segundos predeterminado)                                                                 |
| Dominios de administración activos       | Seleccione si utiliza dominios de administración                                                                            |

|                                            |                                                                                                                                                                |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Recuperar datos MPR                        | Seleccione esta opción para adquirir datos de enrutamiento desde su enrutador multiprotocolo (MPR)                                                             |
| Habilite el solapamiento                   | Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP. |
| Tiempo mínimo entre solapamientos (seg)    | Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)                                                           |
| Descubra todos los switches del entramado  | Seleccione para detectar todos los switches de la estructura                                                                                                   |
| Elija favorecer HBA frente a Alias de zona | Elija si prefiere los alias de HBA o de zona                                                                                                                   |
| Intervalo de sondeo de rendimiento (s)     | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                                                                           |
| Protocolo de autenticación SNMP            | Protocolo de autenticación SNMP (solo SNMP v3)                                                                                                                 |
| Protocolo de privacidad SNMP               | Protocolo de privacidad SNMP (sólo SNMP v3)                                                                                                                    |
| Contraseña de privacidad de SNMP           | Contraseña de privacidad de SNMP (sólo SNMP v3)                                                                                                                |
| Reintentos SNMP                            | Número de intentos de reintento SNMP                                                                                                                           |
| Tiempo de espera de SNMP (ms)              | Tiempo de espera de SNMP (5000 ms predeterminado)                                                                                                              |

### Fuente de datos Brocade Sphereon/Intrepid Switch

OnCommand Insight utiliza la fuente de datos Brocade Sphereon/Intrepid Switch (SNMP) para descubrir el inventario de switches Brocade Sphereon o Intrepid.

#### Requisitos



Este recopilador de datos no está disponible a partir de OnCommand Insight 7.3.11.

- Debe haber conectividad IP a todos los switches de la estructura. Si selecciona la casilla de comprobación detectar todos los switches en la estructura, OCI identifica todos los switches de la estructura; sin embargo, necesita conectividad IP a estos switches adicionales para detectarlos.
- Cadena de comunidad de sólo lectura si se utiliza SNMP V1 o SNMP V2.
- Acceso HTTP al switch para obtener información de división en zonas.

- Acceda a la validación ejecutando el `snmpwalk` utilidad para el interruptor (consulte `<install_path>\>\bin\`).

### Configuración

| Campo               | Descripción                                                                           |
|---------------------|---------------------------------------------------------------------------------------|
| Conmutador Sphereon | Dirección IP o nombre de dominio completo del switch                                  |
| Versión de SNMP     | Versión de SNMP                                                                       |
| Comunidad SNMP      | Cadena de comunidad de sólo lectura de SNMP que se utiliza para acceder al conmutador |
| Nombre de usuario   | Nombre de usuario SMI-S para el conmutador (sólo SNMP v3)                             |
| Contraseña          | Contraseña SMI-S para el conmutador (sólo SNMP v3)                                    |

### Configuración avanzada

| Campo                                    | Descripción                                                                                                                                                    |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 15 minutos)                                                                                              |
| Protocolo de autenticación SNMP          | Protocolo de autenticación SNMP (sólo SNMPv3)                                                                                                                  |
| Protocolo de privacidad SNMP             | Protocolo de privacidad SNMP (sólo SNMPv3)                                                                                                                     |
| Contraseña de privacidad de SNMP         | Contraseña de privacidad de SNMP                                                                                                                               |
| Número SNMP de reintentos                | Número de intentos de reintento SNMP                                                                                                                           |
| Tiempo de espera de SNMP (ms)            | Tiempo de espera de SNMP (5000 ms predeterminado)                                                                                                              |
| Nombre de la estructura                  | El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN.                                    |
| Habilite el solapamiento                 | Seleccione esta opción para activar la adquisición al recibir una captura SNMP del dispositivo. Si selecciona Activar solapamiento, también debe activar SNMP. |

|                                              |                                                                                                      |
|----------------------------------------------|------------------------------------------------------------------------------------------------------|
| Tiempo mínimo entre solapamientos (segundos) | Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos) |
| Intervalo de sondeo de rendimiento (s)       | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                 |

### Origen de datos de firmware de switch FC de Cisco (SNMP)

OnCommand Insight usa el origen de datos 2.0+ (SNMP) del firmware de switch FC de Cisco para detectar el inventario de switches Fibre Channel de Cisco MDS, así como una variedad de switches FCoE de Cisco Nexus en los que se ha habilitado el servicio FC. Además, puede descubrir muchos modelos de dispositivos Cisco que se ejecutan en modo NPV con este origen de datos.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de Cisco FC Switch. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                       |                                 |
|---------------------------------------|---------------------------------|
| Plazo del proveedor/modelo            | Insight plazo                   |
| Conmutador                            | Conmutador                      |
| Puerto                                | Puerto                          |
| VSAN                                  | Estructura                      |
| Zona                                  | Zona                            |
| Cambio lógico                         | Cambio lógico                   |
| Entrada del servidor de nombres       | Entrada del servidor de nombres |
| Zona de enrutamiento entre VSAN (IVR) | Zona IVR                        |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP de un switch en la estructura o en los switches individuales
- Detección del chasis para habilitar la detección de estructura
- Si se utiliza SNMP V2, cadena de comunidad de sólo lectura
- El puerto 161 se utiliza para acceder al dispositivo



- Validación de acceso mediante la `snmpwalk` utilidad para el interruptor (consulte `<install_path>\>\bin\`)

### Configuración

| Campo                    | Descripción                                                                                                   |
|--------------------------|---------------------------------------------------------------------------------------------------------------|
| Switch IP de Cisco       | Dirección IP o nombre de dominio completo del switch                                                          |
| Versión de SNMP          | Se requiere SNMP versión v2 o posterior para la adquisición del rendimiento                                   |
| Cadena de comunidad SNMP | Cadena de comunidad de solo lectura de SNMP que se utiliza para acceder al switch (no aplicable para SNMP v3) |
| Nombre de usuario        | Nombre de usuario para el conmutador (sólo SNMP v3)                                                           |
| Contraseña               | Contraseña utilizada para el conmutador (sólo SNMPv3)                                                         |

### Configuración avanzada

| Campo                                    | Descripción                                                                                                                     |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                                               |
| Protocolo de autenticación SNMP          | Protocolo de autenticación SNMP (sólo SNMPv3)                                                                                   |
| Protocolo de privacidad SNMP             | Protocolo de privacidad SNMP (sólo SNMPv3)                                                                                      |
| Contraseña de privacidad de SNMP         | Contraseña de privacidad de SNMP                                                                                                |
| Reintentos SNMP                          | Número de intentos de reintento SNMP                                                                                            |
| Tiempo de espera de SNMP (ms)            | Tiempo de espera de SNMP (5000 ms predeterminado)                                                                               |
| Habilite el solapamiento                 | Seleccione esta opción para activar el solapamiento. Si habilita el solapamiento, también debe activar las notificaciones SNMP. |
| Tiempo mínimo entre solapamientos (seg)  | Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)                            |

|                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descubra los switches de la estructura | Seleccione para detectar todos los switches de la estructura                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Excluir dispositivos                   | Lista separada por comas de IP de dispositivo que se van a excluir del sondeo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Incluir dispositivos                   | Lista separada por comas de IP de dispositivo que se van a incluir en el sondeo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Compruebe el tipo de dispositivo       | Seleccione esta opción para aceptar sólo los dispositivos que se anuncian explícitamente como dispositivos Cisco                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Tipo de alias principal                | <p>Proporcione una primera preferencia para la resolución del alias. Elija una de las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <b>Alias del dispositivo</b> <p>Este es un nombre descriptivo de usuario de un WWN de puerto (pWWN) que se puede utilizar en todos los comandos de configuración, según sea necesario. Todos los switches de la familia Cisco MDS 9000 admiten Distributed Device Alias Services (alias de dispositivo).</p> </li> <li>• <b>Ninguno</b> <p>No informe ningún alias</p> </li> <li>• <b>Descripción del puerto</b> <p>Una descripción que ayuda a identificar el puerto en una lista de puertos</p> </li> <li>• <b>Alias de zona (todos)</b> <p>Un nombre descriptivo para el usuario de un puerto que solo se puede utilizar para la configuración de división en zonas</p> </li> <li>• <b>Alias de zona (sólo activo)</b> <p>Nombre descriptivo para un puerto que solo se puede utilizar para la configuración activa. Este es el valor predeterminado.</p> </li> </ul> |
| Tipo de alias secundario               | Proporcione una segunda preferencia para la resolución del alias                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                                                           |                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Tipo de alias terciario                                   | Proporcione una tercera preferencia para la resolución del alias                                                                     |
| Habilite la compatibilidad con el modo de proxy de SANTap | Seleccione si el conmutador Cisco está utilizando SANTap en modo proxy. Si utiliza EMC RecoverPoint, es probable que utilice SANTap. |
| Intervalo de sondeo de rendimiento (s)                    | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                                                 |

### Fuente de datos de EMC Celerra

El origen de datos de Celerra (SSH) recopila información de inventario de sistemas de almacenamiento de Celerra. Para la configuración, este origen de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de \_sólo lectura.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC Celerra. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                          |                                |
|----------------------------------------------------------|--------------------------------|
| Plazo del proveedor/modelo                               | Insight plazo                  |
| Servidor de red Celerra                                  | Reducida                       |
| Meta Volume de Celerra/Pool de almacenamiento de Celerra | Pool de almacenamiento         |
| Sistema de archivos                                      | Volumen interno                |
| Transmisor de datos                                      | Controladora                   |
| Sistema de archivos montado en un transmisor de datos    | Recurso compartido de archivos |
| Exportaciones CIFS y NFS                                 | Share                          |
| Volumen de disco                                         | LUN back-end                   |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- La dirección IP del procesador de almacenamiento

- Nombre de usuario y contraseña de solo lectura
- Puerto SSH 22

### Configuración

| Campo                | Descripción                                                        |
|----------------------|--------------------------------------------------------------------|
| Dirección de Celerra | Dirección IP o nombre de dominio completo del dispositivo Celerra  |
| Nombre de usuario    | Nombre utilizado para iniciar sesión en el dispositivo Celerra     |
| Contraseña           | Contraseña utilizada para iniciar sesión en el dispositivo Celerra |

### Configuración avanzada

| Campo                                       | Descripción                                                       |
|---------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (minutos) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |
| Tiempo de espera del proceso SSH (s)        | Tiempo de espera del proceso SSH (600 segundos predeterminado)    |
| Número de reintentos                        | Número de intentos de reintento de inventario                     |
| Tiempo de espera del banner SSH (s)         | Tiempo de espera del banner SSH (20 segundos predeterminado)      |

### Fuente de datos EMC CLARiiON (NaviCLI)

Antes de configurar este origen de datos, asegúrese de que la CLI de EMC Navisphere está instalada en el dispositivo de destino y en el servidor de Insight. La versión de la CLI de Navisphere debe coincidir con la versión de firmware de la controladora. Para la recogida de datos de rendimiento, se debe activar el registro de estadísticas.

### Sintaxis de la interfaz de línea de comandos de Navisphere

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope, use 0 for global scope> -port <use 443 by default> command
```

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC CLARiiON. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en

este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                              |                        |
|------------------------------|------------------------|
| Plazo del proveedor/modelo   | Insight plazo          |
| Disco                        | Disco                  |
| Reducida                     | Reducida               |
| Procesador de almacenamiento | Nodo de almacenamiento |
| Thin Pool y grupo RAID       | Pool de almacenamiento |
| LUN                          | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP de cada procesador de almacenamiento CLARiiON
- Nombre de usuario y contraseña de sólo lectura de Navisphere en las matrices CLARiiON
- Navicli debe instalarse en Insight Server/RAU
- Validación de acceso: Ejecute NaviCLI desde el servidor de Insight a cada matriz utilizando el nombre de usuario y la contraseña anteriores.
- La versión navicli debe corresponder con el código DE BROTE más reciente de la matriz
- Para mejorar el rendimiento, se debe activar el registro de estadísticas.
- Requisitos de los puertos: 80, 443

### Configuración

| Campo                                                    | Descripción                                                                            |
|----------------------------------------------------------|----------------------------------------------------------------------------------------|
| Almacenamiento CLARiiON                                  | La dirección IP o el nombre de dominio completo de CLARiiON Storage                    |
| Nombre de usuario                                        | Nombre utilizado para iniciar sesión en el dispositivo de almacenamiento CLARiiON.     |
| Contraseña                                               | Contraseña utilizada para iniciar sesión en el dispositivo de almacenamiento CLARiiON. |
| La ruta de la CLI a la ruta navicli.exe o naviseccli.exe | Ruta completa a la <code>navicli.exe</code> O. <code>naviseccli.exe</code> ejecutable  |

## Configuración avanzada

| Campo                                                   | Descripción                                                          |
|---------------------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                | Intervalo entre sondeos de inventario (predeterminado 40 minutos)    |
| Usar cliente seguro (naviseccli)                        | Seleccionar para utilizar cliente seguro (navseccli)                 |
| Ámbito                                                  | Ámbito de cliente seguro. El valor predeterminado es Global.         |
| Puerto CLI de CLARiiON                                  | Puerto utilizado para la CLI de CLARiiON                             |
| Tiempo de espera de proceso externo de inventario (seg) | Tiempo de espera de proceso externo (predeterminado 1800 segundos)   |
| Intervalo de sondeo de rendimiento (s)                  | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |
| Tiempo de espera de proceso externo de rendimiento (s)  | Tiempo de espera de proceso externo (predeterminado 1800 segundos)   |

## Fuente de datos de EMC Data Domain

Este origen de datos recopila información de almacenamiento y configuración de los sistemas de almacenamiento de deduplicación de EMC Data Domain. Para añadir el origen de datos, debe utilizar instrucciones y comandos de configuración específicos, así como tener en cuenta los requisitos del origen de datos y las recomendaciones de uso.

## Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de EMC Data Domain. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo | Insight plazo   |
|----------------------------|-----------------|
| Disco                      | Disco           |
| Cabina                     | Reducida        |
| Puerto                     | Puerto          |
| Archivos                   | Volumen interno |
| MTree                      | Qtree           |

|                     |           |
|---------------------|-----------|
| Cuota               | Cuota     |
| Unidades NFS y CIFS | Fileshare |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

#### Requisitos

- Dirección IP del dispositivo Data Domain
- Nombre de usuario y contraseña de sólo lectura para el almacenamiento de Data Domain
- Puerto SSH 22

#### Configuración

| Campo             | Descripción                                                                                |
|-------------------|--------------------------------------------------------------------------------------------|
| Dirección IP      | La dirección IP o el nombre de dominio completo de la cabina de almacenamiento Data Domain |
| Nombre de usuario | El nombre de usuario para la cabina de almacenamiento Data Domain                          |
| Contraseña        | La contraseña de la cabina de almacenamiento de Data Domain                                |

#### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |
| Tiempo de espera del proceso SSH (s)     | Tiempo de espera del proceso SSH (180 segundos predeterminado)    |
| Puerto SSH                               | Puerto del servicio SSH                                           |

#### Fuente de datos de EMC ECC StorageScope

El dispositivo StorageScope EMC ECC tiene tres tipos de fuentes de datos: 5.x, 6.0 y 6.1.

#### Configuración



Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

| <b>Campo</b>      | <b>Descripción</b>                                         |
|-------------------|------------------------------------------------------------|
| Servidor ECC      | Dirección IP o nombre de dominio completo del servidor ECC |
| Nombre de usuario | Nombre de usuario del servidor ECC                         |
| Contraseña        | Password r el servidor ECC                                 |

#### Configuración avanzada

| <b>Campo</b>                                  | <b>Descripción</b>                                                                  |
|-----------------------------------------------|-------------------------------------------------------------------------------------|
| Puerto ECC                                    | Puerto utilizado para el servidor ECC                                               |
| Intervalo de sondeo de inventario (mín.)      | Intervalo entre sondeos de inventario (predeterminado 30 minutos)                   |
| Protocolo para conectarse a la base de datos  | Protocolo utilizado para conectarse a la base de datos                              |
| Consultar Información del sistema de archivos | Seleccione esta opción para recuperar detalles de alias WWN y sistemas de archivos. |

#### Fuente de datos de Dell EMC ECS

Este recopilador de datos adquiere datos de inventario y rendimiento de los sistemas de almacenamiento de EMC ECS. Para la configuración, el recopilador de datos requiere una dirección IP del servidor ECS y una cuenta de dominio de nivel administrativo.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de EMC ECS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Cluser                     | Reducida               |
| Inquilino                  | Pool de almacenamiento |
| Cucharón                   | Volumen interno        |
| Disco                      | Disco                  |





Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP de la consola de administración de ECS
- Cuenta de dominio de nivel administrativo para el sistema ECS
- Puerto 443 (HTTPS). Requiere conectividad saliente al puerto TCP 443 del sistema ECS.
- Para obtener rendimiento, nombre de usuario y contraseña de solo lectura para acceso a ssh/scp.
- Para el rendimiento, se necesita el puerto 22.

### Configuración

| Campo                  | Descripción                                                   |
|------------------------|---------------------------------------------------------------|
| Host ECS               | Direcciones IP o nombres de dominio completos del sistema ECS |
| Puerto de host ECS     | Puerto utilizado para la comunicación con el host ECS         |
| ID de proveedor de ECS | ID de proveedor de ECS                                        |
| Contraseña             | Contraseña utilizada para ECS                                 |

### Configuración avanzada

| Campo                                       | Descripción                                                                    |
|---------------------------------------------|--------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (minutos) | Intervalo entre sondeos de inventario. El valor predeterminado es 360 minutos. |

### Fuente de datos de EMC Isilon

La fuente de datos SSH de Isilon recopila inventario y rendimiento del almacenamiento NAS de escalabilidad horizontal de EMC Isilon.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a través de la fuente de datos de EMC Isilon. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |               |
|----------------------------|---------------|
| Plazo del proveedor/modelo | Insight plazo |
| Unidad                     | Disco         |

|                     |                        |
|---------------------|------------------------|
| Clúster             | Reducida               |
| Nodo                | Nodo de almacenamiento |
| Sistema de archivos | Volumen interno        |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Permisos de administrador para el almacenamiento Isilon
- Acceso validado mediante `telnet` al puerto 22

### Configuración

| Campo             | Descripción                                                        |
|-------------------|--------------------------------------------------------------------|
| Dirección IP      | La dirección IP o el nombre de dominio completo del clúster Isilon |
| Nombre de usuario | El nombre de usuario del clúster Isilon                            |
| Contraseña        | La contraseña del clúster de Isilon                                |

### Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)    |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |
| Tiempo de espera del proceso SSH         | Tiempo de espera del proceso SSH (60 segundos predeterminado)        |
| Puerto SSH                               | Puerto del servicio SSH                                              |

### Ejecutando comandos de la CLI

A partir de OnCommand Insight versión 7.3.11 y Service Pack 9, la fuente de datos de EMC Isilon contiene una mejora que hará que Insight ejecute más comandos de la CLI. Si utiliza un usuario que no es raíz dentro de su origen de datos, es probable que haya configurado un archivo "sudoers" para otorgar a esa cuenta de usuario la capacidad de ejecutar comandos CLI específicos a través de SSH.

Para que Insight comprenda la función "zonas de acceso" de EMC, Insight ejecutará ahora, además, los

siguientes nuevos comandos CLI:

- `sudo isi zone zones list --format json -verbose`
- `sudo isi zone zones list`

Insight analiza el resultado de estos comandos y ejecuta más instancias de comandos existentes para obtener la configuración lógica de objetos como qtrees, cuotas y recursos compartidos/exportaciones NAS que residen en zonas de acceso no predeterminadas. Insight ahora informa de esos objetos para zonas de acceso no predeterminadas como resultado de esta mejora. A medida que Insight obtiene los datos ejecutando comandos existentes (con opciones diferentes), no se requiere ningún cambio en el archivo de sudoers para que funcionen; sólo con la introducción de los nuevos comandos anteriores es necesario el cambio.

Actualice el archivo sudoers para permitir que su cuenta de servicio de Insight ejecute esos comandos antes de actualizar a esta versión de Insight. De lo contrario, sus orígenes de datos de Isilon fracasarán.

### Estadísticas de "sistema de archivos"

A partir de OnCommand Insight 7.3.12, el recopilador de datos de EMC Isilon introduce estadísticas de "sistema de archivos" sobre el objeto de nodo para EMC Isilon. Las estadísticas del nodo existentes indicadas por OnCommand Insight se basan en el "disco", es decir, para IOPS y rendimiento de un nodo de almacenamiento. ¿Qué hacen los discos de este nodo en el agregado? Sin embargo, para las cargas de trabajo donde se almacenan en caché las lecturas en la memoria o la compresión, la carga de trabajo del sistema de archivos puede ser significativamente superior a lo que afecta a los discos. Un conjunto de datos que comprime 5:1 podría tener un valor de "rendimiento de lectura del sistema de archivos" cinco veces el rendimiento de lectura del nodo de almacenamiento. esta última mide las lecturas del disco, que se expanden cinco veces cuando el nodo descomprime los datos para atender la solicitud de lectura del cliente.

### Fuente de datos Dell EMC PowerStore

El recopilador de datos Dell EMC PowerStore recopila información de inventario del sistema de almacenamiento Dell EMC PowerStore. Para la configuración, el recopilador de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de sólo lectura.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir de la fuente de datos de EMC Data Domain. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo                                      | Insight plazo           |
|-----------------------------------------------------------------|-------------------------|
| host                                                            | host                    |
| asignación_volumen_host                                         | asignación_volumen_host |
| Hardware (tiene unidades bajo objeto "extra_details"): Unidades | Disco                   |
| Dispositivo                                                     | StoragePool             |

|                     |                          |
|---------------------|--------------------------|
| Clúster             | Cabina de almacenamiento |
| Nodo                | Nodo de almacenamiento   |
| puerto_fc           | Puerto                   |
| volumen             | Volumen                  |
| InternalVolume      | sistema_de_archivos      |
| Archivos            | Volumen interno          |
| MTree               | Qtree                    |
| Cuota               | Cuota                    |
| Unidades NFS y CIFS | Fileshare                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura

### Se explica el número de serie padre

Tradicionalmente, Insight es capaz de generar informes sobre el número de serie de la cabina de almacenamiento o los números de serie de cada nodo de almacenamiento. Sin embargo, algunas arquitecturas de cabinas de almacenamiento no se alinean correctamente con esto. Un clúster PowerStore puede estar compuesto por 1-4 dispositivos y cada dispositivo tiene 2 nodos. Si el dispositivo en sí tiene un número de serie, ese número de serie no es ni el número de serie del clúster ni los nodos.

El atributo "número de serie principal" en el objeto del nodo de almacenamiento se rellena de forma adecuada para las matrices Dell/EMC PowerStore cuando los nodos individuales se encuentran dentro de un dispositivo/gabinete intermedio que es sólo parte de un clúster mayor.

### Configuración

| Campo                        | Descripción                                                                |
|------------------------------|----------------------------------------------------------------------------|
| Puertas de enlace PowerStore | Direcciones IP o nombres de dominio completos de almacenamiento PowerStore |
| Nombre de usuario            | Nombre de usuario de PowerStore                                            |

|            |                                  |
|------------|----------------------------------|
| Contraseña | Contraseña usada para PowerStore |
|------------|----------------------------------|

### Configuración avanzada

| Campo                                       | Descripción                                                                   |
|---------------------------------------------|-------------------------------------------------------------------------------|
| Puerto HTTPS                                | El valor predeterminado es 443                                                |
| Intervalo de sondeo de inventario (minutos) | Intervalo entre sondeos de inventario. El valor predeterminado es 60 minutos. |

La colección de rendimiento PowerStore de OnCommand Insight utiliza los datos de fuente de granularidad de 5 minutos de PowerStore. De este modo, Insight sondea esos datos cada cinco minutos; por el contrario, no se puede configurar.

### Fuente de datos de EMC RecoverPoint

El origen de datos de EMC RecoverPoint recopila información de inventario del almacenamiento de EMC RecoverPoint. Para la configuración, el origen de datos requiere la dirección IP de los procesadores de almacenamiento y un nombre de usuario y contraseña de \_sólo lectura.

El origen de datos de EMC RecoverPoint recopila las relaciones de replicación de volumen a volumen que RecoverPoint coordina en otras cabinas de almacenamiento. OnCommand Insight muestra una cabina de almacenamiento para cada clúster RecoverPoint, y recopila datos de inventario de los nodos y los puertos de almacenamiento de ese clúster. No se recopilan datos de volúmenes o pool de almacenamiento.

### Requisitos

- Dirección IP o nombre de dominio completo del procesador de almacenamiento
- Nombre de usuario y contraseña de solo lectura
- Acceso a API DE REST a través del puerto 443
- Acceso SSH a través de PuTTY

### Configuración

| Campo                     | Descripción                                                        |
|---------------------------|--------------------------------------------------------------------|
| Dirección de RecoverPoint | Dirección IP o nombre de dominio completo del clúster RecoverPoint |
| Nombre de usuario         | Nombre de usuario del clúster RecoverPoint                         |
| Contraseña                | Contraseña del clúster RecoverPoint                                |

### Configuración avanzada

| Campo                                       | Descripción                                                                                 |
|---------------------------------------------|---------------------------------------------------------------------------------------------|
| Puerto TCP                                  | Puerto TCP utilizado para conectarse al clúster RecoverPoint                                |
| Intervalo de sondeo de inventario (minutos) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)                           |
| Clústeres excluidos                         | Lista de nombres o ID de clúster separados por comas para excluirllos al realizar el sondeo |

### Habilitador de soluciones EMC con fuente de datos de rendimiento SMI-S.

OnCommand Insight descubre las cabinas de almacenamiento Symmetrix mediante el uso del habilitador de soluciones `symcli` Comandos junto con un servidor existente del capacitador de soluciones de su entorno. El servidor existente de Solution facilitadora tiene conectividad con la cabina de almacenamiento de Symmetrix mediante el acceso a volúmenes de gatekeeper. Se requieren permisos de administrador para acceder a este dispositivo.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos del habilitador de soluciones de EMC. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                                 |                        |
|-----------------------------------------------------------------|------------------------|
| Plazo del proveedor/modelo                                      | Insight plazo          |
| Disco                                                           | Disco                  |
| Grupo de discos                                                 | Grupo de discos        |
| Cabina de almacenamiento                                        | Reducida               |
| Director                                                        | Nodo de almacenamiento |
| Grupo de dispositivos, pool de recursos de almacenamiento (SRP) | Pool de almacenamiento |
| Dispositivo, TDev                                               | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

Antes de configurar este origen de datos, debe asegurarse de que el servidor OnCommand Insight tiene conectividad TCP con el puerto 2707 del servidor existente del capacitador de soluciones. OnCommand Insight descubre todos los arreglos Symmetrix que son "local" de este servidor, como se ve en la salida "lista de DYcfg" de ese servidor.

- El habilitador de soluciones de EMC (CLI) con la aplicación del proveedor SMI-S debe estar instalado y la versión debe coincidir o ser anterior a la versión que se ejecuta en el servidor de capacitadores de soluciones.
- Un configurado correctamente `{installdir}\EMC\SYMAPI\config\netcnfg` el archivo es obligatorio. Este archivo define los nombres de servicio de los servidores de Solution facilitation, así como el método de acceso (SECURE / NOSECURE /ANY).
- Si necesita una latencia de lectura/escritura a nivel de nodo de almacenamiento, SMI-S Provider debe comunicarse con una instancia en ejecución de UNISPHERE para la aplicación VMAX.
- Permisos de administrador en el servidor del habilitador de soluciones (se)
- Nombre de usuario y contraseña de sólo lectura para el software se
- Requisitos DEL solutions facilitadora SERVER 6.5X:
  - Proveedor SMI-S 3.3.1 para SMIS-S V1.2 instalado
  - Después de la instalación, ejecute `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- LA aplicación UNISPHERE para VMAX debe ejecutar y recopilar estadísticas para las cabinas de almacenamiento Symmetrix VMAX que se gestionan mediante la instalación del proveedor SMI-S
- Validación de acceso: Verifique que el proveedor de SMI-S esté en ejecución: `telnet <se_server> 5988`

## Configuración



Si la autenticación de usuario de SMI-S no está habilitada, se ignoran los valores predeterminados en el origen de datos de OnCommand Insight.


El hecho de tener activado symauth en cabinas Symmetrix puede inhibir la capacidad de OnCommand Insight para descubrirlas. OnCommand Insight Acquisition se ejecuta como usuario DEL SISTEMA en el servidor de OnCommand Insight / Unidad de adquisición remota que se comunica con el servidor de facilitadores de soluciones. Si hostname\SYSTEM no tiene privilegios symauth, OnCommand Insight no puede detectar la matriz.

La fuente de datos de la CLI de Symmetrix facilitadora de soluciones de EMC incluye soporte para la configuración de dispositivos para thin provisioning y Symmetrix Remote Data Facility (SRDF).

Se proporcionan definiciones para los paquetes Fibre Channel y Switch Performance.

| Campo                  | Descripción                                                 |
|------------------------|-------------------------------------------------------------|
| Nombre del servicio    | Nombre de servicio como se especifica en el archivo netcnfg |
| Ruta completa a la CLI | Ruta completa a la CLI de Symmetrix                         |

## Configuración avanzada

| Campo                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Excluir dispositivos de inventario                     | Lista separada por comas de los ID de dispositivo que se van a incluir o excluir                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Almacenamiento en caché de conexión                    | <p>Elija el método de almacenamiento en caché de conexión:</p> <ul style="list-style-type: none"> <li>• LOCAL significa que el servicio de adquisición de OnCommand Insight se está ejecutando en el servidor de Solution facilitadora, que tiene conectividad Fibre Channel con los arreglos de Symmetrix que desea detectar y tiene acceso a volúmenes de gatekeeper. Esto puede verse en algunas configuraciones de la unidad de adquisición remota (RAU).</li> <li>• REMOTE_CACHED es el valor predeterminado y se debe utilizar en la mayoría de los casos. De este modo, se utiliza la configuración del archivo NETTNFG para conectar mediante IP con el servidor Solutions facilitadora, que debe tener conectividad Fibre Channel con los arreglos Symmetrix que busca detectar y tener acceso a los volúmenes de Gatekeeper.</li> <li>• Si las opciones REMOTE_CACHE hacen que los comandos de la CLI fallen, utilice la opción REMOTE. Tenga en cuenta que ralentizará el proceso de adquisición (posiblemente a horas o incluso días en casos extremos). La configuración del archivo NETTNFG se sigue utilizando para una conexión IP con el servidor Solutions facilitadora que tenga conectividad Fibre Channel con los arreglos Symmetrix que se van a detectar.</li> </ul> <div>  <p>Esta configuración no cambia el comportamiento de OnCommand Insight con respecto a las matrices enumeradas COMO REMOTAS mediante la salida "symcfg list". OnCommand Insight recopila datos sólo en los dispositivos que se muestran COMO LOCALES mediante este comando.</p> </div> |



|                                                |                                                                                                         |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Tiempo de espera de la CLI (s)                 | Tiempo de espera del proceso de la CLI (7200 segundos predeterminados)                                  |
| IP DEL HOST DE SMI-S.                          | Dirección IP del host del proveedor SMI-S.                                                              |
| Puerto SMI-S.                                  | Puerto que utiliza el host del proveedor SMI-S.                                                         |
| Protocolo                                      | Protocolo utilizado para conectar con el proveedor SMI-S.                                               |
| Espacio de nombres SMI-S.                      | Espacio de nombres de interoperabilidad que el proveedor SMI-S está configurado para utilizar           |
| Nombre de usuario de SMI-S.                    | Nombre de usuario para el host del proveedor de SMI-S.                                                  |
| Contraseña SMI-S.                              | Nombre de usuario para el host del proveedor de SMI-S.                                                  |
| Intervalo de sondeo de rendimiento (s)         | Intervalo entre sondeos de rendimiento (predeterminado 1000 segundos)                                   |
| Tipo de filtro de rendimiento                  | Especifique si desea incluir o excluir la siguiente lista de matrices al recopilar datos de rendimiento |
| Lista de dispositivos de filtro de rendimiento | Lista separada por comas de los ID de dispositivo que se van a incluir o excluir                        |
| Intervalo de sondeo de RPO (s)                 | Intervalo entre sondeos RPO (predeterminado 300 segundos)                                               |

### Fuente de datos de EMC VNX

Para la configuración, el origen de datos de EMC VNX (SSH) requiere la dirección IP de Control Station y un nombre de usuario y contraseña de sólo lectura.

#### Configuración

| Campo                    | Descripción                                                      |
|--------------------------|------------------------------------------------------------------|
| VNX IP                   | Dirección IP o nombre de dominio completo de VNX Control Station |
| Nombre de usuario de VNX | Nombre de usuario de VNX Control Station                         |
| Contraseña de VNX        | Contraseña de VNX Control Station                                |

## Requisitos

- Dirección IP de la estación de control
- Nombre de usuario y contraseña de solo lectura.
- Validación de acceso: Verifique el acceso SSH a través de PuTTY.

## Configuración avanzada

| Campo                                                                  | Descripción                                                                                    |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                               | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                              |
| Tiempo de espera del proceso de SSH de VNX (s)                         | Tiempo de espera del proceso VNX SSH (predeterminado 600 segundos)                             |
| Intentos de reintento de comando Celerra                               | Número de intentos de reintento de comando Celerra                                             |
| Tiempo de espera de proceso externo de CLARiiON para inventario (seg)  | Tiempo de espera de proceso externo de CLARiiON para inventario (predeterminado 1800 segundos) |
| Intervalo de sondeo de rendimiento (s)                                 | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                           |
| Tiempo de espera de proceso externo de CLARiiON para rendimiento (seg) | Tiempo de espera de proceso externo CLARiiON para rendimiento (predeterminado: 1800 segundos)  |

## Fuente de datos VNXe de EMC

La fuente de datos VNXe de EMC proporciona compatibilidad de inventario para cabinas de almacenamiento unificado VNXe y Unity de EMC.

Este origen de datos está basado en CLI y requiere que instale Unisphere en la CLI de VNXe (uemcli.exe) en la unidad de adquisición en la que reside el origen de datos de VNXe. uemcli.exe utiliza HTTPS como protocolo de transporte, por lo que la unidad de adquisición debe poder iniciar conexiones HTTPS con las matrices VNXe/Unity. Debe tener al menos un usuario de sólo lectura para que lo utilice el origen de datos.

## Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de EMC VNXe. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |               |
|----------------------------|---------------|
| Plazo del proveedor/modelo | Insight plazo |
| Disco                      | Disco         |
| Cabina de almacenamiento   | Reducida      |

|                                                              |                            |
|--------------------------------------------------------------|----------------------------|
| Procesador                                                   | Nodo de almacenamiento     |
| Pool de almacenamiento                                       | Pool de almacenamiento     |
| Información general sobre el bloque de iSCSI, VMFS de VMware | Volumen                    |
| Carpeta compartida                                           | Volumen interno            |
| CIFS Share, NFS Share, Share from VMware NFS datastore       | Share                      |
| Sistema remoto con replicación                               | Sincronización             |
| Nodo iSCSI                                                   | Nodo de destino iSCSI      |
| Iniciador iSCSI                                              | Iniciador de destino iSCSI |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

A continuación, se enumeran los requisitos para configurar y utilizar este origen de datos:

- El recopilador de datos de VNXe depende de la interfaz de línea de comandos; debe instalar Unisphere en la CLI de VNXe (uemcli.exe) en la unidad de adquisición donde reside el recopilador de datos de VNXe.
- uemcli.exe utiliza HTTPS como protocolo de transporte, de modo que la unidad de adquisición deberá poder iniciar conexiones HTTPS con el VNXe.
- Debe tener al menos un usuario de sólo lectura para que lo utilice el origen de datos.
- Dirección IP del servidor de activación de soluciones de gestión.
- Se requiere HTTPS en el puerto 443
- El recopilador de datos de EMC VNXe proporciona compatibilidad con iSCSI y NAS para el inventario; se descubrirán volúmenes de Fibre Channel, pero Insight no informará sobre los puertos de almacenamiento, enmascaramiento ni asignación de FC.

## Configuración

| Campo               | Descripción                                                          |
|---------------------|----------------------------------------------------------------------|
| Almacenamiento VNXe | La dirección IP o el nombre de dominio completo del dispositivo VNXe |
| Nombre de usuario   | Nombre de usuario del dispositivo VNXe                               |
| Contraseña          | Contraseña del dispositivo VNXe                                      |

|                                    |                                          |
|------------------------------------|------------------------------------------|
| Ruta completa al ejecutable uemcli | Ruta completa a la uemcli.exe ejecutable |
|------------------------------------|------------------------------------------|

### Configuración avanzada

| Campo                                                   | Descripción                                                        |
|---------------------------------------------------------|--------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                | Intervalo entre sondeos de inventario (predeterminado 40 minutos)  |
| Puerto CLI de VNXe                                      | Puerto utilizado para la CLI de VNXe                               |
| Tiempo de espera de proceso externo de inventario (seg) | Tiempo de espera de proceso externo (predeterminado 1800 segundos) |

### Fuente de datos de EMC VPLEX

Para la configuración, este origen de datos requiere una dirección IP del servidor VPLEX y una cuenta de dominio de nivel administrativo.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de EMC VPLEX. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                        |                                     |
|--------------------------------------------------------|-------------------------------------|
| Plazo del proveedor/modelo                             | Insight plazo                       |
| Clúster                                                | Reducida                            |
| Motor                                                  | Nodo de almacenamiento              |
| Dispositivo, extensión del sistema                     | Pool de almacenamiento back-end     |
| Volumen virtual                                        | Volumen                             |
| Puerto de extremo frontal, puerto de extremo posterior | Puerto                              |
| Dispositivo distribuido                                | Sincronización de almacenamiento    |
| Vista del almacenamiento                               | Mapa de volumen, Máscara de volumen |
| Volumen de almacenamiento                              | LUN back-end                        |
| ITLS                                                   | Ruta de back-end                    |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Una dirección IP del servidor VPLEX
- Cuenta de dominio de nivel administrativo para el servidor VPLEX
- Puerto 443 (HTTPS). Requiere conectividad de salida al puerto TCP 443 en la estación de administración de VPLEX.
- Para obtener rendimiento, nombre de usuario y contraseña de solo lectura para acceso a ssh/scp.
- Para el rendimiento, se necesita el puerto 22.
- Validar el acceso: Verificar mediante `telnet` al puerto 443. Para un puerto que no sea el predeterminado, con cualquier uso del navegador

### Configuración

| Campo                                                                | Descripción                                                               |
|----------------------------------------------------------------------|---------------------------------------------------------------------------|
| Dirección IP de la consola de gestión de VPLEX                       | Dirección IP o nombre de dominio completo de VPLEX Management Console     |
| Nombre de usuario                                                    | Nombre de usuario de la CLI de VPLEX                                      |
| Contraseña                                                           | Contraseña utilizada para la CLI de VPLEX                                 |
| Dirección IP remota de rendimiento de la consola de gestión de VPLEX | Dirección IP remota de rendimiento de la consola de gestión de VPLEX      |
| Nombre de usuario remoto de rendimiento                              | Nombre de usuario remoto de rendimiento de la consola de gestión de VPLEX |
| Contraseña remota de rendimiento                                     | Contraseña remota de rendimiento de la consola de gestión de VPLEX        |

### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Puerto de comunicación                   | Puerto que se utiliza para la CLI de VPLEX                        |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |
| Tiempo de espera de conexión (s)         | Tiempo de espera de conexión (60 segundos predeterminado)         |

|                                                       |                                                                      |
|-------------------------------------------------------|----------------------------------------------------------------------|
| Número de reintentos                                  | Número de intentos de reintento de inventario                        |
| Intervalo de sondeo de rendimiento (s)                | Intervalo entre sondeos de rendimiento (predeterminado 600 segundos) |
| Tiempo de espera de proceso de SSH de rendimiento (s) | Tiempo de espera del proceso SSH (600 segundos predeterminado)       |
| Tiempo de espera del banner SSH (s)                   | Tiempo de espera del banner SSH (20 segundos predeterminado)         |
| Número de reintentos                                  | Número de intentos de reintento de rendimiento                       |

### Fuente de datos de EMC XtremIO

Para configurar el origen de datos de EMC XtremIO (HTTP), debe tener la dirección del host de XtremIO Management Server (XMS) y una cuenta con privilegios de administrador.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de EMC XtremIO. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Disco (SSD)                | Disco                  |
| Clúster                    | Reducida               |
| Controladora               | Nodo de almacenamiento |
| Volumen                    | Volumen                |
| Mapa de LUN                | Asignación de volumen  |
| Iniciador, destino         | Máscara de volumen     |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP de cada servidor de gestión de XtremIO
- Una cuenta con privilegios de administrador

- Acceso al puerto 443 (HTTPS)

### Configuración

| Campo             | Descripción                                                                  |
|-------------------|------------------------------------------------------------------------------|
| Host XMS          | La dirección IP o el nombre de dominio completo de XtremIO Management Server |
| Nombre de usuario | Nombre de usuario del servidor de gestión de XtremIO                         |
| Contraseña        | Contraseña del servidor de gestión de XtremIO                                |

### Configuración avanzada

| Campo                                   | Descripción                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------|
| Puerto TCP                              | Puerto TCP utilizado para conectar con el servidor de administración XTremIO (predeterminado 443 ) |
| Intervalo de sondeo de inventario (min) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)                                  |
| Tiempo de espera de conexión (s)        | Tiempo de espera de conexión (60 segundos predeterminado)                                          |
| Intervalo de sondeo de rendimiento (s)  | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                               |

### Fuente de datos ETERNUS de Fujitsu

El origen de datos ETERNUS de Fujitsu requiere la dirección IP del almacenamiento. No se puede delimitar por comas.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos ETERNUS de Fujitsu. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo | Insight plazo |
|----------------------------|---------------|
| Disco                      | Disco         |
| Reducida                   | Reducida      |

|                                                                                                                           |                        |
|---------------------------------------------------------------------------------------------------------------------------|------------------------|
| Thin Pool, pool de niveles flexible,<br>Grupo RAID                                                                        | Pool de almacenamiento |
| Volumen estándar, volumen de datos Snap (SDV),<br>Volumen de Snap Data Pool (SDPV),<br>Volumen de thin provisioning (TPV) | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP del almacenamiento ETERNUS, que no se puede delimitar entre comas
- Nombre de usuario y contraseña en el nivel de administración de SSH
- Puerto 22
- Asegúrese de que el desplazamiento de página está desactivado. (clienv-show-more-scroll desactivado)

### Configuración

| Campo                                  | Descripción                                   |
|----------------------------------------|-----------------------------------------------|
| Dirección IP de almacenamiento ETERNUS | La dirección IP del almacenamiento ETERNUS    |
| Nombre de usuario                      | Nombre de usuario para almacenamiento ETERNUS |
| Contraseña                             | Contraseña utilizada para el esternus         |

### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |
| Tiempo de espera del proceso SSH (s)     | Tiempo de espera del proceso SSH (600 segundos predeterminado)    |

### Fuente de datos de Hitachi Content Platform (HCP)

Este recopilador de datos admite la Plataforma de Contenido Hitachi (HCP) que utiliza la API de Gestión de HCP.



## Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de HCP. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Clúster HCP                | Reducida               |
| Inquilino                  | Pool de almacenamiento |
| Espacio de nombres         | Volumen interno        |
| Nodo                       | Nodo                   |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos de inventario

- Dirección IP del servidor HCP
- Nombre de usuario y contraseña de sólo lectura para el software HCP y los privilegios del mismo nivel

## Configuración

| Campo                     | Descripción                                            |
|---------------------------|--------------------------------------------------------|
| Host HCP                  | Dirección IP o nombre de dominio completo del host HCP |
| Puerto HCP                | El valor predeterminado es 9090                        |
| ID de usuario de HCP      | Nombre de usuario del host HCP                         |
| Contraseña de HCP         | Contraseña utilizada para el host HCP                  |
| Tipo de autenticación HCP | Elija HCP_LOCAL o ACTIVE_DIRECTORY                     |

## Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)    |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 900 segundos) |

## Fuente de datos de HDS HiCommand Device Manager

Las fuentes de datos HDS HiCommand e HiCommand Lite son compatibles con el servidor HiCommand Device Manager. OnCommand Insight se comunica con el servidor del Administrador de dispositivos HiCommand mediante la API estándar HiCommand.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de las fuentes de datos HiCommand e HiCommand Lite de HDS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo | Insight plazo          |
|----------------------------|------------------------|
| PDEV                       | Disco                  |
| Piscina de diarios         | Grupo de discos        |
| Cabina de almacenamiento   | Reducida               |
| Controlador del puerto     | Nodo de almacenamiento |
| Grupo de cabinas, DP Pool  | Pool de almacenamiento |
| Unidad lógica, LDEV        | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos de inventario

- Dirección IP del servidor de HiCommand Device Manager
- Nombre de usuario y contraseña de sólo lectura para el software HiCommand Device Manager y los privilegios del mismo nivel
- Requisitos de puerto: 2001 (http) o 2443 (https)
- Validar el acceso:
  - Inicie sesión en el software HiCommand Device Manager con el nombre de usuario y la contraseña del mismo nivel.
  - Verifique el acceso a la API de HiCommand Device Manager: `telnet <HiCommand Device_Manager_server_ip> 2001`

### Requisitos de rendimiento

- HDS rendimiento USP, USP V y VSP
  - El Monitor de rendimiento debe tener licencia.
  - El interruptor de supervisión debe estar activado.

- La herramienta de exportación (`Export.exe`) Se debe copiar en el servidor OnCommand Insight.
- La versión de la herramienta de exportación debe coincidir con la versión de microcódigo de la matriz de destino.
- Rendimiento AMS de HDS
  - El Monitor de rendimiento debe tener licencia.
  - Es necesario instalar la utilidad CLI de Storage Navigator Modular 2 (SNM2) en el servidor OnCommand Insight.
  - Debe registrar todas las matrices de almacenamiento AMS, WMS y SMS cuyo rendimiento necesita adquirir OnCommand Insight mediante el siguiente comando:
  - Debe asegurarse de que todas las cabinas que registró aparezcan en la lista de resultados de este comando: `auunitref.exe`.

## Configuración

| Campo                                                                      | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servidor HiCommand                                                         | Dirección IP o nombre de dominio completo del servidor HiCommand Device Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Nombre de usuario                                                          | Nombre de usuario del servidor de HiCommand Device Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Contraseña                                                                 | Contraseña utilizada para el servidor de HiCommand Device Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DISPOSITIVOS: VSP G1000 (R800), VSP (R700), HUS VM (HM700) Y USP STORAGEES | <p>Lista de dispositivos para los sistemas de almacenamiento VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere:</p> <ul style="list-style-type: none"> <li>• Dirección IP de la cabina: Dirección IP del almacenamiento</li> <li>• User Name: Nombre de usuario para el almacenamiento</li> <li>• Password: Contraseña para el almacenamiento</li> <li>• Carpeta que contiene los archivos JAR de la Utilidad de exportación: La carpeta que contiene la utilidad de exportación <code>.jar</code> archivos</li> </ul> |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNM2Devices - almacenes WMS/SMS/AMS        | <p>Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere:</p> <ul style="list-style-type: none"> <li>• Dirección IP de la cabina: Dirección IP del almacenamiento</li> <li>• Ruta de la CLI de Storage Navigator: Ruta de la CLI de SNM2</li> <li>• Autenticación de cuenta válida: Seleccione esta opción para elegir una autenticación de cuenta válida</li> <li>• User Name: Nombre de usuario para el almacenamiento</li> <li>• Password: Contraseña para el almacenamiento</li> </ul> |
| Seleccione Tuning Manager para rendimiento | Elija Tuning Manager para obtener rendimiento y anule otras opciones de rendimiento                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Tuning Manager Host                        | Dirección IP o nombre de dominio completo del administrador de ajustes                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Puerto del administrador de ajuste         | Puerto utilizado para Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Nombre de usuario de Tuning Manager        | Nombre de usuario de Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Tuning Manager Password                    | Contraseña de Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



En HDS USP, USP V y VSP, cualquier disco puede pertenecer a más de un grupo de matrices.

#### Configuración avanzada

| Campo                                                  | Descripción                                                                                              |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Puerto del servidor HiCommand                          | Puerto utilizado para el administrador de dispositivos HiCommand                                         |
| HTTPS habilitado                                       | Seleccione para habilitar HTTPS                                                                          |
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                        |
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos            |
| Excluir o incluir dispositivos                         | Lista separada por comas de los ID de dispositivo o los nombres de matriz que se van a incluir o excluir |

|                                             |                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------|
| Consulte Administrador de hosts             | Seleccione para consultar al administrador de host                            |
| Tiempo de espera HTTP (s)                   | Tiempo de espera de conexión HTTP (60 segundos predeterminado)                |
| Intervalo de sondeo de rendimiento (s)      | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)          |
| Tiempo de espera de exportación en segundos | Tiempo de espera de la utilidad de exportación (300 segundos predeterminados) |

### Recopilador de datos del centro de Hitachi OPS

Este recopilador de datos usa la suite de aplicaciones integrada de Hitachi OPS Center para acceder a los datos de inventario y rendimiento de varios dispositivos de almacenamiento. Para la detección de inventario y capacidad, la instalación del Centro de operaciones debe incluir los componentes de "Servicios comunes" y "Administrador". Para la recopilación del rendimiento, debe tener instalado el "analizador".

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al ver o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo | Término de OnCommand Insight                           |
|----------------------------|--------------------------------------------------------|
| Sistemas de almacenamiento | Reducida                                               |
| Volumen                    | Volumen                                                |
| Grupos de paridad          | Grupos de discos, Storage Pool(RAID)                   |
| Disco                      | Disco                                                  |
| Pool de almacenamiento     | Pool de almacenamiento (fino, SNAP)                    |
| Grupos de paridad externa  | Pool de almacenamiento (backend), grupos de discos     |
| Puerto                     | Nodo de almacenamiento → nodo de controladora → puerto |
| Grupos de hosts            | Asignación de volúmenes y enmascaramiento              |
| Parejas de volúmenes       | Sincronización de almacenamiento                       |

Nota: Sólo son asignaciones de terminología comunes y es posible que no representen todos los casos de este recopilador de datos.

### Requisitos de inventario

Para recopilar datos de inventario, debe contar con lo siguiente:

- Dirección IP o nombre de host del servidor del centro de operaciones que aloja el componente "Servicios

comunes"

- Cuenta de usuario y contraseña de administrador del sistema raíz/administrador del sistema que existen en todos los servidores que alojan componentes del Centro de operaciones. HDS no implementaron la compatibilidad con la API REST para el uso por parte de usuarios LDAP/SSO hasta que OPS Center 10.8+

## Requisitos de rendimiento

Para poder recopilar datos de rendimiento, se deben cumplir los siguientes requisitos:

- Se debe instalar el módulo Analizador del centro de operaciones de HDS
- Las cabinas de almacenamiento deben estar alimentando el módulo Analizador del centro de operaciones

## Configuración

| Campo                                             | Descripción                                                                                                                  |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Dirección IP del centro de operaciones de Hitachi | Dirección IP o nombre de dominio completo del servidor del Centro de operaciones que aloja el componente "Servicios comunes" |
| Nombre de usuario                                 | Nombre de usuario del servidor del Centro de operaciones.                                                                    |
| Contraseña                                        | Contraseña que se utiliza para el servidor del centro de operaciones.                                                        |

## Configuración avanzada

| Campo                                                  | Descripción                                                                                     |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Tipo de conexión                                       | HTTPS (puerto 443) es la opción predeterminada                                                  |
| Anular puerto TCP                                      | Especifique el puerto que se va a utilizar si no es el predeterminado                           |
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario. El valor predeterminado es 40.                           |
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.  |
| Filtrar lista de dispositivos                          | Lista separada por comas de los números de serie del dispositivo que se van a incluir o excluir |
| Intervalo de sondeo de rendimiento (s)                 | Intervalo entre sondeos de rendimiento. El valor predeterminado es 300.                         |

## Almacenamiento en HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de HDS.

## Terminología de almacenamiento de HDS

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Nombre — proviene directamente del atributo `"name"` de HDS HiCommand Device Manager a través de la llamada a la API XML de `GetStorageArray`
- Modelo: Procede directamente del atributo `"arrayType"` de HDS HiCommand Device Manager a través de la llamada API XML de `GetStorageArray`
- Proveedor — HDS
- Familia: Proviene directamente del atributo `"arrayFamily"` de HDS HiCommand Device Manager a través de la llamada API XML de `GetStorageArray`
- IP:- esta es la dirección IP de gestión de la cabina, no una lista exhaustiva de todas las direcciones IP de la cabina
- Capacidad bruta: Valor base2 que representa la suma de la capacidad total de todos los discos de este sistema, sin importar la función de disco.

## Pool de almacenamiento de HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento HDS.

## Terminología de HDS Storage Pool

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pool de almacenamiento de HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Tipo: El valor aquí será uno de:
  - RESERVADA: Si este pool está dedicado a otros fines distintos a los volúmenes de datos, es decir, registro en diario, instantáneas
  - Thin Provisioning — si se trata de un pool HDP
  - RAID Group — probablemente no los verá por algunos motivos:

OCI tiene una postura sólida para evitar el doble de capacidad de conteo a todos los costes. En HDS, normalmente es necesario crear grupos RAID a partir de discos, crear volúmenes de pool en esos grupos RAID y crear pools (a menudo HDP, pero podría ser un propósito especial) a partir de dichos volúmenes de pools. Si OCI notificó tanto los grupos de RAID subyacentes como los pools, la suma de su capacidad bruta superaría en gran medida la suma de los discos.

En su lugar, el recopilador de datos HDS HiCommand de OCI reduce arbitrariamente el tamaño de los grupos RAID según la capacidad de los volúmenes de pools. Esto puede provocar que OCI no informe del grupo RAID. Además, todos los grupos RAID resultantes se marcan de forma que no sean visibles en la WebUI de OCI, pero fluyen al almacén de datos de OCI (DWH). El propósito de estas decisiones es evitar el desorden de la interfaz de usuario para cosas que la mayoría de los usuarios no se preocupan por — si su matriz HDS tiene grupos RAID con 50MB libres, usted probablemente no puede utilizar ese espacio libre para cualquier resultado significativo.

- Nodo: N/A, ya que los pools HDS no están ligados a ningún nodo en concreto

- Redundancia: Nivel de RAID del pool. Posiblemente varios valores para un pool HDP constan de varios tipos de RAID
- Porcentaje de capacidad: El porcentaje utilizado del pool para el uso de datos, con los GB usados y el tamaño total lógico GB del pool
- Capacidad sobrecomprometida - un valor derivado que indique «la capacidad lógica de este pool está sobresuscrita por este porcentaje en virtud de la suma de los volúmenes lógicos que exceden la capacidad lógica del pool por este porcentaje».
- Snapshot: Muestra la capacidad reservada para el uso Snapshot en este pool

#### Nodo de almacenamiento HDS

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de nodo de almacenamiento HDS.

#### Terminología de nodos de almacenamiento de HDS

Los siguientes términos se aplican a los objetos o referencias que puede encontrar en las páginas de destino de activos del nodo de almacenamiento HDS. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Nombre: Nombre del director de interfaz (FED) o del adaptador de canal en matrices monolíticas, o el nombre del controlador en una matriz modular. Una cabina HDS determinada tendrá 2 o más nodos de almacenamiento
- Volúmenes: En la tabla volumen, se mostrarán todos los volúmenes asignados a cualquier puerto que pertenezca a este nodo de almacenamiento

#### Recopilador de datos del centro de Hitachi OPS

Este recopilador de datos usa la suite de aplicaciones integrada de Hitachi OPS Center para acceder a los datos de inventario y rendimiento de varios dispositivos de almacenamiento. Para la detección de inventario y capacidad, la instalación del Centro de operaciones debe incluir los componentes de "Servicios comunes" y "Administrador". Para la recopilación del rendimiento, debe tener instalado el "analizador".

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario de este recopilador de datos. Para cada tipo de activo adquirido, se muestra la terminología más común utilizada para este activo. Al ver o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo | Término de OnCommand Insight                       |
|----------------------------|----------------------------------------------------|
| Sistemas de almacenamiento | Reducida                                           |
| Volumen                    | Volumen                                            |
| Grupos de paridad          | Grupos de discos, Storage Pool(RAID)               |
| Disco                      | Disco                                              |
| Pool de almacenamiento     | Pool de almacenamiento (fino, SNAP)                |
| Grupos de paridad externa  | Pool de almacenamiento (backend), grupos de discos |



| Plazo del proveedor/modelo | Término de OnCommand Insight                           |
|----------------------------|--------------------------------------------------------|
| Puerto                     | Nodo de almacenamiento → nodo de controladora → puerto |
| Grupos de hosts            | Asignación de volúmenes y enmascaramiento              |
| Parejas de volúmenes       | Sincronización de almacenamiento                       |

Nota: Sólo son asignaciones de terminología comunes y es posible que no representen todos los casos de este recopilador de datos.

#### Requisitos de inventario

Para recopilar datos de inventario, debe contar con lo siguiente:

- Dirección IP o nombre de host del servidor del centro de operaciones que aloja el componente "Servicios comunes"
- Cuenta de usuario y contraseña de administrador del sistema raíz/administrador del sistema que existen en todos los servidores que alojan componentes del Centro de operaciones. HDS no implementaron la compatibilidad con la API REST para el uso por parte de usuarios LDAP/SSO hasta que OPS Center 10.8+

#### Requisitos de rendimiento

Para poder recopilar datos de rendimiento, se deben cumplir los siguientes requisitos:

- Se debe instalar el módulo Analizador del centro de operaciones de HDS
- Las cabinas de almacenamiento deben estar alimentando el módulo Analizador del centro de operaciones

#### Configuración

| Campo                                             | Descripción                                                                                                                  |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Dirección IP del centro de operaciones de Hitachi | Dirección IP o nombre de dominio completo del servidor del Centro de operaciones que aloja el componente "Servicios comunes" |
| Nombre de usuario                                 | Nombre de usuario del servidor del Centro de operaciones.                                                                    |
| Contraseña                                        | Contraseña que se utiliza para el servidor del centro de operaciones.                                                        |

#### Configuración avanzada

| Campo                                    | Descripción                                                           |
|------------------------------------------|-----------------------------------------------------------------------|
| Tipo de conexión                         | HTTPS (puerto 443) es la opción predeterminada                        |
| Anular puerto TCP                        | Especifique el puerto que se va a utilizar si no es el predeterminado |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario. El valor predeterminado es 40. |

|                                                        |                                                                                                 |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos.  |
| Filtrar lista de dispositivos                          | Lista separada por comas de los números de serie del dispositivo que se van a incluir o excluir |
| Intervalo de sondeo de rendimiento (s)                 | Intervalo entre sondeos de rendimiento. El valor predeterminado es 300.                         |

## Fuente de datos NAS (Hnas) de HDS

El origen de datos NAS de HDS (HNAS) es una fuente de datos de inventario y configuración para admitir la detección de clústeres NAS de HDS. Insight admite la detección de recursos compartidos de NFS y CIFS, sistemas de archivos (volúmenes internos de Insight) y duraciones (pools de almacenamiento de Insight).

Este origen de datos está basado en SSH, por lo que la unidad de adquisición que la alojará debe poder iniciar sesiones SSH a TCP 22 en el Hnas mismo o la Unidad de Gestión de sistemas (SMU) a la que está conectado el clúster.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos Hnas. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Nivel                      | Grupo de discos        |
| Clúster                    | Reducida               |
| Nodo                       | Nodo de almacenamiento |
| Capacidad de expansión     | Pool de almacenamiento |
| Sistema de archivos        | Volumen interno        |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

A continuación, se enumeran los requisitos para configurar y utilizar este origen de datos:

- Dirección IP del dispositivo
- Puerto 22, protocolo SSH
- Nombre de usuario y contraseña - nivel de privilegio: Supervisor
- NOTA: Este recopilador de datos está basado en SSH, por lo que la unidad principal que la aloja debe ser capaz de iniciar sesiones SSH a TCP 22 en el propio Hnas o la unidad de administración de sistemas

(SMU) a la que está conectado el clúster.



Este recopilador de datos está basado en SSH, por lo que la unidad de datos que la aloja debe ser capaz de iniciar sesiones SSH a TCP 22 en el propio Hnas o la unidad de administración de sistemas (SMU) a la que está conectado el clúster.

### Configuración

| Campo             | Descripción                                                        |
|-------------------|--------------------------------------------------------------------|
| Host Hnas         | Dirección IP o nombre de dominio completo del host de gestión Hnas |
| Nombre de usuario | Nombre de usuario de Hnas CLI                                      |
| Contraseña        | Contraseña usada para Hnas CLI                                     |

### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 30 minutos) |
| Tiempo de espera del banner SSH (s)      | Tiempo de espera del banner SSH (15 segundos predeterminado)      |
| Tiempo de espera de comando SSH (s)      | Tiempo de espera de comando SSH (predeterminado 30 segundos)      |

### Origen de datos HP CommandView AE

Los orígenes de datos HP CommandView Advanced Edition (AE) y CommandView AE CLI/SMI (AE Lite) admiten el inventario y el rendimiento desde un servidor CommandView (también conocido como HiCommand) Device Manager.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de los orígenes de datos HP CommandView AE y AE Lite. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                 |
|----------------------------|-----------------|
| Plazo del proveedor/modelo | Insight plazo   |
| PDEV                       | Disco           |
| Piscina de diarios         | Grupo de discos |

|                           |                        |
|---------------------------|------------------------|
| Cabina de almacenamiento  | Reducida               |
| Controlador del puerto    | Nodo de almacenamiento |
| Grupo de cabinas, DP Pool | Pool de almacenamiento |
| Unidad lógica, LDEV       | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos de inventario

- Dirección IP del servidor de HiCommand Device Manager
- Nombre de usuario y contraseña de sólo lectura para el software CommandView AE y los privilegios de interlocutor
- La versión CommandView AE Lite del administrador de dispositivos sólo tiene licencia de CLI
- Requisito de puerto: 2001

### Requisitos de rendimiento

- HDS rendimiento USP, USP V y VSP
  - El Monitor de rendimiento debe tener licencia.
  - El interruptor de supervisión debe estar activado.
  - La herramienta de exportación (`Export.exe`) Se debe copiar en el servidor OnCommand Insight.
  - La versión de la herramienta de exportación debe coincidir con la versión de microcódigo de la matriz de destino.
- Rendimiento AMS de HDS
  - El Monitor de rendimiento debe tener licencia.
  - Es necesario instalar la utilidad CLI de Storage Navigator Modular 2 (SNM2) en el servidor OnCommand Insight.
  - Debe registrar todas las matrices de almacenamiento AMS, WMS y SMS cuyo rendimiento necesita adquirir OnCommand Insight mediante el siguiente comando:
  - Debe asegurarse de que todas las cabinas que registró aparezcan en la lista de resultados de este comando: `auunitref.exe`.

### Configuración

| Campo              | Descripción                                                                     |
|--------------------|---------------------------------------------------------------------------------|
| Servidor HiCommand | Dirección IP o nombre de dominio completo del servidor HiCommand Device Manager |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de usuario                                 | Nombre de usuario del servidor de HiCommand Device Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Contraseña                                        | Contraseña utilizada para el servidor de HiCommand Device Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Dispositivos: Almacenamiento USP, USP V, VSP/R600 | <p>Lista de dispositivos para los sistemas de almacenamiento VSP G1000 (R800), VSP (R700), HUS VM (HM700) y USP. Cada almacenamiento requiere:</p> <ul style="list-style-type: none"> <li>• Dirección IP de la cabina: Dirección IP del almacenamiento</li> <li>• User Name: Nombre de usuario para el almacenamiento</li> <li>• Password: Contraseña para el almacenamiento</li> <li>• Carpeta que contiene los archivos JAR de la Utilidad de exportación: La carpeta que contiene la utilidad de exportación .jar archivos</li> </ul> |
| SNM2Devices - almacenes WMS/SMS/AMS               | <p>Lista de dispositivos para almacenamientos WMS/SMS/AMS. Cada almacenamiento requiere:</p> <ul style="list-style-type: none"> <li>• Dirección IP de la cabina: Dirección IP del almacenamiento</li> <li>• Ruta de la CLI de Storage Navigator: Ruta de la CLI de SNM2</li> <li>• Autenticación de cuenta válida: Seleccione esta opción para elegir una autenticación de cuenta válida</li> <li>• User Name: Nombre de usuario para el almacenamiento</li> <li>• Password: Contraseña para el almacenamiento</li> </ul>                |
| Seleccione Tuning Manager para rendimiento        | Elija Tuning Manager para obtener rendimiento y anule otras opciones de rendimiento                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Tuning Manager Host                               | Dirección IP o nombre de dominio completo del administrador de ajustes                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Puerto del administrador de ajuste                | Puerto utilizado para Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Nombre de usuario de Tuning Manager               | Nombre de usuario de Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Tuning Manager Password                           | Contraseña de Tuning Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



En HDS USP, USP V y VSP, cualquier disco puede pertenecer a más de un grupo de matrices.

### Configuración avanzada

| Campo                                                  | Descripción                                                                                              |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Puerto del servidor HiCommand                          | Puerto utilizado para el administrador de dispositivos HiCommand                                         |
| HTTPS habilitado                                       | Seleccione para habilitar HTTPS                                                                          |
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                        |
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de matrices a continuación al recopilar datos            |
| Excluir o incluir dispositivos                         | Lista separada por comas de los ID de dispositivo o los nombres de matriz que se van a incluir o excluir |
| Consulte Administrador de hosts                        | Seleccione para consultar al administrador de host                                                       |
| Tiempo de espera HTTP (s)                              | Tiempo de espera de conexión HTTP (60 segundos predeterminado)                                           |
| Intervalo de sondeo de rendimiento (s)                 | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                     |
| Tiempo de espera de exportación en segundos            | Tiempo de espera de la utilidad de exportación (300 segundos predeterminados)                            |

### Fuente de datos de almacenamiento HP EVA

Para la configuración, el origen de datos de almacenamiento EVA (SSSU) requiere la dirección IP del servidor Command View (CV) y un nombre de usuario y una contraseña \_de sólo lectura para el software CV. El usuario debe estar definido en el software CV.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de HP EVA. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                               |
|----------------------------|-------------------------------|
| Plazo del proveedor/modelo | Insight plazo                 |
| Disco                      | Disco                         |
| Grupo de discos            | Grupo de discos (no modelado) |

|                          |                        |
|--------------------------|------------------------|
| Célula de almacenamiento | Reducida               |
| Disco virtual            | Pool de almacenamiento |
| Disco virtual            | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

#### Requisitos de inventario

- Dirección IP del servidor CV
- Nombre de usuario y contraseña de sólo lectura para el software CV. El usuario debe estar definido en el software CV.
- Software de terceros instalado en el servidor OnCommand Insight/RAU: `sssu.exe`. La `sssu.exe` La versión debe corresponder a la versión CV.
- Validación de acceso: Ejecución `sssu.exe` con el nombre de usuario y la contraseña.

#### Requisitos de rendimiento

El paquete de software HP StorageWorks Command View EVA debe estar instalado en el servidor OnCommand Insight. También puede instalar una unidad de adquisición remota (RAU) en el servidor EVA:

1. Instale el conjunto de software HP StorageWorks Command View EVA en el servidor OnCommand Insight o instale una unidad de adquisición remota en el servidor Command View EVA.
2. Localice el `evaperf.exe` comando. Por ejemplo: `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Con la dirección IP del servidor Command View, realice estos pasos:
  - a. Ejecute este comando donde 860 es el puerto predeterminado `Evaperf.exe server <Command View Server IP> 860 <username>`
  - b. Introduzca la contraseña del servidor Command View en el indicador de contraseña.

Esto debería devolver un indicador de línea de comandos y nada más.

4. Verifique la configuración ejecutando `evaperf.exe ls`.

Debe ver una lista de las cabinas o controladoras gestionadas por el servidor de vista de comandos. Cada línea muestra un controlador en una matriz EVA.

#### Configuración

| Campo                 | Descripción                                                      |
|-----------------------|------------------------------------------------------------------|
| Servidor COMMANDVVIEW | Dirección IP o nombre de dominio completo de EVA Storage Manager |

|                                  |                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de usuario                | Nombre de usuario del administrador de Command View. El nombre debe definirse en la vista de comandos.                                    |
| Contraseña                       | Contraseña usada para el administrador de View de comandos.                                                                               |
| Nombre de usuario de rendimiento | Para obtener rendimiento, el nombre de usuario del administrador de vistas de comandos. El nombre debe definirse en la vista de comandos. |
| Contraseña de rendimiento        | Para obtener más rendimiento, la contraseña utilizada para el administrador de vistas de comandos.                                        |

### Configuración avanzada

| Campo                                    | Descripción                                                                                                                                                                           |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                                                                                                     |
| Inicio de la CLI                         | Nombre de ruta completo al directorio inicial de la CLI donde <code>sssu.exe</code> está ubicado                                                                                      |
| Excluir dispositivos de inventario       | Lista separada por comas de los nombres de dispositivo que se van a incluir                                                                                                           |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                                                                                                  |
| Inicio de la CLI de rendimiento          | Para rendimiento de matriz, nombre de ruta completo al directorio inicial de la CLI, donde se encuentra <code>sssu.exe</code> . Para validar el acceso, ejecute <code>sssu.exe</code> |
| Tiempo de espera de comando (s)          | <code>evaperf</code> tiempo de espera de comando (predeterminado 600 segundos)                                                                                                        |
| Rendimiento excluir dispositivos         | Lista separada por comas de nombres de dispositivos para excluir de la recopilación de datos de rendimiento                                                                           |

### Origen de datos HPE Nimble

El recopilador de datos de HPE Nimble admite los datos de inventario y rendimiento de las cabinas de almacenamiento de HPE Nimble.



## Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de HPE Nimble. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                                  |
|----------------------------|----------------------------------|
| Plazo del proveedor/modelo | Insight plazo                    |
| Cabina                     | Reducida                         |
| Disco                      | Disco                            |
| Piscina                    | Pool de almacenamiento           |
| Volumen                    | Volumen                          |
| Iniciador                  | Alias del host de almacenamiento |
| Controladora               | Nodo de almacenamiento           |
| Interfaz Fibre Channel     | Controladora                     |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- La cabina debe estar instalada y configurada, y es posible acceder a ella desde el cliente a través de su nombre de dominio completo (FQDN) o la dirección IP de administración de cabinas.
- El arreglo debe estar ejecutando NimbleOS 2.3.x o posterior.
- Debe tener un nombre de usuario y una contraseña válidos para la cabina.
- El puerto 5392 debe estar abierto en la cabina.

## Configuración

| Campo                                     | Descripción                                                                    |
|-------------------------------------------|--------------------------------------------------------------------------------|
| Dirección IP de administración de cabinas | Nombre de dominio completo (FQDN) o dirección IP de administración de cabinas. |
| Nombre de usuario                         | Nombre de usuario de la cabina Nimble                                          |
| Contraseña                                | Contraseña de la cabina de Nimble                                              |

## Configuración avanzada

| Campo | Descripción |
|-------|-------------|
|-------|-------------|

|                                          |                                                                               |
|------------------------------------------|-------------------------------------------------------------------------------|
| Puerto                                   | Puerto que utiliza la API DE REST de Nimble. El valor predeterminado es 5392. |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)             |

Nota: El intervalo de sondeo de rendimiento predeterminado es de 300 segundos y no se puede cambiar. Este es el único intervalo admitido por Nimble.

### Fuente de datos Huawei OceanStor

OnCommand Insight utiliza la fuente de datos Huawei OceanStor (REST/HTTPS) para descubrir inventarios de sistemas de almacenamiento Huawei OceanStor.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario y rendimiento del OceanStor de Huawei. Para cada tipo de activo adquirido por OnCommand Insight, se muestra la terminología más común utilizada para este activo. Al ver o solucionar problemas de este recopilador de datos, tenga en cuenta la siguiente terminología:

| Plazo del proveedor/modelo         | Término de OnCommand Insight |
|------------------------------------|------------------------------|
| Pool de almacenamiento             | Pool de almacenamiento       |
| Sistema de archivos                | Volumen interno              |
| Controladora                       | Nodo de almacenamiento       |
| Puerto FC (asignado)               | Asignación de volumen        |
| Iniciador de FC de host (asignado) | Máscara de volumen           |
| Recursos compartidos NFS/CIFS      | Share                        |
| Share                              | Nodo de destino iSCSI        |
| Iniciador de enlace iSCSI          | Nodo iniciador iSCSI         |
| Disco                              | Disco                        |
| LUN                                | Volumen                      |

### Requisitos

A continuación se enumeran los requisitos para configurar y utilizar este recopilador de datos:

- IP del dispositivo

- Credenciales para acceder al administrador de dispositivos OceanStor
- El puerto 8088 debe estar disponible

#### Configuración

| Campo                     | Descripción                                                                            |
|---------------------------|----------------------------------------------------------------------------------------|
| OceanStor Host IP Address | Dirección IP o nombre de dominio completo del Administrador de dispositivos OceanStor  |
| Nombre de usuario         | Nombre utilizado para iniciar sesión en el Administrador de dispositivos OceanStor     |
| Contraseña                | Contraseña utilizada para iniciar sesión en el Administrador de dispositivos OceanStor |

#### Configuración avanzada

| Campo                                    | Descripción                                                                                               |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Puerto TCP                               | Puerto TCP utilizado para conectar con el Administrador de dispositivos OceanStor (predeterminado: 8088 ) |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)                                         |
| Tiempo de espera de conexión (s)         | Tiempo de espera de conexión (60 segundos predeterminado)                                                 |

#### Fuente de datos IBM Cleversafe

Este origen de datos recopila datos de inventario y rendimiento para IBM Cleversafe.

#### Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP del administrador o nombre de host
- Un nombre de usuario y una contraseña para el mismo
- Puerto 9440

#### Configuración

| Campo                                               | Descripción                                      |
|-----------------------------------------------------|--------------------------------------------------|
| Dirección IP o nombre de host de Cleversafe Manager | Dirección IP del host del dispositivo CleverSafe |

|                   |                                                        |
|-------------------|--------------------------------------------------------|
| Nombre de usuario | Nombre utilizado para iniciar sesión en Cleversafe     |
| Contraseña        | Contraseña utilizada para iniciar sesión en Cleversafe |

### Configuración avanzada

| Campo                                    | Descripción                            |
|------------------------------------------|----------------------------------------|
| Intervalo de sondeo de inventario (mín.) | El valor predeterminado es 60 minutos  |
| Tiempo de espera de conexión HTTP)       | El valor predeterminado es 60 segundos |

### Origen de datos de IBM DS

El origen de datos de IBM DS (CLI) sólo admite dispositivos DS6xxx y DS8xxx. Los dispositivos DS3xxx, DS4xxx y DS5xxx son compatibles con el origen de datos E-Series de NetApp. Consulte la matriz de compatibilidad de origen de datos de Insight para ver modelos y versiones de firmware admitidas.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de IBM DS. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Módulo de unidad de disco  | Disco                  |
| Imagen de almacenamiento   | Reducida               |
| Pool de extensiones        | Pool de almacenamiento |
| Volumen de bloques fijos   | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Dirección IP de cada matriz DS
- El nombre de visualización de almacenamiento es opcional y sólo cosmético
- Nombre de usuario y contraseña de sólo lectura en cada matriz DS
- Software de terceros instalado en el servidor Insight: Dscli de IBM
- Validación de acceso: Ejecución `dscli` con el nombre de usuario y la contraseña

- Requisitos del puerto: 80, 443 y 1750

### Configuración

| Campo                     | Descripción                                                             |
|---------------------------|-------------------------------------------------------------------------|
| DS                        | Dirección IP o nombre de dominio completo del host de almacenamiento DS |
| Nombre de usuario         | Nombre utilizado para la CLI de DS                                      |
| Contraseña                | Contraseña utilizada para la CLI de DS                                  |
| Ruta ejecutable dscli.exe | Ruta completa a la <code>dscli.exe</code> utilidad.                     |

### Configuración avanzada

| Campo                                          | Descripción                                                                                                         |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)       | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                                   |
| Nombre para mostrar almacenamiento             | Nombre de la matriz de almacenamiento de IBM DS                                                                     |
| Excluir dispositivos de inventario             | Lista separada por comas de los números de serie del dispositivo que se van a excluir de la colección de inventario |
| Intervalo de sondeo de rendimiento (s)         | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                                |
| Tipo de filtro de rendimiento                  | Incluir: Datos recopilados sólo de dispositivos de la lista. Excluir: No se recopilan datos de estos dispositivos   |
| Lista de dispositivos de filtro de rendimiento | Lista separada por comas de ID de dispositivo para incluir o excluir de la colección de rendimiento                 |

### Fuente de datos IBM PowerVM

La fuente de datos de IBM PowerVM (SSH) recopila información sobre particiones virtuales que se ejecutan en instancias de hardware DE IBM POWER gestionadas por una consola de administración de hardware (HMC). Para la configuración, este origen de datos requiere el nombre de usuario para iniciar sesión en el HMC a través de SSH, y el permiso de nivel de vista en las configuraciones de HMC.

## Terminología

OnCommand Insight adquiere la siguiente información de inventario desde el origen de datos de IBM PowerVM. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                  |
|----------------------------|------------------|
| Plazo del proveedor/modelo | Insight plazo    |
| disco hdisk                | Disco virtual    |
| Sistema gestionado         | Host             |
| LPAR, servidor VIO         | Máquina virtual  |
| Grupo de volúmenes         | Almacén de datos |
| Volumen físico             | LUN              |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- Dirección IP de la Consola de administración de hardware (HMC)
- Nombre de usuario y contraseña que proporcionan acceso a HMC mediante SSH
- Se requiere el puerto SSH-22
- Permiso de vista en todos los sistemas de administración y dominios de seguridad de partición lógica

El usuario también debe tener permiso View en las configuraciones HMC y la capacidad de recopilar información de VPD para la agrupación de seguridad de la consola HMC. También se debe permitir al usuario el acceso al comando de servidor de E/S virtual en la agrupación de seguridad de partición lógica. Es una práctica recomendada empezar desde un rol de operador y después quitar todas las funciones. Los usuarios de sólo lectura de HMC no tienen privilegios para ejecutar comandos proxy en hosts AIX.

- La mejor práctica de IBM es tener los dispositivos controlados por dos o más HMC. Tenga en cuenta que esto puede provocar que OnCommand Insight informe de dispositivos duplicados, por lo que se recomienda encarecidamente agregar dispositivos redundantes a la lista "excluir dispositivos" de la configuración avanzada de este recopilador de datos.

## Configuración

| Campo                                                       | Descripción                                                                      |
|-------------------------------------------------------------|----------------------------------------------------------------------------------|
| Dirección de la consola de administración de hardware (HMC) | Dirección IP o nombre de dominio completo de PowerVM hardware Management Console |
| Usuario de HMC                                              | Nombre de usuario de la Consola de administración de hardware                    |

|            |                                                                    |
|------------|--------------------------------------------------------------------|
| Contraseña | Contraseña utilizada para la Consola de administración de hardware |
|------------|--------------------------------------------------------------------|

#### Configuración avanzada

| Campo                                    | Descripción                                                                                   |
|------------------------------------------|-----------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)                             |
| Puerto SSH                               | Puerto que se utiliza para SSH al PowerVM                                                     |
| Tiempo de espera del proceso SSH (s)     | Tiempo de espera del proceso SSH (600 segundos predeterminado)                                |
| Número de reintentos                     | Número de intentos de reintento de inventario                                                 |
| Excluir dispositivos                     | Lista separada por comas de ID de dispositivo o nombres de visualización que se van a excluir |

#### Fuente de datos IBM SVC

El origen de datos IBM SVC recopila datos de inventario y rendimiento mediante SSH, lo que admite una variedad de dispositivos que ejecutan el sistema operativo SVC. La lista de dispositivos compatibles incluye modelos como SVC, v7000, v5000 y v3700. Consulte la matriz de compatibilidad con orígenes de datos de Insight para ver modelos y versiones de firmware compatibles.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos IBM SVC. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Unidad                     | Disco                  |
| Clúster                    | Reducida               |
| Nodo                       | Nodo de almacenamiento |
| Grupo Mdisk                | Pool de almacenamiento |
| VDisk                      | Volumen                |

|             |              |
|-------------|--------------|
| Disco Mdisk | LUN back-end |
|-------------|--------------|



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

#### Requisitos de inventario

- Dirección IP de cada clúster SVC
- Puerto 22 disponible
- Par de claves públicas y privadas que genere conInsight o reutilice un keyair que ya esté en uso en su SVC

Si está reutilizando un keyair existente, debe convertirlos del formato Putty al formato OpenSSH.

- Clave pública instalada en el clúster SVC
- La clave privada debe identificarse en el origen de datos
- Validación de acceso: Abierta `ssh` Sesión al clúster SVC mediante la clave privada



No es necesario instalar software de terceros.

#### Requisitos de rendimiento

- Consola SVC, que es obligatoria para cualquier clúster SVC y necesaria para el paquete básico de la detección SVC.
- El nivel de acceso administrativo solo se requiere para copiar los archivos de datos de rendimiento de los nodos de clúster al nodo de configuración.



Dado que este nivel de acceso no es necesario para el paquete de detección de la base SVC, es posible que el usuario de la base SVC no funcione correctamente.

- Se requiere el puerto 22
- Se debe generar una clave SSH pública y privada para este usuario, y la clave privada se almacena para que sea accesible desde la Unidad de adquisición. Si el usuario de la base SVC tiene los permisos adecuados, el mismo usuario y la misma clave funcionan. Se puede utilizar la misma clave SSH para los datos de inventario y rendimiento.
- Active la recopilación de datos mediante la conexión al clúster SVC mediante SSH y ejecutando: `svctask startstats -interval 1`



También puede activar la recopilación de datos mediante la interfaz de usuario de administración de SVC.

#### Se explica el número de serie padre

Tradicionalmente, Insight es capaz de generar informes sobre el número de serie de la cabina de almacenamiento o los números de serie de cada nodo de almacenamiento. Sin embargo, algunas arquitecturas de cabinas de almacenamiento no se alinean correctamente con esto. Un clúster SVC puede componerse de 1-4 dispositivos y cada dispositivo tiene 2 nodos. Si el dispositivo en sí tiene un número de



serie, ese número de serie no es ni el número de serie del clúster ni los nodos.

El atributo "número de serie principal" del objeto del nodo de almacenamiento se rellena de forma adecuada para las matrices IBM SVC cuando los nodos individuales se encuentran dentro de un gabinete o dispositivo intermedio que es sólo parte de un clúster mayor.

#### Configuración

| Campo                                                                                   | Descripción                                                                    |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Dirección IP del clúster/s.                                                             | La dirección IP del nombre de dominio completo para el almacenamiento SVC      |
| Elija 'Contraseña' o 'Archivo de claves OpenSSH' para especificar el tipo de credencial | El tipo de credencial utilizado para conectarse al dispositivo a través de SSH |
| Nombre de usuario del inventario                                                        | Nombre de usuario de la CLI de SVC                                             |
| Contraseña de inventario                                                                | Contraseña para la CLI de SVC                                                  |
| Ruta completa a la clave privada de inventario                                          | Ruta completa al archivo de claves privadas de inventario                      |
| Nombre de usuario de rendimiento                                                        | Nombre de usuario de la CLI SVC para la recopilación de rendimiento            |
| Contraseña de rendimiento                                                               | Contraseña para la CLI de SVC para la recopilación del rendimiento             |
| Ruta completa a la clave privada de rendimiento                                         | Ruta completa al archivo de claves privadas de rendimiento                     |

#### Configuración avanzada

| Campo                                    | Descripción                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 40 minutos)                                    |
| Excluir dispositivos                     | Lista separada por comas de los ID de dispositivo que se van a excluir de la colección de inventario |
| Tiempo de espera del proceso SSH (s)     | Tiempo de espera del proceso SSH (200 segundos predeterminado)                                       |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                 |

|                                                             |                                                                                                   |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Rendimiento excluir dispositivos                            | Lista separada por comas de ID de dispositivo que se van a excluir de la colección de rendimiento |
| Tiempo de espera de proceso de SSH de rendimiento (s)       | Tiempo de espera del proceso SSH (200 segundos predeterminado)                                    |
| Para limpiar los archivos de estadísticas objeto de dumping | Selecciona para limpiar los archivos de estadísticas objeto de dumping                            |

## Origen de datos de IBM Tivoli Monitoring

Este origen de datos se utiliza exclusivamente para el uso del sistema de archivos. Se comunica directamente con Tivoli Monitoring Database, también conocido como Tivoli Monitoring Data Warehouse. Compatibilidad con las bases de datos de Oracle y DB2.

### Mensaje de error de Oracle



Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

Si el SID especificado genera el mensaje de error que contiene "ORA-12154" al intentar conectarse, compruebe dos veces la configuración del servicio de red de Oracle DB. Si la configuración de acceso especifica un nombre de host completo (por ejemplo, "NAMES.DEFAULT\_DOMAIN"), intente insertar el nombre de servicio completo en el campo SID. Un ejemplo sencillo sería que la conexión a SID `testdb` Está fallando y la configuración de Oracle especifica un dominio `decompany.com`. Se puede utilizar la siguiente cadena en lugar del SID base para intentar conectar: `testdb.company.com`.

### Configuración

| Campo                                       | Descripción                                                              |
|---------------------------------------------|--------------------------------------------------------------------------|
| IP de la base de datos de Tivoli Monitoring | Dirección IP o nombre de dominio completo del servidor Tivoli Monitoring |
| Nombre de usuario                           | Nombre de usuario del servidor de Tivoli Monitoring                      |
| Contraseña                                  | Contraseña del servidor de Tivoli Monitoring                             |

### Configuración avanzada

| Campo                                          | Descripción                                                           |
|------------------------------------------------|-----------------------------------------------------------------------|
| Puerto de base de datos de Tivoli Monitoring   | Puerto utilizado para la base de datos de supervisión de Tivoli       |
| Nombre de la base de datos de Oracle SID o DB2 | ID del servicio de escucha de Oracle o nombre de la base de datos DB2 |

|                                                        |                                                                   |
|--------------------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario (predeterminado 60 minutos) |
| Controlador de base de datos que se va a utilizar      | Seleccione controlador de base de datos para utilizar             |
| Protocolo utilizado para conectarse a la base de datos | Protocolo utilizado para conectarse a la base de datos            |
| Esquema de base de datos                               | Introduzca el esquema de base de datos                            |

### Fuente de datos IBM TotalStorage DS4000

Este origen de datos recopila información de inventario y rendimiento. Hay dos configuraciones posibles (firmware 6.x y 7.x+) y ambas tienen los mismos valores. La API recoge las estadísticas de datos de volúmenes.

#### Configuración

| Campo                                                                      | Descripción                                                                        |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Lista separada por comas de las IP de controladora SANtricity de la cabina | Direcciones IP o nombres de dominio completos de controladoras separados por comas |

#### Requisitos

- Dirección IP de cada matriz DS5 o FAStT
- Validación de acceso: Haga ping a la dirección IP de ambas controladoras en cada matriz.

#### Configuración avanzada

| Campo                                                    | Descripción                                                          |
|----------------------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                 | Intervalo entre sondeos de inventario (predeterminado 30 minutos)    |
| Intervalo de sondeo de rendimiento (hasta 3600 segundos) | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

### Origen de datos de IBM XIV

El inventario del origen de datos de IBM XIV (CLI) se realiza mediante la interfaz de línea de comandos de XIV. El rendimiento de XIV se consigue realizando llamadas SMI-S a la matriz XIV, que ejecuta un proveedor SMI-S en el puerto 5989.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de IBM XIV. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver

o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Disco                      | Disco                  |
| Sistema de almacenamiento  | Reducida               |
| Pool de almacenamiento     | Pool de almacenamiento |
| Volumen                    | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- Requisito de puerto: Puerto TCP 7778
- Dirección IP de la interfaz de gestión de XIV
- Nombre de usuario y contraseña de solo lectura
- La CLI de XIV debe instalarse en Insight Server o RAU
- Validación de acceso: Inicie sesión en la interfaz de usuario de XIV desde el servidor de Insight con el nombre de usuario y la contraseña.

### Configuración

| Campo                                        | Descripción                                                                   |
|----------------------------------------------|-------------------------------------------------------------------------------|
| Dirección IP                                 | La dirección IP o el nombre de dominio completo para el almacenamiento de XIV |
| Nombre de usuario                            | Nombre de usuario del almacenamiento de XIV                                   |
| Contraseña                                   | Contraseña para el almacenamiento XIV                                         |
| Ruta completa al directorio de la CLI de XIV | Ruta completa al directorio de la CLI de XIV                                  |

### Configuración avanzada

| Campo                                      | Descripción                                                       |
|--------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)   | Intervalo entre sondeos de inventario (predeterminado 40 minutos) |
| Tiempo de espera de proceso de la CLI (ms) | Tiempo de espera del proceso de CLI (7200000 ms predeterminado)   |

|                                         |                                                                      |
|-----------------------------------------|----------------------------------------------------------------------|
| IP DEL HOST DE SMI-S.                   | Dirección IP del host del proveedor SMI-S.                           |
| Puerto SMI-S.                           | Puerto que utiliza el host del proveedor SMI-S.                      |
| Protocolo SMI-S.                        | Protocolo utilizado para conectar con el proveedor SMI-S.            |
| Espacio de nombres SMI-S.               | Espacio de nombres SMI-S.                                            |
| Nombre de usuario                       | Nombre de usuario para el host del proveedor de SMI-S.               |
| Contraseña                              | Contraseña para el host del proveedor SMI-S.                         |
| Intervalo de sondeo de rendimiento (s)  | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |
| Número de reintentos de conexión SMI-S. | Número de intentos de reintento de conexión SMI-S.                   |

### Fuente de datos Infinidat InfiniBox

La fuente de datos Infinidat InfiniBox (HTTP) se utiliza para recopilar información del almacenamiento Infinidat InfiniBox. Debe tener acceso al nodo de gestión de InfiniBox.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de InfiniBox. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Unidad                     | Disco                  |
| InfiniBox                  | Reducida               |
| Nodo                       | Nodo de almacenamiento |
| Piscina                    | Pool de almacenamiento |
| Volumen                    | Volumen                |
| Puerto FC                  | Puerto                 |
| Sistema de archivos        | Volumen interno        |

|                                       |           |
|---------------------------------------|-----------|
| Sistema de archivos                   | Fileshare |
| Exportaciones de sistemas de archivos | Share     |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Configuración

| Campo             | Descripción                                                                |
|-------------------|----------------------------------------------------------------------------|
| Host InfiniBox    | Dirección IP o nombre de dominio completo del nodo de gestión de InfiniBox |
| Nombre de usuario | Nombre de usuario para el nodo de gestión de InfiniBox                     |
| Contraseña        | Contraseña para el nodo de gestión de InfiniBox                            |

### Configuración avanzada

| Campo                                    | Descripción                                                                   |
|------------------------------------------|-------------------------------------------------------------------------------|
| Puerto TCP                               | Puerto TCP utilizado para conectarse a InfiniBox Server (predeterminado 443 ) |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)             |
| Tiempo de espera de conexión             | Tiempo de espera de conexión (60 segundos predeterminado)                     |

### Origen de datos de computación de Microsoft Azure

OnCommand Insights utiliza el recopilador de datos de computación de Azure para adquirir datos de inventario y rendimiento de instancias de computación de Azure.

### Requisitos

Necesita la siguiente información para configurar este recopilador de datos:

- Requisito de puerto: 443 HTTPS
- IP de REST de Azure Management (management.azure.com)
- Azure Service Principal Application (Cliente) ID (cuenta de usuario)
- Clave de autenticación principal de servicio de Azure (contraseña de usuario)

Debe configurar una cuenta de Azure para la detección de Insight. Una vez que la cuenta se haya configurado

correctamente y registre la aplicación en Azure, tendrá las credenciales necesarias para descubrir la instancia de Azure con Insight. El siguiente enlace describe cómo configurar la cuenta para Discovery:<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

### Configuración

Introduzca los datos en los campos de origen de datos según la tabla siguiente:

| Campo                                                                               | Descripción                                                                                                               |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ID de aplicación principal de servicios Azure (cliente) (se requiere rol de lector) | ID de inicio de sesión en Azure. Requiere acceso a la función Reader.                                                     |
| ID de inquilino de Azure                                                            | ID de inquilino de Microsoft                                                                                              |
| Clave de autenticación principal del servicio Azure                                 | Clave de autenticación de inicio de sesión                                                                                |
| Entiendo que Microsoft me factura por las solicitudes de API                        | Marque esto para verificar que Microsoft le da la cuenta de las solicitudes de API que ha realizado el sondeo de Insight. |

### Configuración avanzada

Introduzca los datos en los campos de origen de datos según la tabla siguiente:

| Campo                                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                               | El valor predeterminado es 60                                                                                                                                                                                                                                                                                                                                                                 |
| Elija "excluir" o "incluir" para aplicar al filtro de VM por etiquetas | Especifique si desea incluir o excluir las VM por etiquetas al recopilar datos. Si se selecciona "incluir", el campo clave de etiqueta no puede estar vacío.                                                                                                                                                                                                                                  |
| Claves de etiqueta y valores en los que se filtran las VM              | Haga clic en <b>+ Filter Tag</b> para elegir qué equipos virtuales (y discos asociados) incluir/excluir filtrando claves y valores que coincidan con claves y valores de etiquetas en el equipo virtual. Se requiere clave de etiqueta; el valor de etiqueta es opcional. Cuando el valor de etiqueta está vacío, la máquina virtual se filtra siempre que coincida con la clave de etiqueta. |
| Intervalo de sondeo de rendimiento (seg.)                              |                                                                                                                                                                                                                                                                                                                                                                                               |

### Origen de datos Azure NetApp Files

Este origen de datos adquiere datos de inventario y rendimiento para Azure NetApp Files (ANF).

## Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Requisito de puerto: 443 HTTPS
- IP de REST de Azure Management (management.azure.com)
- Azure Service Principal Application (Cliente) ID (cuenta de usuario)
- Clave de autenticación principal de servicio Azure (contraseña de usuario)
- Debe configurar una cuenta de Azure para la detección de Cloud Insights.

Una vez que la cuenta se haya configurado correctamente y registre la aplicación en Azure, tendrá las credenciales necesarias para descubrir la instancia de Azure con Cloud Insights. En el siguiente enlace se describe cómo configurar la cuenta para la detección:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

## Configuración

| Campo                                                        | Descripción                                                                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ID de aplicación principal de servicios Azure (cliente)      | ID de inicio de sesión en Azure                                                                                           |
| ID de inquilino de Azure                                     | ID de inquilino de Azure                                                                                                  |
| Clave de autenticación principal del servicio Azure          | Clave de autenticación de inicio de sesión                                                                                |
| Entiendo que Microsoft me factura por las solicitudes de API | Marque esto para verificar que Microsoft le da la cuenta de las solicitudes de API que ha realizado el sondeo de Insight. |

## Configuración avanzada

| Campo                                    | Descripción                           |
|------------------------------------------|---------------------------------------|
| Intervalo de sondeo de inventario (mín.) | El valor predeterminado es 60 minutos |

## Origen de datos de Microsoft Hyper-V.

Para la configuración, el origen de datos de Microsoft Hyper-V requiere la dirección IP o el nombre DNS resoluble para el host físico (hipervisor). Este origen de datos utiliza PowerShell (anteriormente usado WMI).

## Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de Hyper-V. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |               |
|----------------------------|---------------|
| Plazo del proveedor/modelo | Insight plazo |
|----------------------------|---------------|



|                                                              |                  |
|--------------------------------------------------------------|------------------|
| Disco duro virtual                                           | Disco virtual    |
| Host                                                         | Host             |
| Máquina virtual                                              | Máquina virtual  |
| Volúmenes compartidos de clúster (CSV), volumen de partición | Almacén de datos |
| Dispositivo SCSI de Internet, LUN SCSI de ruta múltiple      | LUN              |
| Puerto Fibre Channel                                         | Puerto           |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- El Hyper-V requiere que se abra el puerto 5985 para la recopilación de datos y el acceso y la gestión remotos.
- Dirección IP del nodo del grupo de clústeres
- Usuario y contraseña del administrador local en el hipervisor
- Cuenta de usuario de nivel administrativo
- Requisitos de puerto: Puerto 135 y puertos TCP dinámicos asignados a 1024-65535 para Windows 2003 y versiones anteriores, y 49152-65535 para Windows 2008.
- La resolución DNS debe tener éxito, incluso si el recopilador de datos sólo está apuntando a una dirección IP.
- Cada hipervisor de Hyper-V debe tener activado «'medición de recursos» para cada máquina virtual, en cada host. Esto permite que cada hipervisor tenga más datos disponibles para Cloud Insights en cada invitado. Si no se define esto, se adquieren menos métricas de rendimiento para cada invitado. Encontrará más información sobre la medición de recursos en la documentación de microsoft:

["Descripción general de la medición de recursos de Hyper-V."](#)

["Enable-VMResourceMetering"](#)

### Configuración

| Campo                        | Descripción                                                                      |
|------------------------------|----------------------------------------------------------------------------------|
| Dirección IP del host físico | La dirección IP o el nombre de dominio completo para el host físico (hipervisor) |
| Nombre de usuario            | El nombre de usuario del administrador del hipervisor                            |

|            |                                                  |
|------------|--------------------------------------------------|
| Contraseña | Contraseña del hipervisor                        |
| Dominio NT | El nombre DNS que utilizan los nodos del clúster |

#### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |
| Tiempo de espera de conexión (ms)        | Tiempo de espera de conexión (60000 ms predeterminado)            |

#### Origen de datos de Clustered Data ONTAP de NetApp

Este origen de datos se debe utilizar en sistemas de almacenamiento que utilicen Clustered Data ONTAP, y requiere una cuenta de administrador que se utilice para llamadas API de solo lectura.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de Clustered Data ONTAP. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Disco                      | Disco                  |
| Grupo RAID                 | Grupo de discos        |
| Clúster                    | Reducida               |
| Nodo                       | Nodo de almacenamiento |
| Agregado                   | Pool de almacenamiento |
| LUN                        | Volumen                |
| Volumen                    | Volumen interno        |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- Cuenta de administrador utilizada para llamadas API de sólo lectura
- La IP de destino es la LIF de gestión del clúster
- Nombre de usuario (con nombre de rol de solo lectura para la aplicación ontapi en el Vserver predeterminado) y contraseña para iniciar sesión en el clúster de NetApp
- Requisitos del puerto: 80 o 443
- Requisitos de licencia: Se requiere licencia FCP y volúmenes asignados/enmascarados para la detección

## Configuración

| Campo                   | Descripción                                                           |
|-------------------------|-----------------------------------------------------------------------|
| IP de gestión de NetApp | La dirección IP o el nombre de dominio completo del clúster de NetApp |
| Nombre de usuario       | Nombre de usuario del clúster de NetApp                               |
| Contraseña              | La contraseña del clúster de NetApp                                   |

## Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)    |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

## Almacenamiento Clustered Data ONTAP de NetApp

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de Clustered Data ONTAP de NetApp.

## Terminología de almacenamiento de Clustered Data ONTAP

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento de Clustered Data ONTAP de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Modelo — una lista delimitada por comas de los nombres de modelo de nodo discretos únicos dentro de este clúster. Si todos los nodos de los clústeres tienen el mismo tipo de modelo, solo aparecerá un nombre de modelo.
- Proveedor — mismo nombre de proveedor que se vería si estuviera configurando un nuevo origen de datos.
- Número de serie: El número de serie de la matriz. En sistemas de almacenamiento de arquitectura en clúster como Clustered Data ONTAP de NetApp, este número de serie puede ser menos útil que los números de serie de «nodos de almacenamiento» individuales.

- IP — generalmente serán los IP(s) o los hostname(s) tal como están configurados en el origen de datos.
- Versión de microcódigo — firmware.
- Capacidad bruta — base 2 suma de todos los discos físicos del sistema, sin importar su función.
- Latencia: Representación de lo que experimentan las cargas de trabajo que se enfrentan al host, tanto en lecturas como escrituras. Lo ideal es que OCI externe este valor directamente, pero no suele ser el caso. En lugar de que la cabina ofrezca esta configuración, OCI suele realizar un cálculo ponderado por IOPS derivado de las estadísticas de los volúmenes internos individuales.
- Rendimiento: Agregado de volúmenes internos.
- Administración: Puede contener un hipervínculo para la interfaz de administración del dispositivo. Creado mediante programación por el origen de datos de Insight como parte de los informes de inventario.

## Pool de almacenamiento de Clustered Data ONTAP

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento de Clustered Data ONTAP de NetApp.

## Terminología de Clustered Data ONTAP Storage Pool

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pool de almacenamiento de Clustered Data ONTAP de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento: En qué cabina de almacenamiento vive este pool. Obligatorio.
- Tipo — valor descriptivo de una lista de posibilidades enumeradas. Lo más habitual será «agregado» o ««Grupo RAID»»»».
- Nodo: Si la arquitectura de esta cabina de almacenamiento pertenece a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool — Sí/no valor — ¿este pool basado en SATA/SAS tiene SSD utilizados para la aceleración del almacenamiento en caché?
- Redundancia — nivel de RAID o esquema de protección. RAID\_DP es de doble paridad, RAID\_TP es de triple paridad.
- Capacidad: Los valores aquí son los lógicos utilizados, la capacidad utilizable y la capacidad total lógica, así como el porcentaje utilizado en estos.
- Capacidad sobrecomprometida: Si se utilizan tecnologías de eficiencia, se asigna una suma total de capacidades de volumen o volumen interno mayor que la capacidad lógica del pool de almacenamiento, el valor porcentual será mayor que 0 %.
- Snapshot: Las capacidades de Snapshot utilizadas y totales, si su arquitectura de pool de almacenamiento dedica parte de su capacidad a los segmentos, en exclusiva para los snapshots. Es probable que las configuraciones de ONTAP en MetroCluster lo muestren, mientras que otras configuraciones de ONTAP son menos.
- Utilización: Valor de porcentaje que muestra el mayor porcentaje de ocupación de disco de cualquier disco que contribuye a la capacidad de este pool de almacenamiento. El aprovechamiento de disco no tiene necesariamente una fuerte correlación con el rendimiento de la cabina: El aprovechamiento puede ser elevado debido a la recompilación de discos, a actividades de deduplicación, etc. en ausencia de cargas de trabajo basadas en host. Asimismo, las implementaciones de replicación de muchas cabinas pueden impulsar el uso del disco sin mostrar como volumen interno o carga de trabajo de volumen.
- IOPS: La suma de IOPS de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.

- Rendimiento: La suma del rendimiento de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.

#### Nodo de almacenamiento Clustered Data ONTAP

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino del nodo de almacenamiento de Clustered Data ONTAP de NetApp.

#### Terminología de nodos de almacenamiento de Clustered Data ONTAP

Los siguientes términos se aplican a objetos o referencias que puede encontrar en páginas de destino de activos de pool de almacenamiento de Clustered Data ONTAP de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento:- de qué cabina de almacenamiento forma parte este nodo. Obligatorio.
- PARTNER de ALTA DISPONIBILIDAD: En las plataformas en las que un nodo se conmuta al nodo de respaldo uno y solo otro, normalmente se verá aquí.
- Estado:- estado del nodo. Solo disponible cuando la matriz está lo suficientemente sana para ser inventariada por una fuente de datos.
- Modelo — nombre de modelo del nodo.
- Versión: Nombre de versión del dispositivo.
- Número de serie: El número de serie del nodo.
- Memoria — memoria base 2 si está disponible.
- Utilización — en ONTAP, se trata de un índice de tensión del controlador a partir de un algoritmo propio. Con cada encuesta de rendimiento, se informará de una cifra entre 0 y 100 % que es la más alta entre la contención de disco WAFL o el uso medio de CPU. Si observa un valor sostenido > 50 %, esto indica que se ha dimensionamiento insuficiente; potencialmente, una controladora/nodo no tiene lo suficientemente grande o no hay suficientes discos giratorios para absorber la carga de trabajo de escritura.
- IOPS — derivado directamente de las llamadas ZAPI de ONTAP en el objeto del nodo.
- Latencia: Se deriva directamente de las llamadas ZAPI de ONTAP del objeto del nodo.
- Rendimiento — derivado directamente de las llamadas ZAPI de ONTAP en el objeto del nodo.
- Procesadores — número de CPU.

#### Origen de los datos en Clustered Data ONTAP para Unified Manager de NetApp

Este origen de datos recopila datos de ONTAP 8.1.x de la base de datos de Unified Manager (UM) 6.0 o posterior. Mediante este origen de datos, Insight detecta todos los clústeres configurados y rellenados en UM. Para mejorar la eficiencia, Insight no llama ZAPI en el clúster mismo. Este origen de datos no admite el rendimiento.

#### Configuración



Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

| Campo | Descripción |
|-------|-------------|
|-------|-------------|

|                    |                                                                                 |
|--------------------|---------------------------------------------------------------------------------|
| Unified Manager IP | La dirección IP o el nombre de dominio completo de Unified Manager              |
| Nombre de usuario  | Nombre de usuario de Unified Manager                                            |
| Contraseña         | La contraseña de Unified Manager                                                |
| Puerto             | Puerto utilizado para la comunicación con Unified Manager (predeterminado 3306) |

#### Configuración avanzada

| Campo                                   | Descripción                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (min) | Intervalo entre sondeos de inventario (predeterminado 15 minutos)           |
| Excluir clústeres                       | Lista de direcciones IP de clúster separadas por comas que se van a excluir |

#### Origen de datos con sistema operativo Data ONTAP de NetApp en 7-Mode

En los sistemas de almacenamiento que utilizan el software Data ONTAP funcionando en 7-Mode, se debe utilizar el origen de datos de ONAPI, que utiliza la CLI para obtener los números de capacidad.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de Data ONTAP 7-Mode de NetApp. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                    |                        |
|------------------------------------|------------------------|
| Plazo del proveedor/modelo         | Insight plazo          |
| Disco                              | Disco                  |
| Grupo RAID                         | Grupo de discos        |
| Servidor dedicado a almacenamiento | Reducida               |
| Servidor dedicado a almacenamiento | Nodo de almacenamiento |
| Agregado                           | Pool de almacenamiento |
| LUN                                | Volumen                |

|         |                 |
|---------|-----------------|
| Volumen | Volumen interno |
|---------|-----------------|



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- Dirección IP de la controladora de almacenamiento de FAS y el asociado
- Puerto 443
- Nombre de usuario y contraseña para el controlador y el asociado
- Un nombre de usuario y contraseña de nivel de administrador personalizados para la controladora y la controladora asociada con las siguientes funcionalidades de rol para 7-Mode:
  - "api-\*": Utilice esto para permitir que OnCommand Insight ejecute todos los comandos de la API de almacenamiento de NetApp.
  - "login-http-admin": Utilice esto para permitir que OnCommand Insight se conecte al almacenamiento de NetApp a través de HTTP.
  - «Security-api-vfiler»: Utilice esto para permitir a OnCommand Insight ejecutar comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": Utilice esto para leer las opciones del sistema de almacenamiento.
  - "cli-lun": Acceda a estos comandos para gestionar las LUN. Muestra el estado (ruta de LUN, tamaño, estado en línea/sin conexión y estado compartido) de la LUN o clase de LUN determinada.
  - "cli-df": Utilice esta opción para mostrar el espacio libre en disco.
  - "cli-ifconfig": Utilice esta opción para mostrar interfaces y direcciones IP.

## Configuración

| Campo                                                                                                  | Descripción                                                                                                                     |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Dirección del servidor dedicado a almacenamiento                                                       | La dirección IP o el nombre de dominio completo para los servidores dedicados a almacenamiento de NetApp                        |
| Nombre de usuario                                                                                      | Nombre de usuario para servidores dedicados al almacenamiento de NetApp                                                         |
| Contraseña                                                                                             | Contraseña para servidores dedicados a almacenamiento de NetApp                                                                 |
| Dirección del servidor dedicado a almacenamiento de partners de alta disponibilidad en clúster         | La dirección IP o el nombre de dominio completo para el servidor dedicado a almacenamiento para partners de alta disponibilidad |
| Nombre de usuario del servidor dedicado a almacenamiento de partners de alta disponibilidad en clúster | Nombre de usuario del servidor dedicado a almacenamiento para partners de alta disponibilidad de NetApp                         |

|                                                                              |                                                                                                      |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Contraseña de almacenamiento para partners de alta disponibilidad en clúster | Contraseña para el servidor dedicado a almacenamiento para partners de alta disponibilidad de NetApp |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|

### Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)    |
| Tipo de conexión                         | Elija el tipo de conexión                                            |
| Puerto de conexión                       | Puerto que se utiliza para la API de NetApp                          |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

### Conexión de sistemas de almacenamiento

Como alternativa al uso del usuario administrativo predeterminado para este origen de datos, es posible configurar un usuario con derechos administrativos directamente en los sistemas de almacenamiento de NetApp, de tal modo que este origen de datos pueda adquirir los datos de los sistemas de almacenamiento NetApp.

La conexión con los sistemas de almacenamiento NetApp requiere que el usuario, especificado al adquirir el filers principal (en el que existe el sistema de almacenamiento), cumpla las siguientes condiciones:

- El usuario debe estar en vfiler0 (archivador raíz/pfiler).

Los sistemas de almacenamiento se adquieren cuando se adquiere el filer principal.

- Los siguientes comandos definen las capacidades de los roles de usuario:
  - "api-\*": Utilice esto para permitir que OnCommand Insight ejecute todos los comandos de la API de almacenamiento de NetApp. Este comando es necesario para utilizar LA ZAPI.
  - "login-http-admin": Utilice esto para permitir que OnCommand Insight se conecte al almacenamiento de NetApp a través de HTTP. Este comando es necesario para utilizar LA ZAPI.
  - «Security-api-vfiler»: Utilice esto para permitir a OnCommand Insight ejecutar comandos de API de almacenamiento de NetApp para recuperar información de la unidad vFiler.
  - "cli-options": Para el comando "OPTIONS" y se utiliza para la IP del partner y las licencias habilitadas.
  - "cli-lun": Acceda a este comando para gestionar las LUN. Muestra el estado (ruta de LUN, tamaño, estado en línea/sin conexión y estado compartido) de la LUN o clase de LUN determinada.
  - "cli-df": Para comandos "df -s", "df -r", "df -A -r" y se utiliza para mostrar espacio libre.
  - "cli-ifconfig": Para el comando "ifconfig -a" y se utiliza para obtener la dirección IP del servidor de almacenamiento.
  - "cli-rdfile": Para el comando "rdfile /etc/netgroup" y se utiliza para obtener grupos de red.
  - "cli-date": Comando "date" y se usa para obtener la fecha completa para obtener las copias Snapshot.



- "cli-snap": Para el comando "snap list" y se utiliza para obtener copias snapshot.

Si no se proporcionan permisos de cli o snap-cli, la adquisición puede finalizar, pero no se notifican las copias snapshot.

Para adquirir correctamente un origen de datos de 7-Mode y no generar ninguna advertencia en el sistema de almacenamiento, debe usar una de las siguientes cadenas de comandos para definir los roles de usuario. La segunda cadena que aparece aquí es una versión simplificada de la primera:

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-  
df,cli-lun,cli-ifconfig,cli-date,cli-snap,  
or  
login-http-admin,api-*,security-api-vfile,cli-*
```

## Origen de datos E-Series de NetApp

El origen de datos de E-Series de NetApp recopila información de inventario y rendimiento. Hay dos configuraciones posibles (firmware 6.x y firmware 7.x+) y ambas tienen los mismos valores.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos E-Series de NetApp. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Unidad                     | Disco                  |
| Grupo de volúmenes         | Grupo de discos        |
| Cabina de almacenamiento   | Reducida               |
| Controladora               | Nodo de almacenamiento |
| Grupo de volúmenes         | Pool de almacenamiento |
| Volumen                    | Volumen                |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

- La dirección IP de cada controladora de la cabina
- Requisito de puerto 2463

## Configuración

| Campo                                                                      | Descripción                                                                      |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Lista separada por comas de las IP de controladora de SANtricity de cabina | Direcciones IP y/o nombres de dominio completos para las controladoras de cabina |

## Configuración avanzada

| Campo                                                    | Descripción                                                          |
|----------------------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)                 | Intervalo entre sondeos de inventario (predeterminado 30 minutos)    |
| Intervalo de sondeo de rendimiento (hasta 3600 segundos) | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

## Almacenamiento E-Series de NetApp

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento E-Series de NetApp.

### Terminología de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Modelo — nombre del modelo del dispositivo.
- Proveedor — mismo nombre de proveedor que se vería si estuviera configurando un nuevo origen de datos.
- Número de serie: El número de serie de la matriz. En sistemas de almacenamiento de arquitectura en clúster como Clustered Data ONTAP de NetApp, este número de serie puede ser menos útil que los números de serie de «nodos de almacenamiento» individuales.
- IP — generalmente serán los IP(s) o los hostname(s) tal como están configurados en el origen de datos.
- Versión de microcódigo — firmware.
- Capacidad bruta — base 2 suma de todos los discos físicos del sistema, sin importar su función.
- Latencia: Representación de lo que experimentan las cargas de trabajo que se enfrentan al host, tanto en lecturas como escrituras. Insight calcula una media ponderada de IOPS derivada de los volúmenes del almacenamiento.
- Rendimiento:- rendimiento orientado al host total de la cabina. Insight resume el rendimiento de los volúmenes para obtener este valor.
- Administración: Puede contener un hipervínculo para la interfaz de administración del dispositivo. Creado mediante programación por el origen de datos de Insight como parte de los informes de inventario.

### Pool de almacenamiento de E-Series

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de

## destino de activos de pools de almacenamiento E-Series de NetApp.

### Terminología de pools de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento: En qué cabina de almacenamiento vive este pool. Obligatorio.
- Tipo — valor descriptivo de una lista de posibilidades enumeradas. Lo más habitual será «'Thin Provisioning» o «'Grupo RAID'».
- Nodo: Si la arquitectura de esta cabina de almacenamiento pertenece a un nodo de almacenamiento específico, su nombre se verá aquí como un hipervínculo a su propia página de destino.
- Utiliza Flash Pool — valor Sí/no.
- Redundancia — nivel de RAID o esquema de protección. E-Series informa «'RAID 7'» para pools DDP.
- Capacidad: Los valores aquí son los lógicos utilizados, la capacidad utilizable y la capacidad total lógica, así como el porcentaje utilizado en estos. Ambos valores incluyen la capacidad de «'conservación» de E-Series, lo que resulta en números y el porcentaje es superior a lo que puede mostrar la interfaz de usuario de E-Series.
- Capacidad sobrecomprometida: Si se utilizan tecnologías de eficiencia, se ha asignado una suma total de capacidad de volumen mayor que la capacidad lógica del pool de almacenamiento, el valor porcentual será mayor que 0 %.
- Snapshot: Las capacidades de Snapshot utilizadas y totales, si su arquitectura de pool de almacenamiento dedica parte de su capacidad a los segmentos, en exclusiva para los snapshots.
- Utilización: Valor de porcentaje que muestra el mayor porcentaje de actividad de disco de cualquier capacidad que contribuye a este pool de almacenamiento. El aprovechamiento de disco no tiene necesariamente una fuerte correlación con el rendimiento de la cabina: El aprovechamiento puede ser elevado debido a la recompilación de discos, a actividades de deduplicación, etc. en ausencia de cargas de trabajo condicionadas por el host. Asimismo, las implementaciones de replicación de muchas cabinas pueden impulsar el uso del disco sin mostrar como carga de trabajo de volumen.
- IOPS: La suma de IOPS de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.
- Rendimiento: La suma del rendimiento de todos los discos que contribuyen a la capacidad de este pool de almacenamiento.

### Nodo de almacenamiento E-Series

Términos que se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos del nodo de almacenamiento E-Series de NetApp.

### Terminología del nodo de almacenamiento E-Series

Los siguientes términos se aplican a objetos o referencias que puede encontrar en las páginas de destino de activos de pools de almacenamiento E-Series de NetApp. Muchos de estos términos también se aplican a otros recopiladores de datos.

- Almacenamiento:- de qué cabina de almacenamiento forma parte este nodo. Obligatorio.
- PARTNER de ALTA DISPONIBILIDAD: En las plataformas en las que un nodo se conmuta al nodo de respaldo uno y solo otro, normalmente se verá aquí.

- Estado:- estado del nodo. Solo disponible cuando la matriz está lo suficientemente sana para ser inventariada por una fuente de datos.
- Modelo — nombre de modelo del nodo.
- Versión: Nombre de versión del dispositivo.
- Número de serie: El número de serie del nodo.
- Memoria — memoria base 2 si está disponible.
- Utilización — la utilización no está actualmente disponible para E-Series de NetApp.
- IOPS: Calculado sumando todos los IOPS de los volúmenes que pertenecen exclusivamente a este nodo.
- Latencia: Un número que representa la latencia del host o el tiempo de respuesta típicos de esta controladora. Las estadísticas calculan una media ponderada de IOPS de los volúmenes que pertenecen exclusivamente a este nodo.
- Rendimiento: Número que representa el rendimiento impulsado por el host en esta controladora. Calculado sumando todo el rendimiento de los volúmenes que pertenecen exclusivamente a este nodo.
- Procesadores — número de CPU.

### **Origen de datos de sistemas de archivos de VM y host de NetApp**

Puede utilizar el origen de datos de sistemas de archivos de VM y host de NetApp para recuperar detalles del sistema de archivos y asignaciones de recursos de almacenamiento para todos los sistemas de archivos de hosts y máquinas virtuales (máquinas virtuales) de Microsoft Windows y para todos los equipos virtuales Linux compatibles (los que están virtualmente asignados solo) Existente en el servidor de Insight que se anota con el grupo de recursos informáticos (CRG) configurado.

#### **Requisitos generales**

- Esta función debe adquirirse por separado.

Si necesita ayuda, puede ponerse en contacto con su representante de Insight.

- Debe consultar la matriz de compatibilidad de Insight para verificar que el sistema operativo de máquina virtual o host es compatible.

Para verificar que se han creado los enlaces de los sistemas de archivos a los recursos de almacenamiento, compruebe que el tipo y la versión del proveedor de almacenamiento o de virtualización pertinentes informan sobre el volumen o los datos de identificación de discos virtuales necesarios.

#### **Requisitos de Microsoft Windows**

- Este origen de datos utiliza estructuras de datos del Instrumental de administración de ventanas (WMI) para recuperar datos.

Este servicio debe estar operativo y disponible de forma remota. En particular, el puerto 135 debe ser accesible y debe abrirse si está detrás de un firewall.

- Los usuarios de dominio de Windows deben tener los permisos adecuados para tener acceso a las estructuras WMI.
- Se requieren permisos de administrador.

- Puertos TCP dinámicos asignados a 1024-65535 para Windows 2003 y versiones anteriores
- Puertos 49152—65535 para Windows 2008



Como regla general, al intentar utilizar un firewall entre Insight, una AU y este origen de datos, debe consultar con su equipo de Microsoft para identificar los puertos que creen que serán necesarios.

### Requisitos de Linux

- Este origen de datos utiliza una conexión de Secure Shell (SSH) para ejecutar comandos en máquinas virtuales Linux.

El servicio SSH debe estar operativo y disponible de forma remota. En particular, el puerto 22 debe ser accesible y debe abrirse si está detrás de un firewall.

- Los usuarios de SSH deben tener permisos sudo para ejecutar comandos de solo lectura en máquinas virtuales de Linux.

Debe usar la misma contraseña para iniciar sesión en SSH y para responder a cualquier desafío de contraseña sudo.

### Recomendaciones de uso

- Debe anotar un grupo de hosts y máquinas virtuales que tengan credenciales de sistema operativo comunes utilizando la misma anotación Compute Resource Group.

Cada grupo tiene una instancia de este origen de datos que descubre los detalles del sistema de archivos de dichos hosts y máquinas virtuales.

- Si tiene una instancia de este origen de datos para la cual la tasa de éxito es baja (por ejemplo, OnCommand Insight está detectando detalles del sistema de archivos de solo 50 de 1000 hosts y máquinas virtuales de un grupo), Debería mover los hosts y las máquinas virtuales para las que la detección se realiza correctamente a un grupo de recursos de computación independiente.

### Configuración

| Campo                          | Descripción                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nombre de usuario              | Usuario del sistema operativo con derechos adecuados para recuperar datos del sistema de archivos para usuarios del sistema operativo Windows, debe incluir el prefijo de dominio.                                                                                                                                                  |
| Contraseña                     | Contraseña para el usuario del sistema operativo                                                                                                                                                                                                                                                                                    |
| Grupo de recursos informáticos | El valor de anotación utilizado para marcar máquinas virtuales y hosts para el origen de datos detecta sistemas de archivos. Un valor en blanco indica que el origen de datos detecta sistemas de archivos para todos los hosts y máquinas virtuales que no están anotados actualmente con ningún grupo de recursos de computación. |

## Configuración avanzada

| Campo                                   | Descripción                                                        |
|-----------------------------------------|--------------------------------------------------------------------|
| Intervalo de sondeo de inventario (min) | Intervalo entre sondeos de inventario (predeterminado 360 minutos) |

## Fuente de datos SolidFire de NetApp

El origen de los datos de SolidFire de NetApp es compatible con las configuraciones de SolidFire iSCSI y Fibre Channel, tanto para inventario como para recopilación del rendimiento.

El origen de datos de SolidFire utiliza la API DE REST de SolidFire. La unidad de adquisición en la que reside el origen de datos debe poder iniciar conexiones HTTPS con el puerto TCP 443 en la dirección IP de administración del clúster SolidFire. El origen de los datos necesita credenciales capaces de realizar consultas API DE REST en el clúster de SolidFire.

## Terminología

OnCommand Insight adquiere la siguiente información de inventario a partir del origen de datos de NetApp SolidFire. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                 |                        |
|-------------------------------------------------|------------------------|
| Plazo del proveedor/modelo                      | Insight plazo          |
| Unidad                                          | Disco                  |
| Clúster                                         | Reducida               |
| Nodo                                            | Nodo de almacenamiento |
| Volumen                                         | Volumen                |
| Puerto Fibre Channel                            | Puerto                 |
| Grupo de acceso de volúmenes, asignación de LUN | Asignación de volumen  |
| Sesión iSCSI                                    | Máscara de volumen     |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP virtual de gestión
- Puerto 443

## Configuración

| Campo                                  | Descripción                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------|
| Dirección IP virtual de gestión (MVIP) | La dirección IP virtual de gestión del clúster de SolidFire                 |
| Nombre de usuario                      | Nombre que se utiliza para iniciar sesión en el clúster SolidFire           |
| Contraseña                             | La contraseña que se utiliza para iniciar sesión en el clúster de SolidFire |

## Configuración avanzada

| Campo                                    | Descripción                                                                        |
|------------------------------------------|------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)                  |
| Puerto TCP                               | Puerto TCP utilizado para conectar con el servidor SolidFire (predeterminado 443 ) |
| Tiempo de espera de conexión (s)         | Tiempo de espera de conexión (60 segundos predeterminado)                          |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)               |

## Resolución de problemas

Cuando SolidFire informa de un error, se muestra en OnCommand Insight de la siguiente manera:

```
An error message was received from a SolidFire device while trying to retrieve data. The call was <method> (<parameterString> ). The error message from the device was (check the device manual): <message>
```

Donde:

- <method> es un método HTTP, como GET o PUT.
- <parameterString> es una lista separada por comas de parámetros que se incluyeron en LA llamada DE DESCANSO.
- El <message> es lo que el dispositivo devolvió como mensaje de error.

## Fuente de datos StorageGRID de NetApp

Este origen de datos recopila datos de inventario y rendimiento para StorageGRID.

## Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Dirección IP del host StorageGRID
- Nombre de usuario y contraseña para un usuario que tiene asignadas las funciones de consulta métrica y acceso de inquilino
- Puerto 443

## Configuración

| Campo                                       | Descripción                                                  |
|---------------------------------------------|--------------------------------------------------------------|
| Dirección IP del host de StorageGRID (MVIP) | La dirección IP del host de la StorageGRID                   |
| Nombre de usuario                           | Nombre que se utiliza para iniciar sesión en la StorageGRID  |
| Contraseña                                  | Contraseña que se utiliza para iniciar sesión en StorageGRID |

## Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)    |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 900 segundos) |

## Origen de datos de OpenStack

El origen de datos de OpenStack (API DE REST/KVM) recopila información sobre las instancias de hardware de OpenStack. Este origen de datos recopila datos de inventario para todas las instancias de OpenStack y, opcionalmente, datos de rendimiento de los equipos virtuales.

## Requisitos

A continuación, se enumeran los requisitos para configurar el origen de datos de OpenStack.

- La dirección IP de la controladora OpenStack
- Se recomiendan las credenciales de rol de administrador de OpenStack y el acceso sudo al hipervisor KVM de Linux.





Si no utiliza una cuenta de administrador ni privilegios equivalentes de administrador, puede adquirir datos del origen de datos. Deberá modificar el archivo de configuración de políticas (es decir, `etc/nova/policy.json`) para permitir a los usuarios con un rol que no sea administrador llamar a la API:

- `"os_compute_api:os-availability-zone:detail": ""`
- `"os_compute_api:os-hipervisores": ""`
- `os_compute_api:servidores:detail:get_all_arrendatarios": ""`
- Para la recopilación del rendimiento, debe instalarse y configurarse el módulo Ceilometer de OpenStack. La configuración del Ceilometer se realiza editando la `nova.conf` Archivo para cada hipervisor y, a continuación, reinicie el servicio de computación Nova en cada hipervisor. La opción cambia de nombre para diferentes versiones de OpenStack:
  - Icehouse
  - Juno
  - Kilo
  - Libertad
  - Mitaka
  - Newton
  - Ocata
- Para las estadísticas de CPU, `"Compute_Monitores=ComputeDriverCPUMonitor"` debe estar activado en `/etc/nova/nova.conf` en nodos de computación.
- Requisitos de puerto:
  - 5000 para http y 13000 para https, para el servicio Keystone
  - 22 para SSH KVM
  - 8774 para Nova Compute Service
  - 8776 para Cinder Block Service
  - 8777 para el servicio de rendimiento Ceilometer
  - 9292 para el servicio de imágenes Glance



El puerto se enlaza al servicio específico y el servicio puede ejecutarse en la controladora u otro host en los entornos más grandes.

## Configuración

| Campo                                     | Descripción                                                               |
|-------------------------------------------|---------------------------------------------------------------------------|
| Dirección IP de la controladora OpenStack | La dirección IP o el nombre de dominio completo del controlador OpenStack |
| Administrador de OpenStack                | Nombre de usuario para un administrador de OpenStack                      |

|                                                                                         |                                                                                |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Contraseña de OpenStack                                                                 | La contraseña que se usa para el administrador de OpenStack                    |
| Inquilino de administrador de OpenStack                                                 | Inquilino de administrador de OpenStack                                        |
| Usuario sudo KVM                                                                        | Nombre de usuario sudo KVM                                                     |
| Elija 'Contraseña' o 'Archivo de claves OpenSSH' para especificar el tipo de credencial | El tipo de credencial utilizado para conectarse al dispositivo a través de SSH |
| Ruta completa a la clave privada de inventario                                          | Ruta completa a la clave privada de inventario                                 |
| Contraseña sudo KVM                                                                     | Contraseña sudo KVM                                                            |

### Configuración avanzada

| Campo                                                              | Descripción                                                                            |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Habilite la detección de inventario del hipervisor a través de SSH | Compruebe esto para habilitar la detección de inventario de hipervisor a través de SSH |
| Puerto de URL de administrador de OpenStack                        | Puerto de URL de administrador de OpenStack                                            |
| Utilice HTTPS                                                      | Compruebe que utilice HTTP seguro                                                      |
| Tiempo de espera de conexión HTTP (s)                              | Tiempo de espera para la conexión HTTP (predeterminado 300 segundos)                   |
| Puerto SSH                                                         | Puerto utilizado para SSH                                                              |
| Tiempo de espera del proceso SSH (s)                               | Tiempo de espera del proceso SSH (30 segundos predeterminado)                          |
| Reintentos de proceso SSH                                          | Número de intentos de reintento de inventario                                          |
| Intervalo de sondeo de inventario (mín.)                           | Intervalo entre sondeos de inventario (predeterminado 20 minutos)                      |

### Origen de datos de Oracle ZFS

El origen de datos Oracle ZFS admite la recopilación de inventario y rendimiento.

### Terminología

OnCommand Insight adquiere la siguiente información de inventario de este origen de datos. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                        |
|----------------------------|------------------------|
| Plazo del proveedor/modelo | Insight plazo          |
| Disco (SDD)                | Disco                  |
| Clúster                    | Reducida               |
| Controladora               | Nodo de almacenamiento |
| LUN                        | Volumen                |
| Mapa de LUN                | Asignación de volumen  |
| Iniciador, destino         | Máscara de volumen     |
| Share                      | Volumen interno        |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

### Requisitos

A continuación se muestran los requisitos para configurar este origen de datos:

- Nombres de host para ZFS Controller-1 y ZFS Controller-2
- Nombre de usuario y credenciales del administrador
- Requisito de puerto: 215 HTTP/HTTPS

### Configuración

|                                      |                                                                     |
|--------------------------------------|---------------------------------------------------------------------|
| Nombre de host de controladora ZFS-1 | Nombre del host de la controladora de almacenamiento 1              |
| Nombre de host ZFS Controller-2      | Nombre del host de la controladora de almacenamiento 2              |
| Nombre de usuario                    | El nombre de usuario de administrador del sistema de almacenamiento |
| Contraseña                           | Contraseña de la cuenta de usuario administrador                    |

### Configuración avanzada

|            |                                                                  |
|------------|------------------------------------------------------------------|
| Campo      | Descripción                                                      |
| Puerto TCP | Puerto TCP utilizado para conectarse a ZFS (predeterminado 215 ) |

|                                        |                                                                      |
|----------------------------------------|----------------------------------------------------------------------|
| Tipo de conexión                       | HTTP o HTTPS                                                         |
| Intervalo del sondeo de inventario     | Intervalo de sondeo de inventario (predeterminado 60 minutos)        |
| Tiempo de espera de conexión           | El valor predeterminado es 60 segundos                               |
| Intervalo de sondeo de rendimiento (s) | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

### Resolución de problemas

Algunas cosas para intentar si tiene problemas con este recopilador de datos:

|                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Problema:                                                                                | Pruebe lo siguiente:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| "Credenciales de inicio de sesión no válidas"                                            | Validar la cuenta de usuario y contraseña de ZFS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| "Error de configuración" con el mensaje de error "SE ha desactivado EL servicio "RESTST" | Compruebe que el servicio REST esté activado en este dispositivo.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| "Error de configuración " con el mensaje de error ""Usuario no autorizado para comando"" | <p>Probablemente debido a ciertos roles (por ejemplo, 'Advanced_Analytics') no se incluyen para el usuario configurado &lt;userName&gt;.solución posible:</p> <ul style="list-style-type: none"> <li>• Corrija el ámbito de análisis (estadístico) para el usuario \${USER} con la función de sólo lectura:- desde la pantalla Configuración → usuarios, coloque el ratón sobre la función y haga doble clic para permitir la edición</li> <li>• Seleccione "Análisis" en el menú desplegable ámbito. Aparece una lista de las propiedades posibles.</li> <li>• Haga clic en la casilla de verificación situada más arriba y seleccionará las tres propiedades.- haga clic en el botón Agregar situado en el lado derecho.</li> <li>• Haga clic en el botón aplicar situado en la parte superior derecha de la ventana emergente. Se cerrará la ventana emergente.</li> </ul> |

### Origen de datos de FlashArray de Pure Storage

El origen de datos de Pure Storage FlashArray (HTTP) se utiliza para recopilar información de la cabina flash de Pure Storage. Insight admite tanto el inventario como la recopilación de rendimiento.

## Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de FlashArray de Pure Storage. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                             |                                     |
|-------------------------------------------------------------|-------------------------------------|
| Plazo del proveedor/modelo                                  | Insight plazo                       |
| Unidad (SSD)                                                | Disco                               |
| Cabina                                                      | Reducida                            |
| Controladora                                                | Nodo de almacenamiento              |
| Volumen                                                     | Volumen                             |
| Puerto                                                      | Puerto                              |
| Asignación de LUN (host, grupo de hosts, puerto de destino) | Mapa de volumen, Máscara de volumen |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- Dirección IP del sistema de almacenamiento
- El nombre de usuario y la contraseña de la cuenta de administrador del sistema de almacenamiento de Pure.
- Requisito de puerto: HTTP/HTTPS 80/443

## Configuración

| Campo             | Descripción                                                                      |
|-------------------|----------------------------------------------------------------------------------|
| FlashArray Host   | La dirección IIP o el nombre de dominio completo de FlashArray Management Server |
| Nombre de usuario | Nombre de usuario del servidor de FlashArray Management                          |
| Contraseña        | Contraseña del servidor de gestión de FlashArray                                 |

## Configuración avanzada

| Campo | Descripción |
|-------|-------------|
|-------|-------------|

|                                          |                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------|
| Tipo de conexión                         | Servidor de gestión                                                            |
| Puerto TCP                               | Puerto TCP utilizado para conectar con FlashArray Server (predeterminado 443 ) |
| Tiempo de espera de conexión (s)         | Tiempo de espera de conexión (60 segundos predeterminado)                      |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 60 minutos)              |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)           |

### Fuente de datos del switch FC QLogic

Para la configuración, el origen de datos de QLogic FC Switch (SNMP) requiere la dirección de red del dispositivo FC Switch, especificado como una dirección IP, y una cadena de comunidad SNMP *de solo lectura* que se utiliza para acceder al dispositivo.

### Configuración

| Campo                | Descripción                                                            |
|----------------------|------------------------------------------------------------------------|
| Conmutador SANsurfer | Dirección IP o nombre de dominio completo para el conmutador SANSurfer |
| Versión de SNMP      | Versión de SNMP                                                        |
| Comunidad SNMP       | Cadena de comunidad SNMP                                               |
| Nombre de usuario    | Nombre de usuario del conmutador SANSurfer                             |
| Contraseña           | Contraseña para el conmutador SANSurfer                                |

### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 15 minutos) |
| Protocolo de autenticación SNMP          | Protocolo de autenticación SNMP (sólo SNMPv3)                     |
| Reintentos SNMP                          | Número de intentos de reintento SNMP                              |

|                                         |                                                                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Tiempo de espera de SNMP (ms)           | Tiempo de espera de SNMP (5000 ms predeterminado)                                                                           |
| Habilite el solapamiento                | Seleccione esta opción para activar el solapamiento                                                                         |
| Tiempo mínimo entre solapamientos (seg) | Tiempo mínimo entre intentos de adquisición activados por solapamientos (predeterminado 10 segundos)                        |
| Nombre de la estructura                 | El origen de datos informará del nombre de la estructura. Deje en blanco para informar el nombre de la estructura como WWN. |
| Intervalo de sondeo de rendimiento (s)  | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                                        |

### Fuente de datos de Red Hat (RHEV)

El origen de datos de Red Hat Enterprise Virtualization (REST) recopila información sobre las instancias de RHEV a través de HTTPS.

#### Requisitos

- Dirección IP del servidor RHEV a través del puerto 443 a través de la API DE REST
- Nombre de usuario y contraseña de solo lectura
- RHEV versión 3.0+

#### Configuración

| Campo                          | Descripción                                                 |
|--------------------------------|-------------------------------------------------------------|
| Dirección IP del servidor RHEV | Dirección IP o nombre de dominio completo del servidor RHEV |
| Nombre de usuario              | Nombre de usuario del servidor RHEV                         |
| Contraseña                     | Contraseña utilizada para el servidor RHEV                  |

#### Configuración avanzada

| Campo                                    | Descripción                                                       |
|------------------------------------------|-------------------------------------------------------------------|
| Puerto de comunicación HTTPS             | Puerto utilizado para la comunicación HTTPS con RHEV              |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos) |

|                                  |                                                           |
|----------------------------------|-----------------------------------------------------------|
| Tiempo de espera de conexión (s) | Tiempo de espera de conexión (60 segundos predeterminado) |
|----------------------------------|-----------------------------------------------------------|

### Fuente de datos de Violin Flash Memory Array

La fuente de datos Violin 6000-Series Flash Memory Array (HTTP) recopila información de la red para su análisis y validación de las cabinas de memoria flash Violin serie 6000.

#### Terminología



Este recopilador de datos ya no está disponible a partir de OnCommand Insight 7.3.11.

OnCommand Insight adquiere la siguiente información de inventario de la fuente de datos de matriz de memoria flash Violin serie 6000. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                                                 |                                     |
|-------------------------------------------------|-------------------------------------|
| Plazo del proveedor/modelo                      | Insight plazo                       |
| Módulo de memoria inteligente de Violin (VIIMM) | Disco                               |
| Contenedor                                      | Reducida                            |
| Puerta de enlace de memoria                     | Nodo de almacenamiento              |
| LUN                                             | Volumen                             |
| IGroup, destino                                 | Mapa de volumen, Máscara de volumen |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

#### Requisitos

- Se necesita un nombre de usuario y una contraseña de solo lectura para el almacenamiento.
- Se debe validar el acceso con un explorador web mediante la dirección IP de almacenamiento.

#### Configuración

| Campo                                                                       | Descripción                                                                                       |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Dirección IP o FQDN de la puerta de enlace principal de Violin Memory Array | Dirección IP o nombre de dominio completo de la puerta de enlace principal de Violin Memory Array |
| Nombre de usuario                                                           | Nombre de usuario de la puerta de enlace principal de Violin Memory Array                         |



|            |                                                                    |
|------------|--------------------------------------------------------------------|
| Contraseña | Contraseña de la puerta de enlace principal de Violin Memory Array |
|------------|--------------------------------------------------------------------|

#### Configuración avanzada

| Campo                                    | Descripción                                                          |
|------------------------------------------|----------------------------------------------------------------------|
| Puerto de comunicación                   | Puerto utilizado para la comunicación con la matriz Violin           |
| HTTPS habilitado                         | Seleccione para utilizar HTTPS                                       |
| Intervalo de sondeo de inventario (mín.) | Intervalo entre sondeos de inventario (predeterminado 20 minutos)    |
| Tiempo de espera de conexión (s)         | Tiempo de espera de conexión (60 segundos predeterminado)            |
| Intervalo de sondeo de rendimiento (s)   | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos) |

#### Origen de datos de VMware vSphere

El origen de datos de VMware vSphere (Web Services) recopila información del host ESX y requiere privilegios *de solo lectura* en todos los objetos del Centro virtual.

#### Terminología

OnCommand Insight adquiere la siguiente información de inventario del origen de datos de VMware vSphere. Para cada tipo de activo que adquiere Insight, se muestra la terminología más común utilizada en este activo. Al ver o solucionar problemas de este origen de datos, tenga en cuenta la siguiente terminología:

|                            |                  |
|----------------------------|------------------|
| Plazo del proveedor/modelo | Insight plazo    |
| Disco virtual              | Disco            |
| Host                       | Host             |
| Máquina virtual            | Máquina virtual  |
| Almacén de datos           | Almacén de datos |
| LUN                        | LUN              |
| Puerto Fibre Channel       | Puerto           |



Estos son sólo mapas terminológicos comunes y es posible que no representen todos los casos de este origen de datos.

## Requisitos

- Dirección IP del servidor Virtual Center
- Nombre de usuario y contraseña de sólo lectura en Virtual Center
- Privilegios de sólo lectura en todos los objetos del Centro virtual.
- Acceso SDK en el servidor Virtual Center
- Requisitos del puerto: http-80 https-443
- Valide el acceso iniciando sesión en Virtual Center Client con su nombre de usuario y contraseña y verificando que el SDK está activado introduciendo `telnet <vc_ip> 443`.

## Configuración

| Campo                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descripción                                                                                                                                                                               |
| Dirección del centro virtual                                                                                                                                                              |
| Dirección de red para el servidor de Virtual Center o vSphere, especificada como una dirección IP ( <i>nnn.nnn.nnn.nnn</i> ) o como un nombre de host que se puede resolver mediante DNS. |
| Nombre de usuario                                                                                                                                                                         |
| Nombre de usuario del servidor VMware.                                                                                                                                                    |
| Contraseña                                                                                                                                                                                |
| Contraseña del servidor VMware.                                                                                                                                                           |

## Configuración avanzada

| Campo                                                  | Descripción                                                                                             |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Intervalo de sondeo de inventario (mín.)               | Intervalo entre sondeos de inventario (predeterminado 20 minutos)                                       |
| Tiempo de espera de conexión (ms)                      | Tiempo de espera de conexión (60000 ms predeterminado)                                                  |
| Filtrar las máquinas virtuales por                     | Elija cómo filtrar máquinas virtuales                                                                   |
| Elija "excluir" o "incluir" para especificar una lista | Especifique si desea incluir o excluir la lista de máquinas virtuales a continuación al recopilar datos |

|                                                                                                                              |                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Lista de máquinas virtuales que se van a filtrar (separadas por comas o por punto y coma si se utiliza una coma en el valor) | Lista de máquinas virtuales separadas por comas o mediante punto y coma para incluir o excluir del sondeo |
| Número de reintentos para solicitudes a vCenter                                                                              | Número de intentos de reintento de solicitud de vCenter                                                   |
| Puerto de comunicación                                                                                                       | Puerto que se utiliza para el servidor de VMware                                                          |
| Intervalo de sondeo de rendimiento (s)                                                                                       | Intervalo entre sondeos de rendimiento (predeterminado 300 segundos)                                      |

## Cambio de las credenciales de origen de datos

Si varias fuentes de datos del mismo tipo comparten un nombre de usuario y una contraseña, puede cambiar la contraseña de todos los dispositivos del grupo al mismo tiempo.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.


Se abrirá la lista **orígenes de datos**.

2. Haga clic en el botón **acciones** y seleccione la opción **Cambiar credenciales**.
3. En el cuadro de diálogo Credentials Management, seleccione uno de los grupos de orígenes de datos en la lista.

El icono Editar, un bolígrafo en una hoja de papel, se activa a la derecha.

## Credentials Management

Below is a list of groups of data sources with the same credentials. You can change the credentials of the entire group in a single action by pressing the edit button next to the desired group.

| Data source type                                 | Package            | User/Community | Used by                          |                                                                                    |
|--------------------------------------------------|--------------------|----------------|----------------------------------|------------------------------------------------------------------------------------|
| FC Switch Firmware 2.0+ (SNMP)                   | foundation         | UHTSAN         | elr1scvblkodd01 and 1 others     |                                                                                    |
| FC Switch Firmware 4.2+ (SSH)                    | foundation         | ssacct         | ELR5_EvenFabric and 1 others     |  |
| FC Switch Firmware 4.2+ (SSH)                    | performance        | UHTSAN         | ELR5_EvenFabric                  |                                                                                    |
| HiCommand Device Manager                         | foundation         | sanscm         | ELR5_APSWP1008_HCS7 and 1 others |                                                                                    |
| Solutions Enabler (CLI) with Performance (SMT-S) | storageperformance | admin          | ELR1_Vblock EMC                  |                                                                                    |

Showing 1 to 5 of 5 entries

4. Haga clic en **Editar**.

5. Introduzca la nueva contraseña y confírmela.

## Cambios que causan problemas de recopilación de datos

Si tiene problemas de recopilación de datos en OnCommand Insight, los cambios en el entorno son una causa probable. Como regla general de mantenimiento, también debe adaptarse a los cambios que se produzcan en su entorno en Insight.

Puede utilizar esta lista de comprobación para identificar los cambios en la red que puedan causar problemas:

- ¿Ha cambiado alguna contraseña? ¿Se han cambiado esas contraseñas en Insight?
- ¿Ha eliminado un dispositivo de la red? También debe eliminar el dispositivo de OnCommand Insight para evitar que se vuelva a detectar y volver a introducir.
- ¿Actualizó software de infraestructura (como HP CommandView EVA o EMC Solutions facilitadora)?

Asegúrese de que las versiones apropiadas de las herramientas cliente están instaladas en la unidad de adquisición. Si persisten los fallos en el origen de datos, debe ponerse en contacto con el servicio de asistencia técnica para solicitar asistencia y, posiblemente, con un parche en el origen de datos.

- ¿Utilizan todas sus unidades de adquisición de OnCommand Insight la misma versión de OnCommand Insight? Si las unidades de adquisición remota y la unidad de adquisición local ejecutan diferentes versiones de OnCommand Insight, instale la misma versión en todas las unidades para corregir el problema de recopilación de datos.

Si necesita instalar una nueva versión de OnCommand Insight en todas las unidades de adquisición, vaya

al sitio de soporte y descargue la versión correcta.

- ¿Ha cambiado algún nombre de dominio o agregado otro? Debe actualizar los métodos de resolución del dispositivo (anteriormente resolución automática).

## Examinar en detalle un origen de datos

Si observa que un origen de datos ha fallado o se ha ralentizado, es posible que desee examinar un resumen detallado de la información de ese origen de datos para determinar la causa del problema. Las fuentes de datos con condiciones que requieren su atención están marcadas con un círculo rojo sólido.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

Se abrirá la lista **orígenes de datos**. Cualquier origen de datos enumerado con problemas potenciales se marca con un círculo rojo sólido. Los problemas más graves están en la parte superior de la lista.

2. Seleccione el origen de datos que causa preocupación.
3. Haga clic en el enlace del nombre del origen de datos.
4. En la página de resumen del origen de datos, compruebe la información de cualquiera de estas secciones:

- **Escala de tiempo del evento**

Enumera los eventos vinculados al estado actual que se muestra en la lista orígenes de datos. Los eventos de este resumen se muestran por dispositivo. Los errores se muestran en rojo. Puede colocar el puntero del ratón sobre los elementos de la línea de tiempo para mostrar información adicional.

- **Dispositivos notificados por esta fuente de datos**

Enumera los tipos de dispositivos, sus direcciones IP y vínculos a información más detallada para cada dispositivo.

- **Cambios reportados por esta fuente de datos (últimas 3 semanas)**

Muestra los dispositivos que se han agregado o eliminado o que han cambiado la configuración.

5. Después de examinar la información del origen de datos, es posible que desee realizar una de estas operaciones utilizando los botones de la parte superior de la página:

- **Editar** la descripción del origen de datos para corregir el problema.
- **Encuesta de nuevo** obliga a la encuesta a revelar si el problema era persistente o intermitente.
- **Posponer** sondeo de fuente de datos durante 3, 7 o 30 días para darle tiempo para investigar el problema y detener los mensajes de advertencia.
- **Instale un parche** en el origen de datos para corregir el problema.
- Preparar un **informe de errores** para asistencia técnica.
- **Eliminar** el origen de datos de su entorno de supervisión de Insight.

## Investigar una fuente de datos fallida

Si un origen de datos tiene el mensaje "**Inventory failed !**" o "**Performance failed !**" y un impacto alto o medio, debe investigar este problema utilizando la página de resumen del origen de datos con su información vinculada.

### Pasos

1. Haga clic en el **Nombre** vinculado del origen de datos para abrir la página Resumen.
2. En la página Resumen, compruebe el área **Comentarios** para leer las notas que dejó otro ingeniero que también podría estar investigando este error.
3. Anote cualquier mensaje de rendimiento.
4. Si se está aplicando un parche a este origen de datos, haga clic en link para comprobar la página **parche** para ver si esto ha causado el problema.
5. Mueva el puntero del ratón sobre los segmentos del gráfico **escala de tiempo del evento** para ver información adicional.
6. Seleccione un mensaje de error para un dispositivo y se mostrará debajo de la línea de tiempo del evento y haga clic en el icono **Detalles de error** que aparece a la derecha del mensaje.

Los detalles del error incluyen el texto del mensaje de error, las causas más probables, la información en uso, y sugerencias de lo que se puede intentar corregir el problema.

7. En el área dispositivos que informa este origen de datos, puede filtrar la lista para mostrar sólo los dispositivos de interés y puede hacer clic en el **Nombre** enlazado de un dispositivo para mostrar la *página* del recurso correspondiente a ese dispositivo.
8. Para volver a las páginas mostradas anteriormente, utilice una de estas técnicas:
  - Haga clic en la flecha hacia atrás del explorador.
  - Haga clic con el botón secundario del ratón en la flecha de retroceso para mostrar una lista de las páginas y seleccione la página que desee.
9. Para mostrar información detallada sobre otros recursos, haga clic en otros nombres vinculados.
10. Cuando vuelva a la página de resumen del origen de datos, compruebe el área **Changes** en la parte inferior de la página para ver si los cambios recientes causaron el problema.

## Controlando el sondeo del origen de datos

Después de realizar un cambio en un origen de datos, es posible que desee sondear inmediatamente para comprobar sus cambios, o puede que desee posponer la recopilación de datos en un origen de datos durante uno, tres o cinco días mientras trabaja en un problema.

### Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Seleccione el origen de datos para el que desea controlar el sondeo.
3. Haga clic en el enlace del nombre del origen de datos.
4. En la página de resumen del origen de datos, compruebe la información y haga clic en una de estas dos opciones de sondeo:

- **Encuesta de nuevo** para obligar al origen de datos a recopilar datos inmediatamente.
- **Posponer** y seleccionar la duración del retraso de sondeo de 3, 7 o 30 días.

## Después de terminar

Si pospuso la recopilación de datos en un origen de datos y desea reiniciar la colección, haga clic en **Reanudar** en la página de resumen.

## Edición de la información del origen de datos

Puede editar rápidamente la información de configuración del origen de datos.

### Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Localice el origen de datos que desea editar.
3. Utilice uno de estos métodos para iniciar los cambios:
  - Haga clic en **Editar origen de datos** a la derecha del origen de datos seleccionado.
  - Haga clic en el nombre vinculado del origen de datos seleccionado y haga clic en **Editar**. Cualquier método abre el cuadro de diálogo Editar origen de datos.
4. Realice los cambios que desee y haga clic en **Guardar**.

## Edición de información para varios orígenes de datos

Puede editar la mayoría de la información de varias fuentes de datos del mismo proveedor y modelo a la vez. Por ejemplo, si estos orígenes de datos comparten un nombre de usuario y una contraseña, puede cambiar la contraseña en un lugar y, por tanto, actualizar la contraseña para todos los orígenes de datos seleccionados.

### Acerca de esta tarea

Las opciones que no puede editar para los orígenes de datos seleccionados aparecen atenuadas o no se muestran en el cuadro de diálogo Editar origen de datos. Además, cuando una opción muestra un valor de **Mixed**, indica que el valor de la opción varía entre los orígenes de datos seleccionados. Por ejemplo, si la opción **tiempo de espera (seg)** para dos orígenes de datos seleccionados es **mixta**, un origen de datos podría tener un valor de tiempo de espera de 60 y el otro podría tener un valor de 90; por lo tanto, si cambia este valor a 120 y guarda los cambios en los orígenes de datos, la configuración de tiempo de espera para ambos orígenes de datos pasa a ser 120.

### Pasos

1. Haga clic en **Admin** y desplácese a la vista de lista de orígenes de datos
2. Seleccione los orígenes de datos que desea modificar. Los orígenes de datos seleccionados deben pertenecer al mismo proveedor, modelo y unidad de adquisición.
3. Haga clic en el botón **acciones** y seleccione la opción **Editar**.
4. En el cuadro de diálogo de edición, cambie cualquiera de los **Ajustes** según sea necesario.
5. Haga clic en el enlace **Configuración** para cambiar cualquiera de las opciones básicas de los orígenes de datos.

6. Haga clic en el vínculo **Configuración avanzada** para cambiar cualquiera de las opciones avanzadas de los orígenes de datos.
7. Haga clic en **Guardar**.

## Asignación de etiquetas de origen de datos a anotaciones

Cuando un origen de datos está configurado para sondear datos de etiquetas, Insight establece automáticamente valores de anotación para una anotación de Insight existente con el mismo nombre que una etiqueta.

Cuando existe la anotación Insight antes de activar las etiquetas en el origen de datos, los datos de la etiqueta del origen de datos se agregan automáticamente a la anotación Insight.

Cuando se crea una anotación después de activar la etiqueta, el sondeo inicial del origen de datos no actualiza automáticamente la anotación. Hay un retraso en el tiempo que se tarda en reemplazar o rellenar la anotación de Insight. Para evitar el retraso, puede forzar la actualización de la etiqueta posponiendo y, a continuación, reanudando el origen de datos.

## Eliminar un origen de datos

Si ha eliminado un origen de datos del entorno, también debe eliminarlo del entorno de supervisión de OnCommand Insight.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.

Se abrirá la lista orígenes de datos.

2. Seleccione el origen de datos que desea eliminar.
3. Haga clic en el nombre del origen de datos vinculado.
4. Compruebe la información del origen de datos seleccionado en la página de resumen para asegurarse de que es el que desea eliminar.
5. Haga clic en **Eliminar**.
6. Haga clic en **Aceptar** para confirmar la operación.

## Qué son los parches de origen de datos

Los parches del origen de los datos solucionan problemas con los parches existentes y permiten añadir fácilmente nuevos tipos de orígenes de datos (proveedores y modelos). Para cada tipo de origen de datos de la red, puede cargar parches de origen de datos. También puede instalar, probar y administrar el proceso de parches. Sin embargo, solo se puede activar un parche para un tipo de origen de datos a la vez.

Para cada parche, puede realizar estas tareas:

- Compruebe la comparación antes y después de cada origen de datos que recibe el parche.
- Escribir comentarios para explicar las decisiones o resumir la investigación.



- Realice cambios en un origen de datos que no responde correctamente al parche.
- Apruebe el parche que se va a asignar a su servidor de Insight.
- Retrocede un parche que no esté funcionando como se pretendía.
- Reemplace un parche que falla por uno diferente.

## Aplicación de un parche de origen de datos

Los parches de origen de datos están disponibles periódicamente y le permiten solucionar problemas con un origen de datos existente, añadir un origen de datos a un nuevo proveedor o añadir un nuevo modelo a un proveedor.

### Antes de empezar

Debe haber obtenido la `.zip` archivo que contiene el último origen de datos `.patch` archivos del soporte técnico.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para buscar `.patch` archivo.
5. Inspeccione los tipos de fuente de datos **Patch name**, **Description** y **impactados**.
6. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

Si está aplicando un parche que soluciona problemas con un origen de datos, todos los orígenes de datos del mismo tipo se actualizan con el parche y debe aprobar el parche. Los parches que no afectan a ningún origen de datos configurado se aprueban automáticamente.

### Después de terminar

Si está aplicando un parche que agrega un origen de datos para un nuevo proveedor o un nuevo modelo, debe agregar el origen de datos después de aplicar el parche.

## Instalar un parche en un tipo de origen de datos

Después de cargar un parche de origen de datos, puede instalarlo en todos los orígenes de datos del mismo tipo.

### Antes de empezar

Debe haber cargado un archivo de revisión que desee instalar en un tipo de origen de datos.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para localizar el archivo de parche cargado.
5. Compruebe los tipos de fuente de datos , \* **Descripción** y **impactados** de **Patch NAME**.
6. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

Con esta revisión se actualizan todos los orígenes de datos del mismo tipo.

## Gestión de parches

Puede revisar el estado actual de todos los parches de origen de datos que se aplican a la red. Si desea realizar una acción en un parche, puede hacer clic en el nombre vinculado en los parches que se encuentran actualmente en la tabla de revisión.

### Antes de empezar

Debe haber cargado y estar instalando al menos un parche.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

Si no se está instalando ningún parche, la tabla de parches actualmente en revisión está vacía.

3. En **parches actualmente en revisión**, compruebe el estado de los parches del origen de datos que se están aplicando actualmente.
4. Para examinar los detalles asociados a una revisión específica, haga clic en el nombre vinculado de la revisión.
5. Para el parche seleccionado, puede hacer clic en cualquiera de estas opciones para realizar la siguiente acción en el parche:
  - **Aprobar parche** confirma el parche con los orígenes de datos.
  - **Revertir** elimina el parche.
  - **Sustituir parche** le permite seleccionar un parche diferente para esos orígenes de datos.

## Se está cometiendo un parche de origen de datos

La información del resumen parches se utiliza para decidir si el parche se está realizando según lo esperado y, a continuación, se debe confirmar en la red.

### Antes de empezar

Ha instalado un parche y debe decidir si el parche se ha realizado correctamente y se debe aprobar.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.

Si no se está instalando ningún parche, los parches que se están revisando están vacíos.

3. En **parches actualmente en revisión**, compruebe el estado de los parches del origen de datos que se están aplicando actualmente.
4. Para examinar los detalles asociados a una revisión específica, haga clic en el nombre vinculado de la revisión.
5. En la información resumida de Patches, que se muestra en este ejemplo, compruebe **Recomendación** y **Comentarios** para evaluar el progreso del parche.

The screenshot shows the 'Patches' section for 'Brocade SSH'. It includes a 'Summary' box with a green 'Approve' button, a red 'Roll back' button, and a grey 'Replace patch' button. Below the summary is a table titled 'affected data sources' with columns: Name, Ali, Type, Conclusion, Status before patch applied, and Most recent status. The table lists five data sources (ds0 to ds4) with their respective statuses.

| Name | Ali   | Type         | Conclusion                                                   | Status before patch applied | Most recent status   |
|------|-------|--------------|--------------------------------------------------------------|-----------------------------|----------------------|
| ds0  | local | Brocade CLI  | ✓                                                            | All successful              | Currently polling... |
| ds1  | local | Brocade CLI  | No change (success)                                          | All successful              | All successful       |
| ds2  | local | Brocade CLI  | ● Polling is now successful                                  | Configuration failed        | All successful       |
| ds3  | local | Brocade CLI  | ● Configuration is still failing (a different error)         | Configuration failed        | Configuration failed |
| ds4  | au1   | Brocade SNMP | ● Configuration is successful but now Performance is failing | Configuration failed        | Performance failed   |

6. Consulte la tabla **orígenes de datos afectados** para ver el estado de cada origen de datos afectado antes y después del parche.

Si le preocupa que haya un problema con uno de los orígenes de datos que se van a aplicar parches, haga clic en el nombre vinculado en la tabla orígenes de datos afectados.

7. Si concluye que el parche debe aplicarse a ese tipo de origen de datos, haga clic en **aprobar**.

Los orígenes de datos se modifican y el parche se elimina de los parches actualmente en revisión.

## Revertir una revisión de origen de datos

Si un parche de origen de datos no funciona de la forma esperada, puede retroceder. La reversión de un parche lo elimina y restaura la versión anterior tal como era antes de aplicar este parche.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En **parches actualmente en revisión**, haga clic en el nombre vinculado del parche que parece no tener éxito.
4. En la página parches del origen de datos, examine esta información:

- **Resumen** describe cuándo se aplicó el parche, los orígenes de datos afectados y los comentarios sobre el parche de usted u otros miembros de su equipo.
  - **Orígenes de datos afectados** enumera todos los orígenes de datos que se están parchando e incluye una comparación del estado antes y después de la aplicación de parches.
5. Para mostrar los detalles de un origen de datos que no esté procesando correctamente el parche, haga clic en el archivo vinculado **Nombre**.
    - a. Compruebe la información de resumen.
    - b. Compruebe **escala de tiempo de evento** para ver cualquier dato de configuración o rendimiento que pueda afectar a este origen de datos.
  6. Si concluye que el parche no va a ser correcto, haga clic en la flecha de retroceso del explorador para volver a la página de resumen parches.
  7. Haga clic en **Volver** para eliminar ese parche.

Si conoce un parche diferente que es más probable que tenga éxito, haga clic en **sustituir parche** y cargue el nuevo parche.

## Resolución del dispositivo

Debe descubrir todos los dispositivos que desea supervisar con OnCommand Insight. La identificación es necesaria para realizar un seguimiento preciso del rendimiento y del inventario en su entorno. Normalmente, la mayoría de los dispositivos de su entorno se detectan mediante la resolución automática del dispositivo.



Si está realizando una actualización y tiene reglas de resolución automática inactivas en el sistema desde el que está actualizando, estas reglas se eliminarán durante la actualización. Para conservar las reglas de resolución automática inactivas, active las reglas (marque la casilla) antes de realizar la actualización.

Después de instalar y configurar orígenes de datos, se identifican los dispositivos en el entorno, incluidos los switches, las cabinas de almacenamiento y la infraestructura virtual de hipervisores y las máquinas virtuales. Sin embargo, normalmente esto no identifica el 100% de los dispositivos de su entorno.

Una vez configurados los dispositivos de tipo de origen de datos, la mejor práctica consiste en aprovechar las reglas de resolución de dispositivos para ayudar a identificar los dispositivos desconocidos restantes del entorno. La resolución del dispositivo puede ayudarle a resolver dispositivos desconocidos como los siguientes tipos de dispositivos:

- hosts físicos
- cabinas de almacenamiento
- cintas
- interruptores

Los dispositivos que quedan como "unknown" tras la resolución del dispositivo se consideran dispositivos genéricos, que también se pueden mostrar en consultas y en paneles de control.

Las reglas creadas a su vez identificarán automáticamente nuevos dispositivos con atributos similares a los que se agregan a su entorno. En algunos casos, la resolución del dispositivo también permite la identificación manual evitando las reglas de resolución del dispositivo para dispositivos no detectados dentro de Insight.

La identificación incompleta de los dispositivos puede dar lugar a problemas como:

- Rutas incompletas
- Conexiones multivía no identificadas
- Incapacidad para agrupar aplicaciones
- Vistas de topología inexactas
- Datos inexactos en el almacén de datos y la generación de informes

La función resolución de dispositivos (**Administrar > resolución de dispositivos**) incluye las siguientes fichas, cada una de las cuales desempeña un papel en la planificación y visualización de la resolución de dispositivos:

- "FC Identify" contiene una lista WWN e información de puertos de dispositivos Fibre Channel que no se resolvieron mediante la resolución automática de dispositivos. La ficha también identifica el porcentaje de dispositivos que se han identificado.
- «Identificación IP» contiene una lista de dispositivos que acceden a recursos compartidos CIFS y recursos compartidos NFS que no se identificaron mediante la resolución automática del dispositivo. La ficha también identifica el porcentaje de dispositivos que se han identificado.
- "Reglas de resolución automática" contiene la lista de reglas que se ejecutan al realizar la resolución de dispositivos Fibre Channel. Se trata de reglas que se crean para resolver dispositivos Fibre Channel no identificados.
- "Preferencias" proporciona opciones de configuración que se utilizan para personalizar la resolución del dispositivo en su entorno.

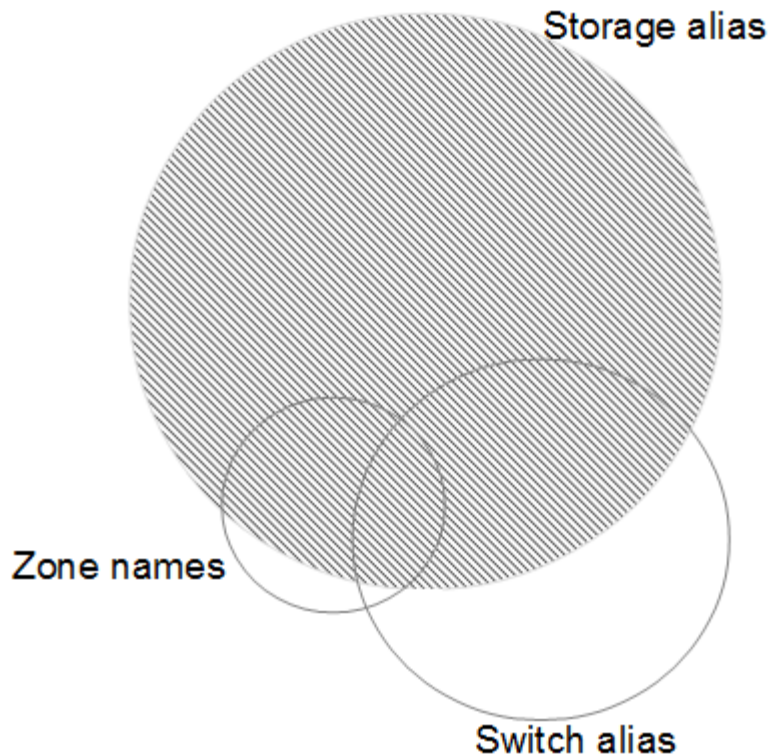
## Antes de empezar

Debe saber cómo se configura el entorno antes de definir las reglas para identificar dispositivos. Cuanto más conozca su entorno, más fácil será identificar los dispositivos.

Debe responder a preguntas similares a las siguientes para ayudarle a crear reglas precisas:

- ¿Su entorno tiene estándares de nomenclatura para las zonas o hosts y qué porcentaje de estos son precisos?
- ¿El entorno usa un alias del switch o un alias de almacenamiento y coincide con el nombre del host?
- ¿Su entorno utiliza una herramienta SRM y puede utilizarla para identificar los nombres de host? ¿Qué cobertura ofrece el SRM?
- ¿Con qué frecuencia cambian los esquemas de nomenclatura en su entorno?
- ¿Ha habido alguna adquisición o fusión que haya introducido diferentes esquemas de nomenclatura?

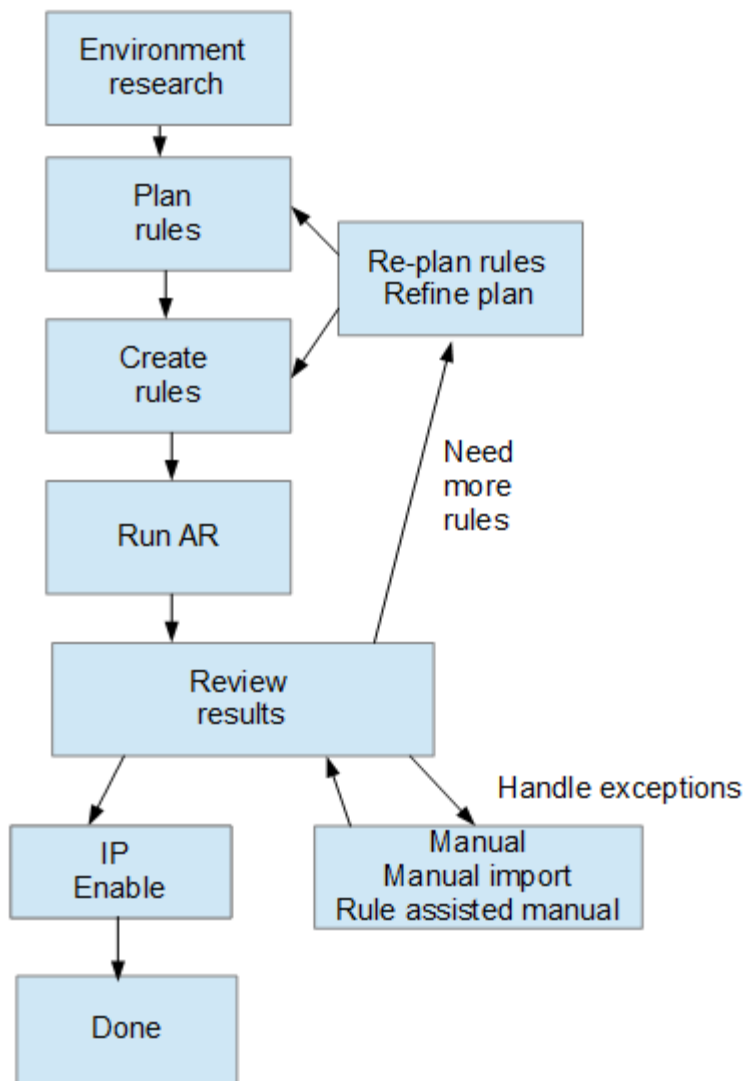
Después de analizar su entorno, debe ser capaz de identificar qué estándares de nomenclatura existen que puede esperar encontrar fiabilidad. La información recopilada puede representarse gráficamente en una figura similar a la siguiente:



En este ejemplo, el mayor número de dispositivos está representado de forma fiable por alias de almacenamiento. Las reglas que identifican hosts que usan alias de almacenamiento deben escribirse primero, las reglas que usan alias de switch deben escribirse Next y las últimas reglas creadas deben usar alias de zona. Debido a la superposición del uso de alias de zona y alias de switch, algunas reglas de alias de almacenamiento pueden identificar dispositivos adicionales, dejando menos reglas necesarias para los alias de zona y los alias de cambio.

### **Pasos para definir dispositivos en el entorno**

Por lo general, use un flujo de trabajo similar al siguiente para identificar los dispositivos en su entorno. La identificación es un proceso iterativo y podría requerir múltiples pasos de reglas de planificación y refinación.



Si dispone de dispositivos no identificados (conocidos como "desconocidos" o genéricos) en su entorno y, a continuación, configura un origen de datos que identifica dichos dispositivos tras el sondeo, ya no se mostrarán ni contarán como dispositivos genéricos.

## Planificación de reglas de resolución de dispositivos para su entorno

El uso de reglas para identificar dispositivos en su entorno suele ser un proceso iterativo que requiere un análisis exhaustivo de su entorno y la creación de múltiples reglas para identificar el mayor número posible de dispositivos. La mejor de los casos consiste en establecer un objetivo para identificar el 100% de los dispositivos de su entorno.

El orden más eficiente para las reglas es colocar primero las reglas más restrictivas, lo que resulta en la mayoría de las inscripciones no en coincidencia de patrones, con el procedimiento que se lleva a cabo para reglas menos restrictivas. Esto permite a Insight aplicar más patrones a cada entrada, lo que aumenta la posibilidad de que los patrones coincidan y de que la identificación de host sea positiva.

Cuando cree reglas, su objetivo debería ser crear reglas que aborden el mayor número posible de dispositivos no identificados. Por ejemplo, crear reglas que siguen un patrón de cobertura similar al siguiente es mucho más eficiente que crear 30 reglas con porcentajes inferiores de cobertura:

| Regla      | Porcentaje de cobertura |
|------------|-------------------------|
| Artículo 1 | 60 %                    |
| Artículo 2 | 25 %                    |
| Artículo 3 | 8 %                     |
| Artículo 4 | 4 %                     |
| Artículo 5 | 1%                      |

## Creación de reglas de resolución de dispositivos

Se crean reglas de resolución de dispositivos para identificar los hosts, el almacenamiento y las cintas que OnCommand Insight no identifica automáticamente actualmente. Las reglas que crea identifican dispositivos actualmente en su entorno y también identifican dispositivos similares a medida que se agregan a su entorno.

### Acerca de esta tarea

Al crear reglas que se inician identificando el origen de la información con el que se ejecuta la regla, el método utilizado para extraer información y si se aplica la búsqueda DNS a los resultados de la regla.

|                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fuente que se utiliza para identificar el dispositivo                                                                                                                                                                                                                                                                 |
| <ul style="list-style-type: none"> <li>• Alias de SRM para hosts</li> <li>• Alias de almacenamiento que contiene un nombre de host o cinta incorporado</li> <li>• Cambie el alias que contiene un nombre de host o cinta incorporado</li> <li>• Nombres de zona que contienen un nombre de host incrustado</li> </ul> |
| Método que se utiliza para extraer el nombre del dispositivo del origen                                                                                                                                                                                                                                               |
| <ul style="list-style-type: none"> <li>• Tal cual (extraer un nombre de un SRM)</li> <li>• Delimitadores</li> <li>• Expresiones regulares</li> </ul>                                                                                                                                                                  |
| Búsqueda de DNS                                                                                                                                                                                                                                                                                                       |
| Especifica si utiliza DNS para verificar el nombre de host.                                                                                                                                                                                                                                                           |

Las reglas se crean en la ficha Reglas de resolución automática. Los siguientes pasos describen el proceso de creación de reglas.



## Pasos

1. Haga clic en **Administrar > resolución del dispositivo**
2. En la ficha **Reglas de resolución automática**, haga clic en **+Agregar**

Aparecerá la pantalla Nueva regla.



La pantalla Nueva regla incluye un icono **?**, que proporciona ayuda y ejemplos para crear expresiones regulares.

3. En la lista **Tipo**, seleccione el dispositivo que desea identificar.

Puede seleccionar Host o cinta.

4. En la lista **Fuente**, seleccione la fuente que desea utilizar para identificar el host.

En función del origen que haya elegido, Insight muestra la siguiente respuesta:

- Las zonas enumeran las zonas y el WWN que debe identificar Insight.
- SRM enumera los alias no identificados que Insight debe identificar
- El alias de almacenamiento enumera los alias de almacenamiento y un WWN que Insight debe identificar
- El alias de switch enumera los alias de switch que Insight debe identificar

5. En la lista **método**, seleccione el método que desea utilizar para identificar el host.

| Origen                  | Método                                               |
|-------------------------|------------------------------------------------------|
| SRM                     | «'tal cual», «delimitados», «expresiones regulares»» |
| Alias de almacenamiento | «Deelitadores» o «expresiones regulares»             |
| Cambiar alias           | «Deelitadores» o «expresiones regulares»             |
| Zonas                   | «Deelitadores» o «expresiones regulares»             |

- Las reglas que usan "demiters" requieren los delimitadores y la longitud mínima del nombre del host.

La longitud mínima del nombre de host es el número de caracteres que Insight debe utilizar para identificar un host. Insight realiza búsquedas de DNS solo para nombres de host que sean largos o prolongados.


Para las reglas que utilizan delimitadores, el delimitador tokeniza la cadena de entrada y se crea una lista de candidatos de nombre de host mediante varias combinaciones del token adyacente. La lista se ordena entonces, de mayor a menor tamaño. Por ejemplo, para vipsnq03\_hba3\_emc3\_12ep0 la lista daría como resultado lo siguiente:

- vipsnq03\_hba3\_emc3\_12ep0
- vipsnq03\_hba3\_emc3

- hba3 emc3\_12ep0
- vipsnq03\_hba3
- emc3\_12ep0
- hba3\_emc3
- vipsq03
- 12p0
- emc3
- hab.3

- Las normas que utilicen «"expresión regular" requieren una expresión regular, el formato y la selección de la sensibilidad de los casos.

6.

Haga clic en  Para ejecutar todas las reglas, o bien haga clic en la flecha abajo del botón para ejecutar la regla que creó (y cualquier otra regla que se haya creado desde la última ejecución completa de AR).

## Resultados

Los resultados de la ejecución de reglas se muestran en la ficha Identificación FC.

## Inicio de una actualización automática de resolución del dispositivo

Una actualización de resolución de dispositivo confirma los cambios manuales que se han agregado desde la última ejecución automática de resolución de dispositivo completa. La ejecución de una actualización se puede utilizar para confirmar y ejecutar sólo las nuevas entradas manuales realizadas en la configuración de resolución del dispositivo. No se ejecuta ninguna resolución completa del dispositivo.

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. En la pantalla **resolución del dispositivo**, haga clic en la flecha hacia abajo del botón **Ejecutar AR**.
4. Haga clic en **Actualizar** para iniciar la actualización.

## Identificación manual asistida por reglas

Esta función se utiliza en casos especiales en los que desea ejecutar una regla específica o una lista de reglas (con o sin una reordenación puntual) para resolver hosts, dispositivos de almacenamiento y cinta desconocidos o grupos de ellas.

## Antes de empezar

Tiene varios dispositivos que no se han identificado y también varias reglas que han identificado correctamente otros dispositivos.

Acerca de esta tarea



Si el origen sólo contiene parte del nombre de un host o dispositivo, utilice una regla de expresión regular y dé formato para agregar el texto que falta.

Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Haga clic en la ficha **FC Identify**.

El sistema muestra los dispositivos identificados y no identificados.

4. Seleccione varios dispositivos no identificados.
5. Haga clic en **Identify > Set host resolution** o **> Set Tape resolution**

El sistema muestra la pantalla de identificación que contiene una lista de todas las reglas que han identificado correctamente los dispositivos.

6. Cambie el orden de las reglas por un orden que satisfaga sus necesidades.

El orden de las reglas se cambia en la pantalla de identificación, pero no se cambian globalmente.

7. Seleccione el método que se ajuste a sus necesidades.

OnCommand Insight ejecuta el proceso de resolución del host en el orden en que se muestran los métodos, comenzando por los que se encuentran en la parte superior.

Cuando se encuentran las reglas que se aplican, los nombres de reglas se muestran en la columna rules y se identifican como manuales.

Resolución de dispositivos Fibre Channel

La pantalla FC Identify muestra el WWN y el WWPN de dispositivos Fibre Channel cuyos hosts no se han identificado mediante la resolución automática del dispositivo. La pantalla también muestra cualquier dispositivo que se haya resuelto mediante la resolución manual del dispositivo.

Los dispositivos que se han resuelto mediante resolución manual contienen el estado "OK" e identifican la regla utilizada para identificar el dispositivo. Los dispositivos que faltan tienen el estado "no identificados". En esta página se muestra la cobertura total para la identificación de dispositivos.

+Add

Total coverage  
30% (3/10)

FC identify (10)

Identify

Unidentify

filter...

↑

↓

| <div><div>☐</div></div> | WWN                     | Port WWN                | IP      | Name          | Type    | Status       | Rule          |  |
|-------------------------|-------------------------|-------------------------|---------|---------------|---------|--------------|---------------|--|
| <div><div>☐</div></div> | 30:E0:00:00:00:00:00:00 | 10:B0:00:00:00:00:28:20 | 1.1.1.1 | ResolvedHost1 | Host    | OK           | Hosts by zone |  |
| <div><div>☐</div></div> | 30:E0:00:00:00:00:00:02 | 10:B0:00:00:00:00:28:22 | 2.2.2.2 | ResolvedHost2 | Host    | OK           | Rule deleted  |  |
| <div><div>☐</div></div> | 30:E0:00:00:00:00:00:03 | 10:B0:00:00:00:00:28:23 |         |               | Unknown | Unidentified |               |  |
| <div><div>☐</div></div> | 30:E0:00:00:00:00:00:04 | 10:B0:00:00:00:00:28:24 |         |               | Unknown | Unidentified |               |  |
| <div><div>☐</div></div> | 30:E0:00:00:00:00:00:05 | 10:B0:00:00:00:00:28:25 |         |               | Unknown | Unidentified |               |  |

Showing 1 to 5 of 10 entries

<

1

2

>

Para realizar acciones masivas, seleccione varios dispositivos en el lado izquierdo de la pantalla FC Identify. Las acciones se pueden realizar en un único dispositivo pasando el ratón por encima de un dispositivo y seleccionando los botones identificar o anular la identificación en el extremo derecho de la lista.

El enlace cobertura total muestra una lista del "número de dispositivos identificados/número de dispositivos disponibles" para su configuración:

- Alias de SRM
- Alias de almacenamiento
- Cambiar alias
- Zonas
- Definido por el usuario

### Adición manual de un dispositivo Fibre Channel

Puede agregar manualmente un dispositivo Fibre Channel a OnCommand Insight mediante la función de adición manual disponible en la ficha Identificación de FC de resolución de dispositivo. Este proceso se puede utilizar para la preidentificación de un dispositivo que se espera descubrir en el futuro.

#### Antes de empezar

Para agregar correctamente una identificación de dispositivo al sistema, debe conocer la dirección WWN o IP y el nombre del dispositivo.

#### Acerca de esta tarea

Puede agregar manualmente un dispositivo Host, almacenamiento, cinta o Fibre Channel desconocido.

#### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight
2. Haga clic en **Administrar > resolución del dispositivo**
3. Haga clic en la ficha **FC Identify**.
4. Haga clic en el botón Agregar.

Aparecerá el cuadro de diálogo Agregar dispositivo

5. Introduzca el WWN o la dirección IP, el nombre del dispositivo y seleccione el tipo de dispositivo.

#### Resultados

El dispositivo que introduzca se añadirá a la lista de dispositivos de la pestaña FC Identify. La «Regla» se identifica como Manual.

### Importe la identificación de dispositivo Fibre Channel desde un archivo CSV

Puede importar manualmente la identificación de dispositivos Fibre Channel a la función resolución de dispositivos OnCommand Insight mediante una lista de dispositivos de un archivo CSV.

## Antes de empezar

Debe tener un archivo CSV formateado correctamente para importar identificaciones de dispositivos directamente a la función resolución de dispositivos. El archivo CSV para dispositivos Fibre Channel requiere la siguiente información:

|        |
|--------|
| WWN    |
| IP     |
| Nombre |
| Tipo   |



Como práctica recomendada, en primer lugar se recomienda exportar la información de identificación de FC a un archivo CSV, hacer los cambios que desee en ese archivo y, a continuación, importar el archivo de nuevo a FC Identify. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Para importar información sobre FC Identify:

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Seleccione la ficha **FC Identify**.
4. Haga clic en **identificar > identificar desde archivo**.

- a. Desplácese hasta la carpeta que contiene los archivos CSV para importar y seleccione el archivo deseado.

Los dispositivos introducidos se agregan a la lista de dispositivos de la pestaña FC Identify. La «Regla» se identifica como «manual».

## Exportación de identificaciones de dispositivos Fibre Channel a un archivo CSV

Puede exportar identificaciones de dispositivos Fibre Channel existentes a un archivo CSV desde la característica de resolución de dispositivos OnCommand Insight. Es posible que desee exportar una identificación de dispositivo para poder modificarla y, a continuación, volver a importarla en Insight, donde se utilizará para identificar dispositivos similares a los que originalmente coinciden con la identificación exportada.


### Acerca de esta tarea

Este escenario se puede utilizar cuando los dispositivos tienen atributos similares que se pueden editar fácilmente en el archivo CSV y luego volver a importar al sistema.

Al exportar una identificación de dispositivo Fibre Channel a un archivo CSV, el archivo contiene la siguiente información en el orden que se muestra:

|        |
|--------|
| WWN    |
| IP     |
| Nombre |
| Tipo   |

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Seleccione la ficha **FC Identify**.
4. Seleccione el dispositivo Fibre Channel o los dispositivos cuya identificación desea exportar.
5. Haga clic en la exportación  .
6. Elija si desea abrir el archivo CSV o guardar el archivo.

## Resolución del dispositivo IP

La pantalla de identificación IP muestra todos los recursos compartidos iSCSI y CIFS o NFS que se han identificado mediante la resolución automática del dispositivo o mediante la resolución manual del mismo. También se muestran dispositivos no identificados. La pantalla incluye la dirección IP, el nombre, el estado, el nodo iSCSI y el nombre compartido de los dispositivos. También se muestra el porcentaje de dispositivos identificados correctamente.

[+ Add](#)

IP identify (10)

Total coverage  
**20% (2/10)**

| <input type="checkbox"/> | Address       | IP            | Name            | Status | iSCSI node                                                    | Share name                                 |
|--------------------------|---------------|---------------|-----------------|--------|---------------------------------------------------------------|--------------------------------------------|
| <input type="checkbox"/> | 1.1.1.1       | 1.1.1.1       | LA3-CNS-SQL-06A | OK     |                                                               | /vol/ServerLogs_STG/                       |
| <input type="checkbox"/> | 0.0.0.0/0     |               |                 |        |                                                               | /vol/ServerLogs_STG/                       |
| <input type="checkbox"/> | 10.56.100.18  |               |                 |        | iqn.1991-05.com.microsoft:la3-cns-sql-06b.cns.comcastnets.com |                                            |
| <input type="checkbox"/> | 10.56.100.19  |               |                 |        | iqn.1991-05.com.microsoft:jec20643597717.fayd.com             | /vol/wc_sc_libraries_prod/libraries_qtree/ |
| <input type="checkbox"/> | 100.54.18.100 | 100.54.18.100 | ushapl000961b   | OK     |                                                               |                                            |

Showing 1 to 5 of 10 entries

## Adición manual de dispositivos IP

Puede agregar manualmente un dispositivo IP a OnCommand Insight mediante la función de adición manual disponible en la pantalla de identificación de IP.

## Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Haga clic en la ficha **Identificación IP**.

4. Haga clic en el botón Agregar.

Aparecerá el cuadro de diálogo Agregar dispositivo

5. Introduzca la dirección, la dirección IP y un nombre de dispositivo único.

## Resultados

El dispositivo que introduzca se agrega a la lista de dispositivos de la ficha Identificación IP.

## Importando identificación de dispositivo IP desde un archivo CSV

Puede importar manualmente identificaciones de dispositivos IP a la función resolución de dispositivos mediante una lista de identificaciones de dispositivos en un archivo CSV.

### Antes de empezar

Debe tener un archivo CSV formateado correctamente para importar identificaciones de dispositivo. El archivo CSV para dispositivos IP requiere la siguiente información:

|           |
|-----------|
| Dirección |
| IP        |
| Nombre    |



Como práctica recomendada, se recomienda exportar primero la información IP Identify a un archivo CSV, realizar los cambios deseados en ese archivo y, a continuación, importar el archivo de nuevo a IP Identify. Esto garantiza que las columnas esperadas estén presentes y en el orden adecuado.

Para importar información de identificación de IP:

### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Seleccione la ficha **Identificación IP**.
4. Haga clic en **identificar > identificar desde archivo** .
  - a. Desplácese hasta la carpeta que contiene los archivos CSV para importar y seleccione el archivo deseado.

Los dispositivos que introduzca se agregarán a la lista de dispositivos de la ficha Identificación IP.

## Exportando identificación de dispositivo IP a un archivo CSV

Puede exportar identificaciones de dispositivos IP existentes desde Insight mediante la función resolución de dispositivos. Es posible que desee exportar una identificación de dispositivo para poder modificarla y volver a importarla en Insight para poder identificar


dispositivos similares a los que figuran en la identificación exportada.

#### Acerca de esta tarea

Al exportar una identificación de dispositivo IP a un archivo CSV, el archivo contiene la siguiente información en el orden que se muestra:

|           |
|-----------|
| Dirección |
| IP        |
| Nombre    |

#### Pasos

1. Inicie sesión en la interfaz de usuario web de Insight.
2. Haga clic en **Administrar > resolución del dispositivo**
3. Seleccione la ficha **Identificación IP**.
4. Seleccione el dispositivo IP o los dispositivos cuya identificación desea exportar.
5. Haga clic en la exportación  .
6. Elija si desea abrir el archivo CSV o guardar el archivo.

### Opciones de configuración en la ficha Preferencias

La ficha Preferencias de resolución de dispositivos permite crear un programa de resolución automática, especificar proveedores de almacenamiento y cintas para incluir o excluir de la identificación y establecer opciones de búsqueda DNS.

#### Programación de resolución automática

Una programación de resolución automática puede especificar cuándo se ejecuta la resolución automática del dispositivo:

| Opción         | Descripción                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------------------|
| Cada           | Utilice esta opción para ejecutar la resolución automática del dispositivo en intervalos de días, horas o minutos. |
| Todos los días | Utilice esta opción para ejecutar la resolución automática del dispositivo diariamente a una hora específica.      |
| Manualmente    | Utilice esta opción para ejecutar la resolución automática del dispositivo de forma manual.                        |



|                           |                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------|
| En cada cambio de entorno | Utilice esta opción para ejecutar la resolución automática del dispositivo siempre que haya un cambio en el entorno. |
|---------------------------|----------------------------------------------------------------------------------------------------------------------|

Si especifica manualmente, la resolución automática nocturna del dispositivo está desactivada.

## Opciones de procesamiento DNS

Las opciones de procesamiento DNS permiten seleccionar las siguientes funciones:

- Cuando el procesamiento de resultados de búsqueda DNS está habilitado, puede agregar una lista de nombres DNS para anexarlos a dispositivos resueltos.
- Puede seleccionar "resolución automática de IP:" para habilitar la resolución automática de host para los iniciadores y hosts iSCSI que acceden a recursos compartidos NFS mediante la búsqueda DNS. Si no se especifica esta opción, solo se lleva a cabo una resolución basada en FC.
- En los resultados, es posible optar por permitir guiones bajos en los nombres de host y utilizar un alias "conectado a" en lugar del alias de puerto estándar.

## Incluidos o excluyen proveedores específicos de cintas y almacenamiento

Puede incluir o excluir proveedores específicos de almacenamiento y cintas para su resolución automática. Tal vez desee excluir proveedores específicos si sabe, por ejemplo, que un host específico se convertirá en un host heredado y debería excluirse del nuevo entorno. También puede volver a agregar proveedores que ha excluido anteriormente pero que ya no desea excluir.



Las reglas de resolución de dispositivos para cinta sólo funcionan para WWN donde el Proveedor para ese WWN está establecido en **incluido como sólo cinta** en las preferencias del proveedor.

## Ejemplos de expresiones regulares

Si ha seleccionado el enfoque de expresión regular como estrategia de nomenclatura de origen, puede utilizar los ejemplos de expresiones regulares como guías para sus propias expresiones utilizadas en los métodos de resolución automática de OnCommand Insight.

### Dar formato a expresiones regulares

Al crear expresiones regulares para la resolución automática de OnCommand Insight, puede configurar el formato de salida introduciendo valores en un campo denominado `FORMAT`.

El valor predeterminado es `\1`, que significa que un nombre de zona que coincide con la expresión regular se reemplaza por el contenido de la primera variable creada por la expresión regular. En una expresión regular, los valores de las variables se crean mediante sentencias entre paréntesis. Si se producen varias sentencias paréntesis, se hace referencia numéricamente a las variables, de izquierda a derecha. Las variables se pueden utilizar en formato de salida en cualquier orden. El texto constante también se puede insertar en la salida, agregándolo al `FORMAT` campo.

Por ejemplo, es posible que tenga los siguientes nombres de zona para esta convención de nomenclatura de zona:

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123\_Miami\_hostname1\_filer\_FC1
- S14\_Tampa\_hostname2\_switch\_FC4
- S3991\_Boston\_hostname3\_windows2K\_FC0
- S44\_Raleigh\_hostname4\_solaris\_FC1

Y la salida podría tener el siguiente formato:

```
[hostname]-[data center]-[device type]
```

Para ello, debe capturar los campos de nombre de host, centro de datos y tipo de dispositivo en variables y utilizarlos en el resultado. La siguiente expresión regular haría esto:

```
. *? _ ( [a-zA-Z0-9]+ ) _ ( [a-zA-Z0-9]+ ) _ ( [a-zA-Z0-9]+ ) _ . *
```

Como hay tres conjuntos de paréntesis, las variables \1, \2 y \3 se rellenaría.

A continuación, puede utilizar el siguiente formato para recibir la salida en el formato que prefiera:

```
\2-\1-\3
```

Su salida sería la siguiente:

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Los guiones entre las variables proporcionan un ejemplo de texto constante que se inserta en el resultado con formato.

### Ejemplo 1 que muestra los nombres de las zonas

En este ejemplo, se utiliza la expresión regular para extraer un nombre de host del nombre de zona. Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- S0032\_myComputer1Name-HBA0
- S0434\_myComputer1Name-HBA1
- S0432\_myComputer1Name-HBA3

La expresión regular que podría utilizar para capturar el nombre de host sería:

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

El resultado es una coincidencia de todas las zonas que comienzan con S seguidas de cualquier combinación de dígitos , seguida de un guión bajo, el nombre de host alfanumérico (myComputer1Name), un guión o guión bajo, el HBA de letras mayúsculas y un solo dígito (0-9). El nombre de host solo se almacena en la variable \1.

La expresión regular se puede dividir en sus componentes:

- "S" representa el nombre de la zona y comienza la expresión. Esto sólo coincide con una "S" al principio del nombre de la zona.
- Los caracteres [0-9] entre paréntesis indican que lo que sigue a "S" debe ser un dígito entre 0 y 9, inclusive.
- El signo + indica que la aparición de la información en los corchetes anteriores debe existir 1 o más veces.
- El \_ (subrayado) significa que los dígitos después de S deben ser seguidos inmediatamente sólo por un carácter de subrayado en el nombre de la zona. En este ejemplo, la convención de nomenclatura de zona utiliza el guión bajo para separar el nombre de zona del nombre de host.
- Después del subrayado requerido, los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-zA-Z0-9] indican que los caracteres que se comparan son todas letras (independientemente del caso) y números.
- El \* (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- Los caracteres entre corchetes [\_-] (subrayado y guión) indican que el patrón alfanumérico debe ir seguido de un guión bajo o un guión.
- Las letras HBA en la expresión regular indican que esta secuencia exacta de caracteres debe producirse en el nombre de la zona.
- El conjunto final de caracteres entre corchetes [0-9] coincide con un solo dígito del 0 al 9, inclusive.

## Ejemplo 2

En este ejemplo, salte hasta el primer subrayado "", *luego iguala E y todo después hasta el segundo ""*, y luego salte todo después de eso.

- Zona:\* Z\_E2FHDBS01\_E1NETAPP

**Nombre de host:** E2FHDBS01

**RegExp:** . ? (**E** . ?) . \* ?

## Ejemplo 3

Los paréntesis "(" )" alrededor de la última sección de la expresión regular (abajo) identifican qué parte es el nombre de host. Si usted quisiera que VSAN3 fuera el nombre de host, sería: \_([a-zA-Z0-9]).\*

- Zona:\* A\_VSAN3\_SR48KENT\_A\_CX2578\_SPA0

**Nombre de host:** SR48KENT

**RegExp:** \_[a-zA-Z0-9]+\_([a-zA-Z0-9]) . \*

#### Ejemplo 4 que muestra un patrón de nomenclatura más complicado

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- MyComputerName123-HBA1\_Symm1\_FA3
- MyComputerName123-HBA2\_Symm1\_FA5
- MyComputerName123-HBA3\_Symm1\_FA7

La expresión regular que podría utilizar para capturar estos elementos sería:

```
([a-zA-Z0-9]*)_.*
```

La \1 la variable sólo contendría myComputerName123 después de ser evaluado por esta expresión.

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-zA-Z0-9] significan que cualquier letra (independientemente del caso) o dígito coincidirán.
- El \* (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- El carácter \_ (subrayado) de la expresión regular significa que el nombre de zona debe tener un guión bajo inmediatamente después de la cadena alfanumérica que coinciden con los corchetes anteriores.
- El . (punto) coincide con cualquier carácter (un comodín).
- El \* (asterisco) indica que el comodín del período anterior puede ocurrir 0 o más veces.

En otras palabras, la combinación .\* indica cualquier carácter, cualquier número de veces.

#### Ejemplo 5 que muestra los nombres de zona sin un patrón

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- MyComputerName\_HBA1\_Symm1\_FA1
- MyComputerName123\_HBA1\_Symm1\_FA1

La expresión regular que podría utilizar para capturar estos elementos sería:

```
(.*?)_.*
```

La variable \1 contendría myComputerName (en el ejemplo del nombre de la primera zona) o myComputerName123 (en el ejemplo del nombre de la segunda zona). Esta expresión regular coincidiría con todo antes del primer guión bajo.

La expresión regular se puede dividir en sus componentes:

- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- El .\* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.

- El \* (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- El ? el personaje hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar de en el último.
- Los caracteres .\* coinciden con el primer guión bajo encontrado y con todos los caracteres que lo siguen.

### Ejemplo 6 que muestra los nombres de los equipos con un patrón

Puede crear una expresión regular si tiene algo similar a los siguientes nombres de zona:

- 1\_Switch1\_myComputerName123A\_A1\_storageFC1
- Almacenamiento2\_Switch2\_myComputerName123B\_A2\_FC2
- Storage3\_Switch3\_myComputerName123T\_A3\_FC3

La expresión regular que podría utilizar para capturar estos elementos sería:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Debido a que la convención de nomenclatura de zona tiene más de un patrón, podríamos utilizar la expresión anterior, que coincidirá con todas las instancias de un nombre de host (myComputerName en el ejemplo) que termina con una A, una B o una T, colocando ese nombre de host en la variable \1.

La expresión regular se puede dividir en sus componentes:

- El .\* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.
- El ? el personaje hace que el partido no sea codicioso. Esto lo obliga a dejar de coincidir en el primer guión bajo, en lugar de en el último.
- El carácter de guion bajo coincide con el primer guión bajo del nombre de la zona.
- Así, la primera combinación .\*?\_ coincide con los caracteres *storage1\_* en el ejemplo del nombre de la primera zona.
- La segunda combinación .\*?\_ se comporta como la primera, pero coincide con *Switch1\_* en el ejemplo del nombre de la primera zona.
- Los paréntesis indican que el patrón contenido en se almacenará en la variable \1.
- Los caracteres entre corchetes [a-zA-Z0-9] significan que cualquier letra (independientemente del caso) o dígito coincidirán.
- El \* (asterisco) que sigue a los corchetes indica que los caracteres entre corchetes ocurren 0 o más veces.
- Los caracteres entre corchetes en la expresión regular [ABT] coinciden con un solo carácter en el nombre de la zona que debe ser A, B o T.
- El \_ (guión bajo) que sigue a los paréntesis indica que se debe realizar un seguimiento de la coincidencia de caracteres [ABT].
- El .\* (asterisco de período) coincide con cualquier carácter, cualquier número de veces.

Por lo tanto, el resultado de esto haría que la variable \1 contenga cualquier cadena alfanumérica que:

- fue precedido por un número de caracteres alfanuméricos y dos caracteres de subrayado
- estaba seguido de un guión bajo (y luego de cualquier número de caracteres alfanuméricos).

- Tenía un carácter final De A, B o T, antes del tercer guión bajo.

### Ejemplo 7

- Zona:\* myComputerName123\_HBA1\_Symm1\_FA1

**Nombre de host:** myComputerName123

**RegExp:** ([a-zA-Z0-9]+)\_.\*

### Ejemplo 8

En este ejemplo se encuentra todo antes de la primera \_.

- Zona:\* MyComputerName\_HBA1\_Symm1\_FA1

MyComputerName123\_HBA1\_Symm1\_FA1

**Nombre de host:** MyComputerName

**RegExp:** (.?)\*\_.

### Ejemplo 9

Este ejemplo lo encuentra todo después de la 1st \_ y hasta la segunda \_.

- Zona:\* Z\_MyComputerName\_StorageName

**Nombre de host:** MyComputerName

**RegExp:** .?(.?) .\*?

### Ejemplo 10

En este ejemplo se extrae "MyComputerName123" de los ejemplos de zona.

- Zona:\* Storage1\_Switch1\_MyComputerName123A\_A1\_FC1

Storage2\_Switch2\_MyComputerName123B\_A2\_FC2

Storage3\_Switch3\_MyComputerName123T\_A3\_FC3

**Nombre de host:** MyComputerName123

**RegExp:** .?.\*?([a-zA-Z0-9]+) [ABT]\*\_.

### Ejemplo 11

- Zona:\* Storage1\_Switch1\_MyComputerName123A\_A1\_FC1

**Nombre de host:** MyComputerName123A

**RegExp:** .?.\*?([a-zA-z0-9]+) .\*?

## Ejemplo 12

El ^ (circumflex o caret) **dentro de corchetes** anula la expresión, por ejemplo, [^FF] significa cualquier cosa excepto mayúsculas F, y [^a-z] significa todo, excepto la minúscula a a z, y en el caso anterior, cualquier cosa excepto la \_. La instrucción format agrega en "-" al nombre del host de salida.

- Zona:\* mhs\_apps44\_d\_A\_10a0\_0429

**Nombre de host:** mhs-apps44-d

**RegExp:** ([^\_])\_([AB]).\*+Formato en OnCommand Insight:

([^\_])\_().\*+Formato en OnCommand Insight:

## Ejemplo 13

En este ejemplo, el alias de almacenamiento está delimitado por "\" y la expresión debe utilizar "\" para definir que se está utilizando realmente "\" en la cadena, y que no forman parte de la expresión misma.

**Alias de almacenamiento:** \Hosts\E2DOC01C1\E2DOC01N1

**Nombre de host:** E2DOC01N1

**RegExp:** \\.?\\.?\\.(.\*?)

## Ejemplo 14

En este ejemplo se extrae "PD-RV-W-AD-2" de los ejemplos de zona.

- Zona:\* PD\_D-PD-RV-W-AD-2\_01

**Nombre de host:** PD-RV-W-AD-2

**RegExp:** [^\_]-(. -\d+).+

## Ejemplo 15

El ajuste de formato en este caso agrega el "US-BV-" al nombre de host.

- Zona:\* SRV\_USBVM11\_F1

**Nombre de host:** US-BV-M11

**RegExp:** SRV\_USBV([A-Za-z0-9]+)\_F[12]

**Formato:** US-BV-\1

# Manteniéndose Insight

Tanto si es nuevo en Insight y tiene que configurar un nuevo sistema como si ya ha estado funcionando durante algún tiempo, debe tomar las medidas necesarias para mantener el funcionamiento perfecto de Insight y de su red. El concepto clave de

mantenimiento es que los cambios en la red normalmente necesitan ser acomodados en Insight.

Estas son las tareas de mantenimiento más comunes:

- Mantenimiento de backups de Insight
- Actualizando licencias de Insight caducadas
- Coordinación de parches de origen de datos
- Actualización de la versión de Insight en todas las unidades de adquisición
- Eliminar orígenes de datos eliminados de Insight

## Información de gestión

OnCommand Insight supervisa su entorno, lo que le permite investigar posibles problemas antes de que se produzca una crisis. La consola de activos proporciona gráficos circulares resumidos, mapas de calor de IOPS y un gráfico interactivo de los 10 pools de almacenamiento más utilizados.

### Pasos

1. Abra **InsightAsset Dashboard** y mueva el cursor sobre los gráficos circulares para examinar la distribución de activos en estos tres gráficos:
  - Capacidad por proveedor muestra la capacidad bruta total del almacenamiento por cada proveedor.
  - La capacidad por nivel muestra la capacidad utilizable total de cada nivel de almacenamiento.
  - El gráfico circular puertos de switch muestra los fabricantes de puertos y muestra el porcentaje de puertos utilizados.
2. Consulte **datos acerca de su entorno** para obtener información acerca de la capacidad usada de su entorno, la eficiencia de la capacidad, los recursos FC consumidos y las estadísticas de infraestructura virtual.
3. Coloque el cursor sobre una barra de la piscina de almacenamiento en el gráfico \* Top 10 Pools\* para ver la capacidad utilizada y no utilizada del pool de almacenamiento.
4. Haga clic en cualquier nombre de activo que aparezca en texto grande (que indica que el activo tiene problemas) en el mapa térmico **IOP** de almacenamiento para mostrar una página que resume el estado actual de ese activo.
5. En la esquina inferior derecha de **panel de activos**, haga clic en cualquier nombre de activo que aparezca en texto grande (que indica que el activo tiene problemas) en el mapa térmico **Virtual Machine IOPS** para mostrar una página que resume el estado actual del activo.
6. En la barra de herramientas Insight, haga clic en **Admin**.
7. Observe cualquier área que muestre círculos rojos sólidos.

En la interfaz de usuario web de OnCommand Insight, los problemas potenciales se marcan con un círculo rojo sólido.

8. Haga clic en **orígenes de datos** para examinar una lista de todos los orígenes de datos supervisados.

Examine cualquier origen de datos con una columna **Estado** que contenga un mensaje con un círculo rojo sólido y con un **impacto** que aparezca como Alto o Medio. Se encuentran en la parte superior de la tabla.



Los problemas con esos orígenes de datos afectan a una parte significativa de la red, que debe abordar.

9. Haga clic en **unidades de adquisición** para anotar el estado de cada dirección IP que ejecuta Insight y reiniciar una unidad de adquisición, si es necesario
10. Haga clic en **Estado** para ver la supervisión de instancias de alto nivel de los servidores Insight.

## Supervise el estado del sistema OnCommand Insight

Debe comprobar periódicamente el estado actual de los componentes del sistema Insight mediante la página de estado, que muestra el estado de cada componente y le alerta cuando hay un problema.

### Pasos

1. Inicie sesión en la interfaz de usuario web Insight.
2. Haga clic en **Admin** y seleccione **Estado**.

Se mostrará la página Estado.

3. Vea el resumen del estado actual de los componentes prestando especial atención a cualquier estado de atención en la columna **Detalles** que está precedida por un círculo rojo, que indica un problema que requiere su atención inmediata.

La página Estado muestra información sobre cualquiera o todos los siguientes componentes de Insight en función de la configuración del sistema:

| Componente  | Prueba                               | Detalles                                                        | Pantallas                                                                                                                                                                                                                                                                                                     |
|-------------|--------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adquisición | Procesamiento de datos de inventario | Estado de la unidad de adquisición local                        | "OK" si el número de orígenes de datos de sondeo simultáneo es inferior al 75% del máximo del grupo de ejecución (el máximo predeterminado es 30).<br>"la adquisición está ocupada" si el uso es superior al 75%, y recomienda aumentar el intervalo de sondeo o agregar más unidades de adquisición remotas. |
| DWH         | Backup                               | Estado de la copia de seguridad programada del almacén de datos | "OK" y la última hora de copia de seguridad de DWH correcta si está activada la copia de seguridad programada DWH. De lo contrario, muestra información sobre cualquier error encontrado.                                                                                                                     |

|          |                       |                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------|-----------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DWH      | ETL                   | Estado de ETL del almacén de datos                 | <p>"OK" y el último tiempo de compilación de DWH satisfactorio si no hay errores. De lo contrario, muestra información sobre cualquier error encontrado.</p>                                                                                                                                                                                                                                                                                                |
| Servidor | ASUP                  | Estado de ASUP                                     | <p>"ASUP activado" y la última hora de fonohogar correcta si está disponible. "error de ASUP" si fonohome está activado pero se ha encontrado un problema.</p> <p>+ "ubicación de copia de seguridad no válida" si el directorio de copia de seguridad no es válido.</p> <p>+ muestra la última hora de fonehome correcta, así como la hora del último intento fallido si está disponible.</p> <p>+ "ASUP desactivado" si el fonohome está desactivado.</p> |
| Servidor | Resolución automática | Estado de la resolución automática del dispositivo | <p>"OK" si no hay errores. "la resolución automática está bloqueada" si los errores de identificación impiden el progreso de la resolución.</p> <p>+ «'tasa de éxito baja'» si se pudiera identificar menos del 75% de los dispositivos genéricos.</p>                                                                                                                                                                                                      |

|          |                            |                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|----------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servidor | Elasticsearch              | Estado del almacén de datos de búsqueda elástico | <p>"OK" si no hay errores.<br/>"Servicio no disponible" si no puede conectarse a un servicio de búsqueda elástico.</p> <p>+ "modo de clúster detectado" si se detecta más de un nodo.</p> <p>+ "uso elevado de memoria" si el espacio de pila utilizado es superior al 85%.</p> <p>+ "Estado: ROJO" indica un error notificado por la búsqueda elástica. Muestra información sobre el error y recomienda ponerse en contacto con el servicio de atención al cliente.</p> |
| Servidor | CPU                        | Uso de CPU Insight                               | <p>«'Aceptar'» si la carga de la CPU es inferior al 65%. "La carga de CPU del sistema es alta. Reduzca la carga de la CPU». Si la carga de CPU es superior al 65%.</p>                                                                                                                                                                                                                                                                                                   |
| Servidor | Espacio en disco adicional | Estado del espacio en disco                      | <p>Espacio libre en disco, espacio en disco utilizado por Insight, y espacio en disco recomendado reservado para Insight. «"espacio en disco bajo»» si el aprovechamiento del disco supera el 80 %.</p>                                                                                                                                                                                                                                                                  |
| Servidor | EventBus                   | Estado de EventBus                               | <p>"EventBus está vacío" si la cola EventBus está vacía, de lo contrario se muestra el estado de la cola EventBus.</p>                                                                                                                                                                                                                                                                                                                                                   |

|          |                                      |                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------|--------------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servidor | Procesamiento de datos de inventario | Estado de la capacidad de procesamiento de datos de inventario de Insight Server | «'OK» si el servidor de Insight no está ocupado. "El servidor está ocupado" si el servidor está ocupado al menos el 75% del tiempo durante la última hora. Recomienda no añadir más orígenes de datos y recomienda dividir el entorno en varios servidores.                                                                                                                                                   |
| Servidor | MySQL                                | Estado de la base de datos de MySQL                                              | <p>""OK"" si no se detectan problemas. ""la base de datos está teniendo problemas de rendimiento. Algunas consultas tardan demasiado en ejecutarse»» si el número de consultas lentas supera el 5 %.</p> <p>+ ""el archivo de registro de la base de datos ha crecido más que &lt;size&gt; en la última hora. Compruebe el archivo de registro de MySQL"" si el registro de errores crece a más de 20 KB.</p> |
| Servidor | Archivado del rendimiento            | Estado del archivado de rendimiento                                              | «"el archivo de rendimiento está activado" o «"el archivo de rendimiento no está activado»».                                                                                                                                                                                                                                                                                                                  |
| Servidor | Memoria física                       | Estado de la memoria física                                                      | <p>""OK"" si el uso de memoria es inferior al 85%. "Mi uso es alto. Reduzca el espacio de memoria total para la estabilidad del sistema» si el uso de la memoria es superior al 85%.</p>                                                                                                                                                                                                                      |

|          |                    |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|--------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Servidor | Service Pack       | Disponibilidad del Service Pack        | Muestra si hay un Service Pack disponible para Insight. Si hay un Service Pack disponible, muestra las instrucciones.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Servidor | Información de uso | Estado del envío de información de uso | <p>Muestra si el envío de información de uso a NetApp está habilitado o deshabilitado. Recomienda habilitar si está deshabilitado. Muestra la última hora de envío que se ha intentado o la última vez que se ha realizado correctamente</p> <p>+ muestra información sobre cualquier problema encontrado.</p>                                                                                                                                                                                                                                                                                                      |
| Servidor | Infracción         | Estado de las infracciones abiertas    | <p>"OK" si el número de violaciones abiertas es inferior al 75% del límite de violaciones. «El número máximo de violaciones abiertas permitidas es &lt;number&gt;» si el número de violaciones abiertas supera el 75% del límite de violaciones. Recomienda revisar la configuración de las políticas de rendimiento.</p> <p>+ "el gestor de violaciones está bloqueado" si el número de violaciones abiertas está en el límite de violaciones.</p> <p>+ tenga en cuenta que el gestor de infracciones no puede crear nuevas infracciones y recomienda revisar la configuración de la directiva de rendimiento.</p> |

|          |                            |                                         |                                                                                                                                  |
|----------|----------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Servidor | Copia de seguridad semanal | Estado de la copia de seguridad semanal | "OK" si la copia de seguridad semanal está activada, en caso contrario muestra "la copia de seguridad semanal no está activada". |
|----------|----------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|

## Eliminando dispositivos inactivos

La eliminación de dispositivos inactivos ayuda a mantener los datos más limpios y fáciles de navegar.

### Acerca de esta tarea

Para eliminar dispositivos inactivos de Insight, haga lo siguiente:

#### Pasos

1. Cree una consulta nueva o abra una consulta existente.
2. Seleccione el tipo de activo *generic device*, *host*, *Storage*, *switch* o *Tape*.
3. Agregue un filtro para **está activo** y ajuste el filtro en **no**.

La tabla resultados muestra sólo los activos que no están activos.

4. Seleccione los dispositivos que desea eliminar.
5. Haga clic en el botón **acciones** y seleccione **Eliminar dispositivos inactivos**.

Los dispositivos inactivos se eliminan y ya no se mostrarán en Insight.

## Auditar las actividades del sistema y del usuario

Si desea localizar cambios inesperados, puede ver un registro de auditoría del sistema OnCommand Insight y sus actividades de usuario. Los mensajes de registro de auditoría pueden enviarse de manera opcional a syslog, además de mostrarse en la página auditoría.

### Acerca de esta tarea

Insight genera entradas de auditoría para las actividades de cualquier usuario que afecten a la red de almacenamiento o a su gestión, incluido lo siguiente:

- Inicio de sesión
- Autorizar o anular la autorización de un camino
- Actualizar una ruta autorizada
- Establecimiento de umbrales o políticas globales
- Agregar o quitar un origen de datos

- Iniciar o detener un origen de datos
- Actualizando las propiedades del origen de datos
- Agregar, editar o eliminar una tarea
- Eliminación de un grupo de aplicaciones
- Identificar o cambiar la identificación de un dispositivo
- Cree un usuario
- Eliminar un usuario
- Cambio de rol de usuario
- Modificar un usuario (Guest à Admin)
- Cierre de sesión de un usuario (cierre de sesión forzado o cierre de sesión manual)
- Eliminación de una unidad de adquisición
- Actualizar licencia
- Habilitar backup
- Desactivando copia de seguridad
- Cuando se habilita ASUP (se informa del proxy en la misma página en el registro de auditoría)
- Si se deshabilita ASUP (se informa sobre la deshabilitación de proxy en la misma página en el registro de auditoría)
- Seguridad: Vuelva a introducir la clave, cambie las contraseñas del sistema.
- Eliminación/adición de anotaciones en activos
- Inicio/cierre de sesión del usuario de CAC
- Tiempo de espera de sesión de usuario de CAC

## Pasos

1. Abra Insight en su navegador.
2. Haga clic en **Admin** y seleccione **Auditoría**.

La página Auditoría muestra las entradas de auditoría en una tabla.

3. Se pueden ver los siguientes detalles en la tabla:

- **Tiempo**

Fecha y hora en la que se realizaron los cambios

- **Usuario**

Nombre del usuario asociado a la entrada de auditoría

- **Rol**

Rol de la cuenta de usuario, que es invitado, usuario o administrador

- **IP**

Dirección IP asociada con la entrada de auditoría

- **Acción**

Tipo de actividad en la entrada de auditoría

- **Detalles**

Detalles de la entrada de auditoría

Si hay una actividad del usuario que afecta a un recurso, como un origen de datos o una aplicación, los detalles incluyen un enlace a la página de destino del recurso.



Cuando se elimina un origen de datos, los detalles de la actividad del usuario relacionados con el origen de datos ya no contienen un enlace a la página de destino del origen de datos.

4. Puede mostrar las entradas de auditoría eligiendo un período de tiempo determinado (1 hora, 3 horas, 24 horas, 3 días y 7 días), Insight muestra un número máximo de 1000 infracciones durante el período de tiempo seleccionado.

Puede hacer clic en un número de página debajo de la tabla para examinar los datos por página si hay más datos que se ajustan en una sola página.

5. Para cambiar el orden de clasificación de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo), haga clic en la flecha del encabezado de la columna; para volver al orden predeterminado, haga clic en cualquier otro encabezado de columna.

De forma predeterminada, la tabla muestra las entradas en orden descendente.

6. Puede utilizar el cuadro **filtro** para mostrar sólo las entradas que desee en la tabla.

Para ver sólo las entradas de auditoría del usuario `izzzyk`, escriba `izzzyk` en el cuadro **filtro**.


## Supervisar las infracciones en la red

Cuando Insight genera infracciones debido a los umbrales establecidos en las políticas de rendimiento, puede visualizarlas mediante la Consola de infracciones. El panel enumera todas las infracciones que se producen en su red y le permite localizar y resolver problemas.


### Pasos

1. Abra OnCommand Insight en el explorador.
2. En la barra de herramientas Insight, haga clic en **Paneles** y seleccione **Panel de infracciones**.

Aparecerá el Panel de infracciones.

3. Puede utilizar el gráfico circular **violaciones por políticas** de las siguientes formas:
  - Puede colocar el cursor sobre cualquier segmento de un gráfico para mostrar el porcentaje de infracciones totales que se han producido para una política o métrica concreta.
  - Puede hacer clic en un corte de un gráfico para "enlarge" él, que le permite enfatizar y estudiar más cuidadosamente ese corte alejándolo del resto del gráfico.
  - Haga clic en el  en la esquina superior derecha para mostrar el gráfico circular en modo de pantalla





completa y haga clic en  de nuevo para minimizar el gráfico circular. Un gráfico circular puede contener un máximo de cinco sectores; por lo tanto, si dispone de seis políticas que generen violaciones, Insight combina el quinto y el sexto sectores en una sección "otros". Insight asigna el mayor número de infracciones al primer segmento, el segundo más infracciones al segundo segmento, etc.



4. Puede utilizar el gráfico **historial de infracciones** de las siguientes formas:


- Puede colocar el cursor sobre el gráfico para mostrar el número total de infracciones que se han producido en un momento determinado y el número que se ha producido fuera del total de cada métrica especificada.
- Puede hacer clic en una etiqueta de leyenda para eliminar los datos asociados a la leyenda del gráfico.

Haga clic en la leyenda para volver a mostrar los datos.

- Haga clic en el  en la esquina superior derecha para mostrar el gráfico en modo de pantalla completa y haga clic en  de nuevo para minimizar el gráfico circular.

5. Puede utilizar la **Tabla de infracciones** de las siguientes formas:

- Haga clic en el  en la esquina superior derecha para mostrar la tabla en modo de pantalla completa y haga clic en  de nuevo para minimizar el gráfico circular.


Si el tamaño de la ventana es demasiado pequeño, la Tabla de infracciones sólo muestra tres columnas; sin embargo, al hacer clic en , se muestran columnas adicionales (hasta siete).

- Puede mostrar infracciones para un período de tiempo determinado (**1h, 3h, 24h, 3d, 7d, Y 30d**), con Insight mostrando un número máximo de 1000 violaciones para el período de tiempo seleccionado.
- Puede utilizar el cuadro **filtro** para mostrar sólo las infracciones que desee.
- Para cambiar el orden de las columnas de una tabla por ascendente (flecha arriba) o descendente (flecha abajo), haga clic en la flecha del encabezado de la columna; para volver al orden predeterminado, haga clic en cualquier otro encabezado de columna.

De forma predeterminada, la tabla muestra las infracciones en orden descendente.

- Puede hacer clic en una infracción en la columna ID para mostrar la página de activos durante el tiempo que dure la infracción.
- Puede hacer clic en los enlaces de recursos (por ejemplo, pool de almacenamiento y volumen de almacenamiento) de la columna Description para mostrar las páginas de activos asociadas con esos recursos.
- Puede hacer clic en el enlace de política de rendimiento de la columna Policy para mostrar el cuadro de diálogo Edit Policy.

Puede que desee ajustar los umbrales de una política si cree que genera demasiadas violaciones o demasiadas.

- Puede hacer clic en un número de página para examinar los datos por página si hay más datos que ajustes en una sola página.
- Puede hacer clic en  para descartar la violación.

## Estado de la unidad de adquisición

La pantalla Unidad de adquisición ofrece una vista de todas las unidades de adquisición, incluido el estado y los errores presentes.

El estado de las unidades de adquisición de Insight conectadas al servidor se muestra en la tabla **Admin > unidades de adquisición**. Esta tabla muestra la siguiente información para cada unidad de adquisición:

- **Nombre**
- **IP**
- **Estado** es el estado de funcionamiento de la unidad de adquisición.
- **Última generación informada** muestra la última vez que se informó de una fuente de datos conectada a la unidad de adquisición.
- **Nota** muestra una nota introducida por el usuario relacionada con la AU.

Si una unidad de adquisición de la lista presenta un problema, el campo Estado mostrará un círculo rojo con información breve sobre el problema. Debería investigar cualquier problema de unidad de adquisición, ya que probablemente afectan a la recopilación de datos.

Para reiniciar una unidad de adquisición, pase el cursor sobre la unidad y haga clic en el botón *Restart Acquisition Unit* que aparece.

Para agregar una nota de texto, coloque el cursor sobre una unidad de adquisición y haga clic en el botón *Add Note* que aparece. Sólo se muestra la nota introducida más recientemente.

## Restauración de la base de datos de Insight

Para restaurar la base de datos de Insight desde un archivo de copia de seguridad verificado, utilice las opciones de solución de problemas. Esta operación sustituye por completo los datos OnCommand Insight actuales.

### Antes de empezar

- **Práctica recomendada:** \*\* Antes de restaurar la base de datos de OnCommand Insight, utilice el proceso de copia de seguridad manual para crear una copia de la base de datos actual. Compruebe que el archivo de copia de seguridad que desea restaurar esté seguro de que se trata de una copia de seguridad correcta que contiene los archivos que desea restaurar.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.

Send / Collect data

| Action                        | Description                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Back up</a>       | Back up the database (configuration and performance) into a ZIP file.                                                                                                                      |
| <a href="#">Bundle logs</a>   | Collect all log files (including acquisition recordings) and bundle them into a ZIP file. Can be used to send data back to NetApp support when troubleshooting an issue with the software. |
| <a href="#">Send ASUP now</a> | Forces an ad-hoc ASUP report. Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.                                          |

Restore a database

[Select backup ▾](#)
No file selected
[Restore](#)

Warning: Your current database will be discarded!

Other tasks

[Couldn't find what you are looking for? Connect to the old OnCommand Insight Portal.](#)  
[Need to send anonymous data back? Open the scrub utilities.](#)

- En la sección Restaurar una base de datos, seleccione el archivo de copia de seguridad que desea restaurar desde el menú **Seleccionar copia de seguridad**.
- Haga clic en **Restaurar**.
- En la advertencia de que se reemplazarán todos los datos, haga clic en **Aceptar**

El estado de la actividad de restauración se muestra en la página de restauración.

## Actualizando licencias caducadas

Si una o varias de sus licencias de Insight han caducado, puede actualizar las licencias rápidamente mediante el mismo procedimiento que hizo para instalar las licencias originalmente.

### Pasos

- En un editor de texto, como Notepad, abra el nuevo archivo de licencia que ha recibido del soporte de NetApp y copie el texto de la clave de licencia en el portapapeles de Windows.
- Abra OnCommand Insight en el explorador.
- Haga clic en **Admin** en la barra de herramientas.
- Haga clic en **Configuración**.
- Haga clic en la ficha **licencias**.
- Haga clic en **Actualizar licencia**.
- Copie el texto de la clave de licencia en el cuadro de texto **Licencia**.
- Seleccione la operación **Actualizar (más común)**.

Esta operación añade sus nuevas licencias a todas las licencias de Insight activas actualmente.

- Haga clic en **Guardar**.
- Si utiliza el modelo de licencias de Insight Consumption, debe marcar la casilla para **Activar el envío de información de uso a NetApp** en la sección de uso. El proxy debe estar configurado y activado correctamente para el entorno.

## Las licencias ya no cumplen

Si observa el mensaje "no compatible" en su página de Insight Licenses, Insight gestionando más terabytes que la licencia de su empresa.

El mensaje "no compatible" significa que su empresa pagó menos terabytes que Insight gestiona actualmente. Junto al mensaje de no conformidad se muestra la diferencia entre los terabytes gestionados y el número de terabytes con licencia.

El funcionamiento de su sistema Insight no se ve afectado, pero debe ponerse en contacto con su representante de NetApp para aumentar la cobertura de su licencia y actualizar la licencia correspondiente.

## Reemplazar licencias de versiones anteriores de Insight

Si ha adquirido una nueva versión de Insight que no sea compatible con versiones anteriores del producto, debe reemplazar las licencias anteriores por las nuevas.

Al instalar las nuevas licencias, debe seleccionar la operación **sustituir** antes de guardar el texto de la clave de licencia.

## Aplicación de un Service Pack

Periódicamente, hay disponibles paquetes de servicio, que puede aplicar para aprovechar las correcciones y mejoras en OnCommand Insight.

### Antes de empezar

- Debe haber descargado el archivo de Service Pack (por ejemplo, 7.2service\_pack\_1.patch) Del sitio NOW.
- Debe haber aprobado todos los parches.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **parches**.
3. En el botón acciones, seleccione **aplicar parche**.
4. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para buscar el archivo del Service Pack.
5. Inspeccione los tipos \* Patch name\*, **Description**, **impactados de origen de datos**, que muestran si se ven afectados los orígenes de datos y **Details**, que describe las mejoras que contiene el Service Pack.
6. Si el Service Pack seleccionado es correcto, haga clic en **aplicar parche**.

Los Service Packs se aprueban automáticamente; no es necesario realizar ninguna otra acción.

## Preparación de un informe especial de solución de problemas

Insight envía información automáticamente al soporte de clientes de NetApp a través del sistema ASUP que configuró tras instalar el software. Sin embargo, es posible que desee crear un informe de solución de problemas y abrir un caso con el equipo de soporte para

un problema específico.

Las herramientas se pueden usar en Insight para realizar una copia de seguridad manual de Insight, empaquetar los registros y enviar esa información al servicio de soporte al cliente de NetApp.

### Realizar manualmente un backup de la base de datos de OnCommand Insight

Si se habilitaron backups semanales para la base de datos de OnCommand Insight, automáticamente se generan copias que puede utilizar para restaurar la base de datos, si es necesario. Si necesita crear un backup antes de una operación de restauración o enviar al soporte técnico de NetApp para obtener ayuda, puede crear un backup .zip archivar manualmente.

#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.
3. En la sección Enviar/recopilar datos, haga clic en **copia de seguridad**.
4. Haga clic en **Guardar archivo**.
5. Haga clic en **Aceptar**.

### Agrupación de registros para soporte

Al solucionar un problema con el software Insight, puede generar rápidamente un archivo zip (con el formato "gz") de los registros y grabaciones de adquisición para enviarlo al soporte técnico de NetApp.

#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **solución de problemas**.
3. En la sección Enviar / recopilar datos, haga clic en **Bundle logs**.
4. Haga clic en **Guardar archivo**.
5. Haga clic en **Aceptar**.

### Envío de información a Soporte de NetApp

La instalación de soporte automatizado (ASUP) de NetApp envía información para la solución de problemas directamente al equipo de soporte al cliente de NetApp. Puede forzar el envío de un informe especial.

#### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin**.
2. Haga clic en **Configuración**.
3. Haga clic en la ficha **copia de seguridad/ASUP**.
4. En el área Enviar/recopilar datos, haga clic en **Enviar ASUP ahora** para enviar sus registros, grabaciones

y backup al servicio de soporte de NetApp.

Send / Collect data

| Action                         | Description                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <button>Back up</button>       | Back up the database (configuration and performance) into a ZIP file.                                                                                                                         |
| <button>Bundle logs</button>   | Collect all log files (including acquisition recordings) and bundle them into a ZIP file.<br>Can be used to send data back to NetApp support when troubleshooting an issue with the software. |
| <button>Send ASUP now</button> | Forces an ad-hoc ASUP report.<br>Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.                                          |

Restore a database

Select backup ▾ No file selected Restore

Warning: Your current database will be discarded!

Other tasks

Couldn't find what you are looking for? Connect to the old [OnCommand Insight Portal](#).

Need to send anonymous data back? Open the [Scrub utilities](#).

## Eliminación de datos para su transferencia a soporte

Los clientes que dispongan de entornos seguros deben comunicarse con el servicio de atención al cliente de NetApp para solucionar los problemas que se produzcan sin comprometer la información sobre bases de datos. Las utilidades de Scrub de OnCommand Insight le permiten configurar un diccionario completo de palabras clave y patrones para que pueda "limpiar" datos confidenciales y enviar archivos depurados al servicio de atención al cliente.

### Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área de otras tareas, haga clic en el enlace **utilidades de Scrub**.

Hay varias secciones de matorral: Buscar en Diccionario, Scrub datos, y construir diccionario, palabras clave personalizadas, y expresiones regulares.

+ .. En la sección **Lookup in Dictionary**, escriba un código para mostrar el valor que reemplaza o escriba un valor para ver el código que lo reemplaza. Nota: Antes de poder realizar una búsqueda, debe **construir** el diccionario para identificar los valores que se van a eliminar de los datos de soporte.

1. Para agregar sus propias palabras clave para eliminar de los datos de soporte, en la sección **palabras clave personalizadas**, haga clic en **acciones > Agregar palabra clave personalizada**. Introduzca una palabra clave y haga clic en **Guardar**. La palabra clave se agrega al diccionario.
2. Expanda **patrones (regex)**. Haga clic en **Agregar** para obtener el cuadro de diálogo para introducir un nuevo patrón.
3. Para utilizar una expresión regular para identificar palabras o frases para matarlas, introduzca un patrón o patrones en la sección **expresiones regulares**. Haga clic en menú:acciones[Agregar expresión regular], escriba un nombre para el patrón y la expresión regular en los campos y haga clic en **Guardar**. La

información se ha agregado al diccionario.



Los patrones deben estar comprendidos entre paréntesis redondos para identificar un grupo de captura de expresiones regulares.

4. En la sección **Crear diccionario**, haga clic en **generar** para iniciar la compilación del diccionario de todas las palabras identificadas como sensibles desde la base de datos OnCommand Insight.

Al finalizar, aparece un mensaje que le informa de que el diccionario revisado está disponible. La descripción de la base de datos incluye una línea que indica cuántas palabras clave hay en el diccionario. Compruebe la precisión de sus palabras clave en el diccionario. Si encuentra problemas y desea reconstruir el diccionario, haga clic en **Restablecer** en el bloque base de datos para eliminar todas las palabras clave recopiladas de la base de datos OnCommand Insight del diccionario. Como se indica en el mensaje, no se eliminarán otras palabras clave. Vuelva a las utilidades de Scrub e introduzca sus palabras clave personalizadas de nuevo.

5. Después de crear un diccionario Scrub, puede usarlo para eliminar un archivo de registro, XML u otro archivo de texto para que los datos sean anónimos.
6. Para eliminar un archivo de registro, XML u otro archivo de texto, en la sección **datos de archivo de Scrub**, busque el archivo y haga clic en **Archivo de Scrub**.

## Resolución avanzada de problemas

Para completar la configuración de OnCommand Insight, debe utilizar las herramientas avanzadas de solución de problemas. Estas herramientas se ejecutan en el explorador y se abren desde la página **Admin > solución de problemas**.

Para abrir las herramientas de solución de problemas avanzadas en el explorador, haga clic en el enlace **solución avanzada de problemas** que se encuentra en la parte inferior de la página.

Las herramientas avanzadas de solución de problemas le permiten ver varios informes, información del sistema, paquetes instalados y registros, así como realizar numerosas acciones como reiniciar el servidor o las unidades de adquisición, actualizar las anotaciones DWH e importar anotaciones.

Consulte la página solución avanzada de problemas para obtener información sobre todas las opciones disponibles.

### Configuración del número de horas para ignorar datos dinámicos

Es posible configurar el número de horas durante las cuales OnCommand Insight ignora la actualización de datos dinámicos, como la capacidad utilizada. Si se utiliza el valor predeterminado de seis horas y no se producen cambios en la configuración, los informes no se actualizarán con datos dinámicos hasta después del número predeterminado de horas. Esta opción mejora el rendimiento porque esta opción desacelera las actualizaciones cuando sólo cambian los datos dinámicos.

#### Acerca de esta tarea

Si se establece un valor para esta opción, OnCommand Insight actualizará los datos dinámicos basándose en las siguientes reglas:

- Si no se producen cambios de configuración, pero cambian los datos de capacidad, no se actualizarán los datos.
- Los datos dinámicos (distintos de los cambios de configuración) sólo se actualizarán después del tiempo de espera especificado en esta opción.
- Si se producen cambios en la configuración, se actualizan los datos dinámicos y de configuración.

Los datos dinámicos afectados por esta opción incluyen lo siguiente:

- Datos sobre infracciones de capacidad
- Capacidad asignada y capacidad utilizada de los sistemas de archivos
- Hipervisor
  - Capacidad utilizada de los discos virtuales
  - Capacidad utilizada de la máquina virtual
- Volumen interno
  - Capacidad asignada de datos
  - Datos capacidad utilizada
  - Ahorro con la deduplicación
  - Hora de último acceso conocido
  - Última hora de snapshot
  - Otra capacidad utilizada
  - Número de copias Snapshot
  - Capacidad utilizada de Snapshot
  - Capacidad total utilizada
- IP de iniciador de sesión iSCSI, ID de sesión de destino e ID de sesión del iniciador
- La cuota de qtree utilizada la capacidad
- Archivos de cuota usados y capacidad utilizada
- Tecnología de eficiencia del almacenamiento, ganancia/pérdida, y posible ganancia/pérdida
- Pool de almacenamiento
  - Datos capacidad utilizada
  - Ahorro con la deduplicación
  - Otra capacidad utilizada
  - Capacidad utilizada de Snapshot
  - Capacidad total utilizada
- Volumen
  - Ahorro con la deduplicación
  - Hora de último acceso conocido
  - Capacidad utilizada



## Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. Haga clic en la ficha **Configuración avanzada**, en la sección atributos dinámicos de adquisición, introduzca el número de horas que OnCommand Insight debe ignorar los datos dinámicos para los atributos dinámicos de adquisición.
4. Haga clic en **Guardar**.
5. (Opcional) para reiniciar la unidad de adquisición, haga clic en el enlace **Reiniciar unidad de adquisición**.

Al volver a restaurar la unidad de adquisición local, se vuelven a cargar todas las vistas del origen de datos de OnCommand Insight. Este cambio se aplica durante la siguiente encuesta, por lo que no tiene que reiniciar la unidad de adquisición.

## Generando registros para el soporte al cliente

Si lo solicita el servicio de soporte al cliente, genere un servidor, una adquisición o un registro remoto para solucionar problemas.

### Acerca de esta tarea

Si solicitudes de soporte al cliente de NetApp, use esta opción para generar los registros.

## Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área otras tareas, haga clic en **solución avanzada de problemas**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en el vínculo **solución de problemas**.
4. Haga clic en la ficha **Logs** y seleccione el archivo de registro que desea descargar.

Se abre un cuadro de diálogo que permite abrir el registro o guardar el registro localmente.

## Mostrar información del sistema

Puede mostrar la información de configuración de IP de Microsoft Windows acerca del sistema en el que se ha implementado OnCommand Insight Server.

## Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.
4. Haga clic en **Información del sistema**.

La configuración IP de Windows incluye información como el nombre de host, DNS, dirección IP, máscara de subred, información del sistema operativo, memoria, dispositivo de inicio y nombre de conexión.

## Enumerar los componentes de OnCommand Insight instalados

Es posible mostrar una lista de los componentes de OnCommand Insight instalados que incluyen, entre otros, el inventario, la capacidad, las dimensiones, Y las vistas del almacén de datos. Es posible que el servicio de soporte al cliente le solicite esta información o que desee ver qué versiones de software se han instalado y cuándo se han instalado.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.
4. Haga clic en **Paquetes de software instalados**.

## Calculando el número de objetos de base de datos

Para determinar el número de objetos de la base de datos OnCommand Insight, utilice la función calcular escala.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página solución de problemas avanzada, haga clic en la ficha **Informes**.
4. Haga clic en **escala calculada**.

## Reiniciar el servidor OnCommand Insight

Al reiniciar el servidor OnCommand Insight, actualice la página e inicie sesión de nuevo en el portal OnCommand Insight.

### Acerca de esta tarea



Solo el servicio de soporte al cliente de NetApp debe utilizar ambas opciones previa solicitud. No hay confirmación antes de reiniciar.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en la ficha **acciones**.
4. Haga clic en **Reiniciar servidor**.

## Mover datos de MySQL con la opción Migrate

Puede utilizar migrar un directorio de datos de MySQL a otro directorio. Puede conservar el directorio de datos actual. Puede utilizar la opción migrar del menú solución de problemas o la línea de comandos. Este procedimiento describe cómo utilizar la opción **solución de problemas > migración de datos MySQL**.

### Acerca de esta tarea

Si conserva el directorio de datos actual, se conservará como copia de seguridad y se cambiará el nombre.

### Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. Haga clic en **solución avanzada de problemas**.
3. Seleccione la ficha **acciones**
4. Seleccione **Migrate MySQL Data**.
5. Introduzca la ruta a la que desee migrar los datos.
6. Para conservar el directorio de datos existente, marque **mantener el directorio de datos existente**.
7. Haga clic en **migrar**.

## Mover datos de MySQL con la línea de comandos

Puede utilizar migrar un directorio de datos de MySQL a otro directorio. Puede conservar el directorio de datos actual. Puede utilizar la opción Migrate del menú Troubleshooting (solución de problemas) o, si lo prefiere, puede utilizar la línea de comandos. En este procedimiento, se describe cómo utilizar la línea de comandos.

### Acerca de esta tarea

Si conserva el directorio de datos actual, se conservará como copia de seguridad y se cambiará el nombre.

Puede utilizar la utilidad Migrate MySQL Data o puede utilizar un `java -jar mysqldatamigrator.jar` En la ruta OnCommand Insight de `\bin\mysqldatamigrator` donde deben utilizarse los siguientes parámetros:

- Parámetros obligatorios

- **-path**

La nueva ruta de datos a la que se copiará la carpeta de datos.

- Parámetros opcionales

- **-myCnf <my .cnf file>**

La ruta del archivo .cnf. El valor predeterminado es `<install path>\mysql\my.cnf`. Utilice este indicador sólo si se utiliza un MySQL no predeterminado.

- **-doBackup**

Si se establece este indicador, se cambiará el nombre de la carpeta de datos actual, pero no se

eliminará.

## Pasos

1. Acceda a la herramienta de línea de comandos aquí: `<installation path>\bin\mysqldatamigrator\mysqldatamigrator.jar`

## Ejemplo de uso

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

## Forzar actualizaciones de anotaciones

Si ha cambiado las anotaciones y desea utilizarlas inmediatamente en los informes, utilice una de las opciones de anotación de fuerza.

### Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página, haga clic en el enlace **solución avanzada de problemas**.
3. Haga clic en la ficha **acciones**.
4. Seleccione una de estas opciones:
  - **Actualizar anotaciones DWH** para forzar la actualización de las anotaciones en el almacén de datos a ser utilizadas para los informes.
  - **Actualizar anotaciones DWH (incl eliminado)** para forzar una actualización de anotaciones (incluidos los objetos eliminados) en el almacén de datos que se utilizará para los informes.

## Comprobar el estado de los recursos del servidor

Esta opción muestra la información del servidor OnCommand Insight, incluida la memoria del servidor, el espacio en disco, el SO y la información de la base de datos OnCommand Insight y CPU, incluido el tamaño de los datos de InnoDB y el espacio libre en disco donde reside la base de datos.

### Pasos

1. En la barra de herramientas Insight, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página en el área de otras tareas, haga clic en el vínculo **Portal de OnCommand Insight**.
3. En la página siguiente del menú Opciones avanzadas, haga clic en el vínculo **solución de problemas**.
4. Haga clic en **Estado de los recursos del servidor**.

**Para usuarios avanzados de OnCommand Insight:** el administrador puede ejecutar algunas pruebas SQL para comprobar el tiempo de respuesta de la base de datos y el servidor desde el botón al final del resumen de información. Esta opción muestra una advertencia si el recurso del servidor es bajo.

## Búsqueda de orígenes de datos fantasma

Si ha eliminado un dispositivo pero los datos del dispositivo permanecen, puede localizar cualquier origen de datos fantasma para que pueda eliminarlos.

### Pasos

1. En la interfaz de usuario web, haga clic en **Admin** y seleccione **solución de problemas**.
2. En la parte inferior de la página del área otras tareas, haga clic en el vínculo **solución avanzada de problemas**.
3. En la ficha **Informes**, haga clic en el enlace **fuentes de datos fantasma**.

OnCommand Insight crea una lista de los autores con la información de su dispositivo.

## Agregar un modelo de disco ausente

Si la adquisición falla debido a un modelo de disco desconocido, puede agregar el modelo de disco que falta al `new_disk_models.txt` vuelva a ejecutar la adquisición y el archivo.

### Acerca de esta tarea

Como parte del sondeo de un dispositivo de almacenamiento realizado por OnCommand Insight, se leen los modelos de disco del dispositivo de almacenamiento. Si un proveedor ha añadido nuevos modelos de disco a su cabina de los que no se conoce Insight o si hay alguna discrepancia entre el número de modelo que busca Insight y el que devuelve el dispositivo de almacenamiento, la adquisición de dicho origen de datos se producirá un error. Para evitar estos errores, es necesario actualizar la información de modelo de disco que se conoce en Insight. Los nuevos modelos de disco se añaden a Insight con actualizaciones, parches y versiones de mantenimiento. Sin embargo, puede decidir actualizar esta información manualmente en lugar de esperar a una revisión o actualización.

Dado que OnCommand Insight lee el archivo de modelo de disco cada cinco minutos, toda la información de nuevo modelo de datos introducida se actualiza automáticamente. No es necesario reiniciar el servidor para que los cambios surtan efecto, pero puede optar por reiniciar el servidor y cualquier unidad de adquisición remota (raus) para que los cambios surtan efecto antes de la siguiente actualización.

Las actualizaciones del modelo de disco se agregan a la `new_disk_models.txt` archivo ubicado en `la<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directorio. Comprenda la información necesaria para describir su nuevo modelo de disco antes de actualizar el `new_disk_models.txt` archivo. La información inexacta en el archivo produce datos incorrectos del sistema y podría dar lugar a una adquisición fallida.

Siga estas instrucciones para actualizar manualmente los modelos de disco de Insight:

### Pasos

1. Busque la información adecuada para su modelo de disco.
2. Con un editor de texto, abra el `new_disk_models.txt` archivo.
3. Agregue la información necesaria para el nuevo origen de datos.
4. Guarde el archivo en la `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directorio en

el servidor.

5. Realice una copia de seguridad del `new_disk_models.txt` archivar en una ubicación segura. Durante cualquier actualización de OnCommand Insight posterior, este archivo se sobrescribirá. Si la información del modelo de disco no está presente en el archivo actualizado, deberá volver a introducirla.

#### Localizar la información necesaria para el nuevo modelo de disco

Para localizar la información del modelo de disco, identifique el proveedor y el número de modelo y ejecute una búsqueda en Internet.

#### Acerca de esta tarea

Localizar la información del modelo de disco es tan simple como ejecutar una búsqueda en Internet. Asegúrese de indicar el nombre del proveedor y el número de modelo de disco antes de realizar la búsqueda.

#### Pasos

1. Se recomienda utilizar una búsqueda avanzada en Internet para el proveedor, el modelo y el tipo de documento «PDF» para buscar la hoja de datos del proveedor y/o la guía de instalación de la unidad. Estas hojas de datos suelen ser la mejor fuente de información sobre discos del proveedor.
2. Las especificaciones del proveedor no siempre proporcionan toda la información necesaria en función del número de modelo completo. A menudo es útil buscar diferentes partes de la cadena de número de modelo en el sitio del proveedor para localizar toda la información.
3. Localice el nombre del proveedor de discos, el número de modelo completo, el tamaño y la velocidad del disco y el tipo de interfaz para definir el nuevo modelo de discos en OnCommand Insight, puede utilizar la tabla siguiente como guía para ayudar a tener en cuenta esta información al buscar:

| Para este campo:                                   | Que es:     | Introduzca lo siguiente:                           |
|----------------------------------------------------|-------------|----------------------------------------------------|
| Número de modelo (también conocido como clave)     | Obligatorio |                                                    |
| Proveedor                                          | Obligatorio |                                                    |
| Velocidad del disco (RPM)                          | Obligatorio |                                                    |
| Tamaño (en GB)                                     | Obligatorio |                                                    |
| Tipo de interfaz (seleccione uno)                  | Obligatorio | ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, OTROS |
| Tiempo de búsqueda en ms                           | Opcional    |                                                    |
| Velocidad de transferencia máxima en MB/s.         | Opcional    |                                                    |
| Velocidad de transferencia de la interfaz en MB/s. | Opcional    |                                                    |

|                                           |                           |  |
|-------------------------------------------|---------------------------|--|
| Enlace a información del modelo/proveedor | Opcional pero recomendado |  |
|-------------------------------------------|---------------------------|--|

4. Introduzca esa información en el `new_disk_models.txt` archivo. Consulte "[Contenido del archivo new\\_disk\\_models.txtl.](#)" para formato, orden y ejemplos.

### Contenido del archivo `new_disk_models.txtl`.

La `new_disk_models.txt` el archivo tiene campos obligatorios y opcionales. Los campos están separados por comas, por lo que no utilice comas *dentro de* los campos.

Todos los campos son obligatorios excepto el tiempo de búsqueda, las tarifas de transferencia y `adicional_info`. Si está disponible, incluya el enlace del sitio web del proveedor/modelo en el campo `adicional_info`.

Con un editor de texto, introduzca la siguiente información en este orden, separada por comas, para cada nuevo modelo de disco que desee agregar:

1. **tecla**: utilice el número de modelo (obligatorio)
2. **proveedor**: nombre (obligatorio)
3. **número de modelo**: número completo (normalmente el mismo valor que en "tecla") (obligatorio)
4. **rpm del disco**: por ejemplo 10000 o 15000 (requerido)
5. **Tamaño**: Capacidad en GB (requerido)
6. **Tipo de interfaz**: ATA, SATA, FC, SAS, FATA, SSD, OTROS (obligatorio)
7. **tiempo de búsqueda**: en ms (opcional)
8. **Velocidad de transferencia potencial**: La velocidad de transferencia potencial en MB/s. Velocidad de transferencia máxima del disco. (opcional)
9. **Velocidad de transferencia de interfaz**: La velocidad desde y hacia el host en MB/s (opcional).
10. **Información adicional**: Cualquier información adicional que desee capturar. Lo más recomendable es introducir el enlace a la página del proveedor donde se encuentren las especificaciones, como referencia (opcional)

Si deja en blanco los campos opcionales, asegúrese de incluir la coma.

Ejemplos (cada uno en una línea sin espacios):

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfiles/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf
```

```
SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,,
```

```
X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

## Supervisión de su entorno

Insight le ayuda a evitar problemas en su entorno y a resolver rápidamente posibles

problemas.

## Datos de páginas de activos

Las páginas de activos proporcionan datos de solución de problemas de rendimiento e información de resumen acerca de un activo base (como una máquina virtual o un volumen) y los activos relacionados que utiliza (como pools de almacenamiento, nodos de almacenamiento y puertos de switch conectados), con enlaces a información adicional.

A partir de OnCommand Insight 7.3.1, todas las páginas de activos tienen una página **Principal** y una página **datos adicionales**. En la página Principal se muestra un resumen del activo y de las diferentes secciones de gráficos, topología y otra información. La página **datos adicionales** le permite configurar una página de panel personalizable para el tipo de activo actual.

Un círculo rojo sólido junto a una línea o mensaje en la pestaña principal de la página de activos indica problemas potenciales con el entorno supervisado.

### Tipos de páginas de activos

Las páginas de activos resumen el estado actual de un activo y contienen vínculos a información adicional sobre el activo y sus activos relacionados.

OnCommand Insight proporciona páginas de activos para los siguientes activos:

- Máquina virtual
- Volumen
- Volumen interno
- Host físico
- Del banco de almacenamiento
- Reducida
- Almacén de datos
- Hipervisor
- Cliente más
- Nodo de almacenamiento
- Qtree
- Disco
- VMDK
- Puerto
- Conmutador
- Estructura
- Almacenamiento de objetos (por ejemplo, Atmos, Centera, Amazon S3)
- Zona

La información de asignación y enmascaramiento se puede ver en las tablas de las páginas de activos Zone,






La información de resumen está disponible para activos de almacenamiento de objetos; sin embargo, solo puede acceder a esta información desde la página de detalles orígenes de datos.

## Buscar activos específicos en su entorno

Puede localizar información sobre activos específicos mediante la función de búsqueda. Por ejemplo, si un usuario del sistema se pone en contacto con el administrador de almacenamiento con un reclamo acerca de un servidor en particular, el administrador puede buscar el nombre del servidor y mostrar una página de activos que resume el estado y proporciona información adicional vinculada.

### Pasos

1. Abra la interfaz de usuario web de OnCommand Insight.
2. En la barra de herramientas, haga clic en .

Aparece el cuadro **Buscar activos**.

3. Introduzca el nombre de un activo o una parte del nombre.
4. Seleccione el recurso que desea de los resultados de búsqueda.

Se muestra la página de activos de ese recurso.

### Técnicas avanzadas de búsqueda

Se pueden utilizar varias técnicas de búsqueda para buscar datos u objetos en el entorno supervisado.

### Búsqueda con comodín

Puede realizar una búsqueda con varios caracteres comodín con el carácter \*. Por ejemplo, *aplic\*n* devolverá la aplicación.

### Frases utilizadas en la búsqueda

Una frase es un grupo de palabras rodeadas de comillas dobles; por ejemplo, "PAW VNX LUN 5". Puede utilizar comillas dobles para buscar documentos que contengan espacios en sus nombres o atributos.

### Operadores booleanos

Mediante operadores booleanos, puede combinar varios términos para formar una consulta más compleja.

#### • O

- EL operador OR es el operador conjunto predeterminado.

Si no hay ningún operador booleano entre dos términos, se utiliza el operador OR.

- El operador OR vincula dos términos y busca un documento coincidente si alguno de los términos

existe en un documento.

Por ejemplo, «almacenamiento O netapp» busca documentos que contengan «almacenamiento» o «netapp».

- Se dan puntuaciones altas a los documentos que coinciden con la mayoría de los términos.

#### • Y

Puede usar el operador AND para buscar documentos en los que tanto los términos de búsqueda existen en un único documento. Por ejemplo, «'aurora Y netapp'» busca documentos que contengan «almacenamiento» y «'netapp'».

Puede utilizar el símbolo && en lugar de la palabra Y.

#### • NO

Cuando utiliza EL operador NOT, todos los documentos que contienen el término después DE NO se excluyen de los resultados de la búsqueda. Por ejemplo, «almacenamiento NO netapp» busca documentos que solo contengan «almacenamiento» y no «'netapp'».

Puede utilizar el símbolo ! En vez DE la palabra NO.

### Búsqueda de prefijo y sufijo

- Tan pronto como comience a escribir una cadena de búsqueda, el motor de búsqueda realiza una búsqueda de prefijo y sufijo para encontrar la mejor coincidencia.
- Las coincidencias exactas reciben una puntuación mayor que la coincidencia de prefijo o sufijo. La puntuación se calcula en función de la distancia del término de búsqueda del resultado de búsqueda real. Por ejemplo, tenemos tres almacenes: «aurora», «aurora» y «aurora». Si busca "aur", se devolverán las tres cigüeñas. Sin embargo, el resultado de búsqueda de "aurora" tendrá la puntuación más alta porque tiene la distancia más cercana a la cadena de búsqueda de prefijo.
- El motor de búsqueda también busca términos en orden inverso, lo que le permite realizar una búsqueda de sufijo. Por ejemplo, cuando escribe «'345'» en el cuadro de búsqueda, el motor de búsqueda busca «'345'».
- La búsqueda no distingue mayúsculas y minúsculas.

### Búsqueda mediante términos indexados

Las búsquedas que coinciden con más de los términos indexados tienen como resultado puntuaciones más altas.

La cadena de búsqueda se divide en términos de búsqueda separados por espacio. Por ejemplo, la cadena de búsqueda «de almacenamiento aurora de netapp» se divide en tres palabras clave: «De almacenamiento», «'aurora'» y «'netapp'». La búsqueda se realiza utilizando los tres términos. Los documentos que coincidan con la mayoría de estos términos tendrán la puntuación más alta. Cuanta más información proporcione, mejores serán los resultados de la búsqueda. Por ejemplo, puede buscar un almacenamiento por su nombre y modo.

La interfaz de usuario muestra los resultados de la búsqueda en todas las categorías, con los tres resultados principales por categoría. Si no ha encontrado un documento que esperaba, puede incluir más términos en la cadena de búsqueda para mejorar los resultados de la búsqueda.

En la tabla siguiente se proporciona una lista de términos indexados que se pueden agregar a la cadena de búsqueda.

| Categoría       | Términos indexados                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reducida        | <ul style="list-style-type: none"> <li>• «almacenamiento»</li> <li>• nombre</li> <li>• proveedor</li> <li>• modelo</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                 |
| StoragePool     | <ul style="list-style-type: none"> <li>• «buen pool»</li> <li>• nombre</li> <li>• nombre del almacenamiento</li> <li>• Las direcciones IP del almacenamiento</li> <li>• el número de serie del almacenamiento</li> <li>• proveedor de almacenamiento de netapp</li> <li>• modelo de almacenamiento</li> <li>• nombres de todos los volúmenes internos asociados</li> <li>• nombres de todos los discos asociados</li> </ul>                                                                                   |
| Volumen interno | <ul style="list-style-type: none"> <li>• «'internalvolume»</li> <li>• nombre</li> <li>• nombre del almacenamiento</li> <li>• Las direcciones IP del almacenamiento</li> <li>• el número de serie del almacenamiento</li> <li>• proveedor de almacenamiento de netapp</li> <li>• modelo de almacenamiento</li> <li>• nombre del pool de almacenamiento</li> <li>• nombres de todos los recursos compartidos asociados</li> <li>• nombres de todas las aplicaciones y entidades de negocio asociadas</li> </ul> |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volumen                | <ul style="list-style-type: none"> <li>• «'volumen»</li> <li>• nombre</li> <li>• etiqueta</li> <li>• nombres de todos los volúmenes internos</li> <li>• nombre del pool de almacenamiento</li> <li>• nombre del almacenamiento</li> <li>• Las direcciones IP del almacenamiento</li> <li>• el número de serie del almacenamiento</li> <li>• proveedor de almacenamiento de netapp</li> <li>• modelo de almacenamiento</li> </ul> |
| Nodo de almacenamiento | <ul style="list-style-type: none"> <li>• "tormagenodo"</li> <li>• nombre</li> <li>• nombre del almacenamiento</li> <li>• Las direcciones IP del almacenamiento</li> <li>• serialnumber del almacenamiento</li> <li>• proveedor de almacenamiento de netapp</li> <li>• modelo de almacenamiento</li> </ul>                                                                                                                        |
| Host                   | <ul style="list-style-type: none"> <li>• «'host'»</li> <li>• nombre</li> <li>• Direcciones IP</li> <li>• nombres de todas las aplicaciones y entidades de negocio asociadas</li> </ul>                                                                                                                                                                                                                                           |
| Almacén de datos       | <ul style="list-style-type: none"> <li>• «datastore»</li> <li>• nombre</li> <li>• IP del centro virtual</li> <li>• nombres de todos los volúmenes</li> <li>• nombres de todos los volúmenes internos</li> </ul>                                                                                                                                                                                                                  |

|                                |                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Equipos virtuales              | <ul style="list-style-type: none"> <li>• «"máquina virtual"»</li> <li>• nombre</li> <li>• Nombre DNS</li> <li>• Direcciones IP</li> <li>• nombre del host</li> <li>• Direcciones IP del host</li> <li>• nombres de todos los almacenes de datos</li> <li>• nombres de todas las aplicaciones y entidades de negocio asociadas</li> </ul> |
| Interruptores (normales y NPV) | <ul style="list-style-type: none"> <li>• "bruja"</li> <li>• Dirección IP</li> <li>• wwn</li> <li>• nombre</li> <li>• número de serie</li> <li>• modelo</li> <li>• ID de dominio</li> <li>• nombre de la estructura</li> <li>• wwn de la estructura</li> </ul>                                                                            |
| Cliente más                    | <ul style="list-style-type: none"> <li>• «"aplicación"»</li> <li>• nombre</li> <li>• inquilino</li> <li>• línea de negocio</li> <li>• unidad de negocio</li> <li>• proyecto</li> </ul>                                                                                                                                                   |
| Cinta                          | <ul style="list-style-type: none"> <li>• «'cinta'»</li> <li>• Dirección IP</li> <li>• nombre</li> <li>• número de serie</li> <li>• proveedor</li> </ul>                                                                                                                                                                                  |
| Puerto                         | <ul style="list-style-type: none"> <li>• «'puerto'»</li> <li>• wwn</li> <li>• nombre</li> </ul>                                                                                                                                                                                                                                          |

|            |                                                                                               |
|------------|-----------------------------------------------------------------------------------------------|
| Estructura | <ul style="list-style-type: none"> <li>• «tejido»</li> <li>• wwn</li> <li>• nombre</li> </ul> |
|------------|-----------------------------------------------------------------------------------------------|


## Cambiar el intervalo de tiempo de los datos mostrados


De forma predeterminada, una página de activo muestra las últimas 24 horas de datos; sin embargo, puede cambiar el segmento de datos que se muestra seleccionando otro tiempo fijo o un intervalo de tiempo personalizado para ver menos o más datos.

### Acerca de esta tarea

Puede cambiar el segmento de tiempo de los datos mostrados mediante una opción que se encuentra en cada página de activos, independientemente del tipo de activo.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. En la esquina superior izquierda de la página, haga clic en cualquiera de los siguientes iconos de tiempo para cambiar el segmento de datos que se muestra:
  - **3h**  
Muestra las últimas tres horas de datos.
  - **24h**  
Muestra las últimas 24 horas de datos.
  - **3d**  
Muestra los últimos tres días de datos.
  - **7d**  
Muestra los últimos siete días de datos.
  - **30d**  
Muestra los últimos treinta días de datos.
  - **Personalizado**  
Muestra un cuadro de diálogo que permite elegir un intervalo de tiempo personalizado. Puede visualizar hasta 31 días de datos a la vez.

4. Si elige **personalizado**, haga lo siguiente:
- Haga clic en el campo de fecha y seleccione un mes, día y año para la fecha de inicio.
  - Haga clic en la lista Hora y seleccione una hora de inicio.
  - Repita los pasos a y b para los datos y la hora final.
  - Haga clic en .

### Determinación del estado de adquisición del origen de datos



Dado que los orígenes de datos son la fuente principal de información de Insight, es imprescindible que se garantice que permanezcan en estado en ejecución.

La capacidad de ver el estado de adquisición del origen de datos está disponible en cada página de activos para todos los activos adquiridos directamente. Puede ocurrir cualquiera de los siguientes escenarios de adquisición, en los que el estado se muestra en la esquina superior derecha de la página de activos:

- Se ha adquirido correctamente desde el origen de datos

Muestra el estado "adquirido xxxx`", where `xxxx indica el tiempo de adquisición más reciente de los orígenes de datos del activo.

- Hay un error de adquisición.

Muestra el estado "adquirido xxxx`", where `xxxx indica el tiempo de adquisición más reciente del activo con uno o varios orígenes de datos . Al hacer clic , una ventana muestra cada origen de datos del activo, el estado del origen de datos y la última vez que se adquirieron los datos. Al hacer clic en un origen de datos se muestra la página de detalles del origen de datos.

Si un activo no se adquiere directamente, no se muestra ningún estado.

### Secciones de páginas de activos

Una página de activos muestra varias secciones que contienen información relevante para el activo. Las secciones que vea dependen del tipo de activo.

#### Resumen

La sección Resumen de una página de activos muestra un resumen de la información sobre el activo en particular y muestra los problemas relacionados con el activo, indicados por un círculo rojo, con hipervínculos a información adicional sobre activos relacionados y a cualquier política de rendimiento asignada al activo.

En el siguiente ejemplo, se muestran algunos de los tipos de información disponibles en la sección Summary de una página de activos para una máquina virtual. Cualquier elemento con un círculo rojo fijo junto a él indica posibles problemas con el entorno supervisado.


## Summary

|                       |                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------|
| Power state:          | On                                                                                                    |
| Guest state:          | Running                                                                                               |
| Datastore:            | DS_SP1_1                                                                                              |
| CPU:                  | 41.05%                                                                                                |
| Memory:               | ● 51% (1,047 / 2,048 MB)                                                                              |
| Capacity:             | 10% (19.5 / 195.3 GB)                                                                                 |
| Latency:              | 1.93 ms (6.00 ms max)                                                                                 |
| IOPS:                 | 1,317.33 IO/s (4,964.00 IO/s max)                                                                     |
| Throughput:           | 38.79 MB/s (142.00 MB/s max)                                                                          |
| DNS name:             | VM_Cs_travBookcomp.com                                                                                |
| IP:                   | 10.97.133.23                                                                                          |
| OS:                   | Microsoft Windows Server 2008 R2(64-bit)                                                              |
| Processors:           | 4                                                                                                     |
| FC Fabrics Connected: | 1                                                                                                     |
| Performance Policies: | VM Latency-Critical<br>VM Latency-Warning<br>Comp Corp.Customer Support SLA latency<br>● Exchange SLO |

## Uso de la sección Resumen

Puede ver la sección Resumen para ver información general sobre un activo. Concretamente, resulta útil ver si cualquier métrica (por ejemplo, memoria, capacidad y latencia) o cualquier política de rendimiento son un motivo de preocupación, lo que indica OnCommand Insight cuando se muestra un círculo rojo junto a la métrica o la política de rendimiento.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.



La información que se muestra en la sección Resumen depende del tipo de página de activos que esté viendo.

3. Puede hacer clic en cualquiera de los vínculos de activos para ver sus páginas de activos.

Por ejemplo, si está viendo un nodo de almacenamiento, puede hacer clic en un enlace para ver la página de activos del almacenamiento al que está asociado o hacer clic en para ver la página del activo del partner de alta disponibilidad.



#### 4. Puede ver las métricas asociadas al activo.

Un círculo rojo junto a una métrica indica que podría necesitar diagnosticar y resolver problemas potenciales.



Puede observar que la capacidad del volumen puede mostrar más del 100 % en algunos activos de almacenamiento. Esto se debe a que los metadatos relacionados con la capacidad del volumen que forma parte de los datos de capacidad consumida que notifica el activo.

#### 5. Si corresponde, puede hacer clic en un enlace de política de rendimiento para ver la política de rendimiento o las políticas asociadas con el activo.

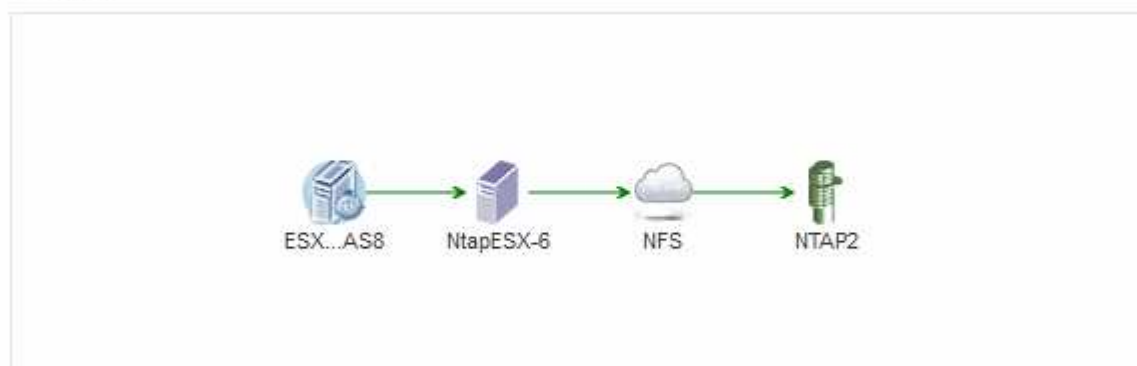
Si aparece un círculo rojo junto a una política de rendimiento, indica que un activo ha superado el umbral definido de la política de rendimiento. Debe examinar la política de rendimiento para diagnosticar el problema con más detalle.

### Topología

La sección Topology, si corresponde a un activo, le permite ver cómo está conectado un activo base con sus activos relacionados.

A continuación, se muestra un ejemplo de lo que puede aparecer en la sección Topology de una página de activos de máquinas virtuales.

#### Topology




Si la topología del activo es mayor de lo que cabe en la sección, se muestra en su lugar el enlace **haga clic para ver el hipervínculo topolog.**

### Uso de la sección Topology

La sección Topología le permite ver cómo los activos de su red están conectados entre sí y mostrar información sobre los activos relacionados.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:

- En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. La sección Topología se encuentra en la esquina superior derecha de la página de activos.

Si la topología del activo es mayor de lo que cabe en la sección, haga clic en el enlace **haga clic para ver el hipervínculo topolog**.



3. Para ver más información sobre los activos relacionados del activo base, sitúe el cursor sobre un activo relacionado en la topología y haga clic en su nombre, que muestra su página de activos.

### Datos de usuarios

Se muestra la sección datos de usuario de una página de activos y permite cambiar cualquier dato definido por el usuario, como aplicaciones, entidades de negocio y anotaciones.

A continuación se muestra un ejemplo de lo que podría mostrarse en la sección datos de usuario de una página de activos de máquina virtual cuando se asigna una aplicación, una entidad de negocio y una anotación al activo:


#### User Data



|                       |                                                                                                                                                                                    |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application(s):       | <a href="#">Concur</a>                                                                                                                                                             |
| Business Entities:    | <a href="#">Hybridsoft Corporation.Sales.Wes...</a>                                                                                                                                |
| Birthday:             | 01/30/2016   |
| <a href="#">+ Add</a> |                                                                                                                                                                                    |

### Uso de la sección datos de usuario para asignar o modificar aplicaciones

Es posible asignar aplicaciones en ejecución en el entorno a ciertos activos (host, máquinas virtuales, volúmenes, volúmenes internos e hipervisores). La sección datos de usuario permite cambiar la aplicación asignada a un activo o asignar una aplicación o aplicaciones adicionales a un activo.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Puede hacer lo siguiente:
  - Para ver la página de activos de la aplicación, haga clic en el nombre de la aplicación.

- Para cambiar la aplicación asignada o para asignar una aplicación o aplicaciones adicionales, coloque el cursor sobre el nombre de la aplicación, si hay una aplicación asignada o sobre **ninguna**, si no hay ninguna aplicación asignada, haga clic en  , escriba para buscar una aplicación o selecciónela de la lista y, a continuación, haga clic en .




Si elige una aplicación asociada a una entidad de negocio, la entidad de negocio se asignará automáticamente al activo. En este caso, cuando coloca el cursor sobre el nombre de la entidad comercial, se muestra la palabra *derived*. Si desea mantener la entidad sólo para el activo y no para la aplicación asociada, puede anular manualmente la asignación de la aplicación.

- Para eliminar una aplicación, haga clic en .

## Uso de la sección datos de usuario para asignar o modificar entidades de negocio

Puede definir entidades de negocio para realizar un seguimiento de los datos de su entorno y crear informes a un nivel más granular. La sección datos de usuario de una página de activos permite cambiar la entidad de negocio asignada a un activo o quitar una entidad de negocio de un activo.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en  , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Puede hacer lo siguiente:
  - Para cambiar la entidad asignada o para asignar una entidad, haga clic en  y seleccione una entidad de la lista.
  - Para quitar una entidad de negocio, haga clic en .




No se puede quitar una entidad derivada de una aplicación asignada al activo.

## Uso de la sección datos de usuario para asignar o modificar anotaciones

Al personalizar OnCommand Insight para realizar un seguimiento de los datos de sus requisitos corporativos, puede definir notas especializadas, llamadas *anotaciones*, y asignarlas a sus activos. La sección datos de usuario de una página de activos muestra las anotaciones asignadas a un activo y también permite cambiar las anotaciones asignadas a ese activo.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en  , escriba el nombre del activo y, a continuación,

seleccione el activo en la lista.

- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.

3. En la sección **datos de usuario** de la página de activos, haga clic en **+ Add**.

Aparece el cuadro de diálogo Agregar anotación.


4. Haga clic en **anotación** y seleccione una anotación de la lista.

5. Haga clic en **valor** y realice una de las siguientes acciones, según el tipo de anotación que haya seleccionado:

- Si el tipo de anotación es lista, fecha o booleano, seleccione un valor de la lista.
- Si el tipo de anotación es texto, escriba un valor.

6. Haga clic en **Guardar**.

La anotación se asigna al activo. Posteriormente, puede filtrar los activos mediante anotaciones mediante una consulta.

7. Si desea cambiar el valor de la anotación después de asignarla, haga clic en  y seleccione un valor diferente.

Si la anotación es del tipo de lista para el que está seleccionada la opción **Agregar valores dinámicamente al asignar anotaciones**, puede escribir para agregar un nuevo valor además de seleccionar un valor existente.

## Vista experta

La sección Vista de experto de una página de activos le permite ver una muestra de rendimiento del activo base en función del número de métricas aplicables en contexto con un período de tiempo elegido (3 horas, 24 horas, 3 días, 7 días, o un período de tiempo personalizado) en el gráfico de rendimiento y cualquier activo relacionado con él.

A continuación se muestra un ejemplo de la sección Vista de experto en una página de activos de volumen:



Puede seleccionar las métricas que desea ver en el gráfico de rendimiento durante el período de tiempo seleccionado.

La sección Recursos muestra el nombre del activo base y el color que representa el activo base en el gráfico de rendimiento. Si la sección correlación superior no contiene un activo que desea ver en el gráfico de rendimiento, puede utilizar el cuadro **Buscar activos** de la sección Recursos adicionales para localizar el activo y agregarlo al gráfico de rendimiento. A medida que se añaden recursos, aparecen en la sección Recursos adicionales.

También se muestra en la sección Resources, cuando corresponda, cualquier activo relacionado con el activo base en las siguientes categorías:

- Arriba correlacionado

Muestra los activos con una alta correlación (porcentaje) con una o más métricas de rendimiento al activo base.

- Principales colaboradores

Muestra los activos que contribuyen (porcentaje) al activo base.

- Avaricia

Muestra los activos que eliminan los recursos del sistema del activo al compartir los mismos recursos, como hosts, redes y almacenamiento.

- Degradado

Muestra los activos agotados de los recursos del sistema debido a este activo.

Definiciones de métricas de Expert View

La sección Vista de experto de una página de activos muestra varias métricas en función del período de tiempo seleccionado para el activo. Cada métrica se muestra en su propio gráfico de rendimiento. Puede agregar o quitar métricas y activos relacionados de los gráficos en función de los datos que desee ver.

| Métrico                        | Descripción                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BB Credit Zero Rx, Tx          | Número de veces que el recuento de créditos de búfer a búfer de recepción/transmisión pasó a cero durante el período de muestreo. Esta métrica representa el número de veces que el puerto conectado tuvo que dejar de transmitir porque este puerto estaba fuera de créditos para proporcionar. |
| BB duración cero de crédito Tx | Tiempo en milisegundos durante el cual el crédito de transmisión BB fue cero durante el intervalo de muestreo.                                                                                                                                                                                   |

|                                                               |                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Proporción de aciertos de caché (total, lectura, escritura) % | Porcentaje de solicitudes que provocan aciertos en caché. Cuanto mayor sea el número de aciertos en comparación con el acceso al volumen, mejor será el rendimiento. Esta columna está vacía para las cabinas de almacenamiento que no recopilan información de acierto en caché. |
| Uso de caché (total) %                                        | Porcentaje total de solicitudes de caché que producen aciertos en caché                                                                                                                                                                                                           |
| Clase 3 descarta                                              | Recuento de descartes de transporte de datos de clase 3 de Fibre Channel.                                                                                                                                                                                                         |
| % De uso de CPU (total)                                       | Cantidad de recursos de CPU utilizados activamente, como porcentaje del total disponible (en todas las CPU virtuales).                                                                                                                                                            |
| Error de CRC                                                  | Número de tramas con comprobaciones de redundancia cíclicas no válidas (CRCs) detectadas por el puerto durante el período de muestreo                                                                                                                                             |
| Velocidad de fotogramas                                       | Velocidad de transmisión de fotogramas por segundo (FPS)                                                                                                                                                                                                                          |
| Promedio de tamaño de cuadro (Rx, Tx)                         | Relación entre el tráfico y el tamaño del fotograma. Esta métrica le permite identificar si hay alguna estructura general.                                                                                                                                                        |
| Tamaño del marco demasiado largo                              | El número de tramas de transmisión de datos de Fibre Channel es demasiado largo.                                                                                                                                                                                                  |
| Tamaño del marco demasiado corto                              | El número de tramas de transmisión de datos de Fibre Channel es demasiado corto.                                                                                                                                                                                                  |
| Densidad de I/o (total, lectura, escritura)                   | Número de IOPS dividido por la capacidad usada (tal como se adquirió de la encuesta de inventario más reciente del origen de datos) para el volumen, el volumen interno o el elemento de almacenamiento. Medida en el número de operaciones de I/o por segundo por TB.            |
| IOPS (total, lectura, escritura)                              | Número de solicitudes de servicio de I/o de lectura/escritura que pasan por el canal de I/o o una parte de ese canal por unidad de tiempo (medidas en I/o por segundo)                                                                                                            |


|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rendimiento de IP (total, lectura, escritura) | <p>Total: Velocidad agregada a la que se transmitieron y recibieron datos IP en megabytes por segundo. Read: Rendimiento de IP (recibir): Tasa media a la que se recibieron los datos de IP en megabytes por segundo.</p> <p>Write: Rendimiento IP (transmisión): Velocidad media a la que se transmiten los datos IP en megabytes por segundo.</p>                                                                                                                                                                        |
| Latencia (total, lectura, escritura)          | <p>Latencia (I+W): Tasa a la que se leen o se escriben los datos en las máquinas virtuales en un tiempo fijo. El valor se mide en megabytes por segundo.</p> <p>Latencia: Tiempo de respuesta medio de los equipos virtuales de un almacén de datos.</p> <p>Top latencia: El mayor tiempo de respuesta de las máquinas virtuales de un almacén de datos.</p>                                                                                                                                                               |
| Error de enlace                               | Número de fallos de enlace detectados por el puerto durante el período de muestreo.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Restablecer Rx, Tx                            | El número de enlaces de recepción o transmisión se restablece durante el período de muestreo. Esta métrica representa el número de restablecimientos de enlace que emitió el puerto conectado a este puerto.                                                                                                                                                                                                                                                                                                               |
| Uso de memoria (total) %                      | Umbral de la memoria utilizada por el host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| R/W parcial (total) %                         | <p>Número total de veces que una operación de lectura/escritura cruza un límite de franja en cualquier módulo de disco en una LUN RAID 5, RAID 1/0 o RAID 0 en general, los pasos de franja no son beneficiosos, ya que cada uno requiere un I/O adicional. Un porcentaje bajo indica un tamaño de elemento de franja eficiente y es un indicador de alineación incorrecta de un volumen (o un LUN de NetApp).</p> <p>Para CLARiiON, este valor es el número de cruces de franja dividido por el número total de IOPS.</p> |
| Errores de puerto                             | Informe de errores de puerto durante el período de muestreo/período de tiempo dado.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Recuento de pérdidas de señal                 | Número de errores de pérdida de señal. Si se produce un error de pérdida de señal, no hay conexión eléctrica y existe un problema físico.                                                                                                                                                                                                                                                                                                                                                                                  |

|                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tasa de intercambio (tasa total, tasa en tasa, tasa de salida) | Velocidad a la que se cambia la memoria, hacia fuera o ambos desde el disco a la memoria activa durante el período de muestreo. Este contador se aplica a las máquinas virtuales.                                                                                                                                                                                                                                                           |
| Número de pérdidas de sincronización                           | Cantidad de errores de pérdida de sincronización. Si se produce un error de pérdida de sincronización, el hardware no puede detectar el tráfico ni bloquearlo. Es posible que todos los equipos no utilicen la misma velocidad de datos, o que la óptica o las conexiones físicas puedan ser de mala calidad. El puerto debe resincronizar después de cada uno de estos errores, lo que afecta al rendimiento del sistema. Se mide en KB/s. |
| Rendimiento (total, lectura, escritura)                        | Velocidad a la que se transmiten, reciben o ambos datos en un tiempo fijo en respuesta a las solicitudes de servicio de I/O (medidas en MB por segundo).                                                                                                                                                                                                                                                                                    |
| Tiempo de espera descartar tramas - Tx                         | Recuento de tramas de transmisión descartadas causadas por el tiempo de espera.                                                                                                                                                                                                                                                                                                                                                             |
| Velocidad de tráfico (total, lectura, escritura)               | Tráfico transmitido, recibido o ambos recibidos durante el período de muestreo, en mebibytes por segundo.                                                                                                                                                                                                                                                                                                                                   |
| Utilización del tráfico (total, lectura, escritura)            | Relación entre el tráfico recibido/transmitido/total y la capacidad de recepción/transmisión/total durante el período de muestreo.                                                                                                                                                                                                                                                                                                          |
| Porcentaje de utilización (total, lectura, escritura)          | Porcentaje del ancho de banda disponible utilizado para la transmisión (Tx) y la recepción (Rx).                                                                                                                                                                                                                                                                                                                                            |
| Escritura pendiente (total)                                    | Número de solicitudes de servicio I/O de escritura pendientes.                                                                                                                                                                                                                                                                                                                                                                              |

### Uso de la sección Vista experta

La sección Vista de experto le permite ver gráficos de rendimiento de un activo basados en cualquier número de métricas aplicables durante un período de tiempo elegido y agregar activos relacionados para comparar y contrastar el rendimiento de activos y activos relacionados durante diferentes períodos de tiempo.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación,



seleccione el activo en la lista.

- Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. De forma predeterminada, el gráfico de rendimiento muestra dos métricas para el período de tiempo seleccionado para la página del activo. Por ejemplo, para un almacenamiento, el gráfico de rendimiento muestra la latencia y el total de IOPS de forma predeterminada. La sección Resources muestra el nombre del recurso y una sección de recursos adicionales, que le permiten buscar activos. Dependiendo del activo, también puede ver los activos en las secciones correlacionadas Top, contribuidor Top, avaricioso y degraded.

3. Puede hacer clic en **Seleccionar métricas para mostrar** y seleccionar una métrica para agregar un gráfico de rendimiento para una métrica.

Se agrega un gráfico de rendimiento para la métrica seleccionada. El gráfico muestra los datos del período de tiempo seleccionado. Puede cambiar el período de tiempo haciendo clic en otro período de tiempo en la esquina superior izquierda de la página del activo.

Puede volver a realizar el paso y hacer clic para borrar una métrica. Se elimina el gráfico de rendimiento de la métrica.

4. Puede colocar el cursor sobre el gráfico y cambiar los datos de métrica que se muestran haciendo clic en cualquiera de los siguientes, dependiendo del activo:

- **Leer o escribir**
- **Txo Rx total** es el valor predeterminado.

5. Puede arrastrar el cursor sobre los puntos de datos del gráfico para ver cómo cambia el valor de la métrica en el período de tiempo seleccionado.


6. En la sección **Recursos**, puede realizar cualquiera de las siguientes acciones, si procede, para agregar cualquier activo relacionado a los gráficos de rendimiento:

- Puede seleccionar un activo relacionado en las secciones correlación superior, contribuyentes principales, codiciosos o degradados para agregar datos de ese activo al gráfico de rendimiento para cada métrica seleccionada. Los activos deben tener una correlación o contribución mínima del 15% para ser mostrados.

Después de seleccionar el activo, aparece un bloque de color junto al activo para indicar el color de sus puntos de datos en el gráfico.

- Para cualquier activo mostrado, puede hacer clic en el nombre del activo para mostrar su página de activo, o puede hacer clic en el porcentaje que el activo correlaciona o contribuye con el activo base para ver más información acerca de la relación de activos con el activo base.

Por ejemplo, al hacer clic en el porcentaje vinculado junto a un activo correlacionado superior se muestra un mensaje informativo que compara el tipo de correlación que tiene el activo base.

- Si la sección correlación superior no contiene un activo que desea mostrar en un gráfico de rendimiento con fines de comparación, puede utilizar la casilla **Buscar activos** de la sección Recursos adicionales para localizar otros activos. Después de seleccionar un activo, este se muestra en la sección Recursos adicionales. Cuando ya no desee ver información sobre el activo, haga clic en .

## Activos relacionados




Si corresponde, una página de activos muestra una sección de activos relacionados. Por ejemplo, una página de activos de volúmenes puede mostrar información acerca de activos como Storage Pools, puertos de switch conectados y recursos de computación.




Cada sección incluye una tabla que enumera cualquiera de los activos relacionados de esa categoría, con vínculos a sus respectivas páginas de activos y varias estadísticas de rendimiento relacionadas con el activo.


### Uso de la sección activos relacionados

La sección activos relacionados le permite ver cualquiera de los activos relacionados con el activo base. Cada activo relacionado se muestra en una tabla junto con las estadísticas pertinentes del activo. Puede exportar la información de activos, ver las estadísticas de activos en los gráficos de rendimiento de la vista experto o mostrar un gráfico que muestre estadísticas de sólo activos relacionados.

### Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset.
3. Para controlar cómo se muestran los activos en la tabla:
  - Haga clic en el nombre de cualquier activo para mostrar su página de activo.
  - Utilice el cuadro **filtro** para mostrar sólo activos específicos.
  - Haga clic en un número de página para examinar los activos por página si hay más de cinco activos en la tabla.
  - Cambie el orden de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
  - Agregue un activo relacionado a cualquier gráfico de rendimiento en la sección Vista experto colocando el cursor sobre el activo relacionado y haciendo clic en .
4. Para exportar la información mostrada en la tabla a un .CSV archivo:
  - a. Haga clic en .
  - b. Haga clic en **Abrir con** y luego en **Aceptar** para abrir el archivo con Microsoft Excel y guardarlo en una ubicación específica, o haga clic en **Guardar archivo** y luego en **Aceptar** para guardar el archivo en la carpeta Descargas.

Todos los atributos de objeto de las columnas actualmente seleccionadas para su visualización se exportan al archivo. Sólo se exportarán los atributos de las columnas mostradas. Tenga en cuenta que sólo se exportan las primeras 10,000 filas de la tabla.
5. Para mostrar la información de activos relacionada en un gráfico debajo de la tabla, haga clic en  y realice cualquiera de las siguientes acciones:
  - Haga clic en **Leer, escribir** o **total** para cambiar los datos de la métrica que se muestran. **Total** es el valor predeterminado.
  - Haga clic en  para seleccionar una métrica diferente.
  - Haga clic en  para cambiar el tipo de gráfico. **Diagrama de línea** es el valor predeterminado.

- Mueva el cursor por los puntos de datos del gráfico para ver cómo cambia el valor de la métrica en el período de tiempo seleccionado para cada activo relacionado.
- Haga clic en un activo relacionado en la leyenda del gráfico para agregarlo o quitarlo del gráfico.
- Haga clic en un número de página de la tabla de activos relacionados para ver otros activos relacionados en el gráfico.
- Haga clic en  para cerrar el gráfico.

## Infracciones

Puede utilizar la sección de infracciones de una página de activos para ver las infracciones, si las hay, que ocurren en su entorno como resultado de una política de rendimiento asignada a un activo. Las políticas de rendimiento supervisan los umbrales de la red y le permiten detectar una infracción de un umbral inmediatamente, identificar las implicaciones y analizar el impacto y la causa raíz del problema de una manera que permita una corrección rápida y efectiva.


En el siguiente ejemplo se muestra la sección aViolations que se muestra en una página de activos de un hipervisor:

| Time                   | Description                                                                           |
|------------------------|---------------------------------------------------------------------------------------|
| 06/05/2015 5:00:00 pm  | Port balance index of 74 on <a href="#">esx1</a> exceeds the threshold of 50          |
| 06/12/2015 8:59:54 am  | 2 violations for <a href="#">esx2</a> with 'Swap out rate' > 3                        |
| 06/12/2015 12:04:54 pm | <a href="#">esx1</a> violation with 'Swap out rate' > 3.00 KB/s (value of 86.85 KB/s) |
| 06/12/2015 12:29:54 pm | <a href="#">esx1</a> violation with 'Swap in rate' > 3.00 KB/s (value of 59.90 KB/s)  |
| 06/12/2015 1:04:54 pm  | 7 violations for <a href="#">ds-30</a> with 'Latency - Total' > 50                    |

## Uso de la sección violaciones


La sección infracciones le permite ver y administrar cualquiera de las infracciones que se produzcan en la red como resultado de una política de rendimiento asignada a un activo.

## Pasos

1. Inicie sesión en la interfaz de usuario web de OnCommand Insight.
2. Localice una página de activos realizando una de las siguientes acciones:
  - En la barra de herramientas Insight, haga clic en , escriba el nombre del activo y, a continuación, seleccione el activo en la lista.
  - Haga clic en **Paneles**, seleccione **Panel de activos**, busque un nombre de activo y haga clic en él. Aparece la página Asset. La sección violaciones muestra el tiempo en que se produjo la infracción y una descripción del umbral que se atravesó, junto con un hipervínculo al activo en el que se produjo la violación (por ejemplo «2 violaciones de los derechos de propiedad DS-30 con latencia - total > 50»).
3. Puede realizar cualquiera de las siguientes tareas opcionales:
  - Utilice el cuadro **filtro** para mostrar sólo infracciones específicas.
  - Haga clic en un número de página para examinar las violaciones por página si hay más de cinco infracciones en la tabla.

- Cambie el orden de las columnas de una tabla a ascendente (flecha arriba) o descendente (flecha abajo) haciendo clic en la flecha del encabezado de la columna.
- Haga clic en el nombre del activo en cualquier descripción para mostrar su página de activos; un círculo rojo indica los problemas que necesitan más investigación.

Puede hacer clic en la política de rendimiento, que se muestra en el cuadro de diálogo Edit Policy, para revisar la política de rendimiento y realizar cambios en la política de ser necesario.

- Haga clic en  eliminar una infracción de la lista si determina que el problema ya no es motivo de preocupación.

### **Página de activos personalizable**

Los datos adicionales se pueden mostrar en widgets personalizables en cada página de activo. Personalizar la página de un activo aplica la personalización a las páginas para todos los activos de ese tipo.

Para personalizar los widgets de páginas de activos, realice las siguientes acciones:

1. Agregue un widget a la página
2. Cree una consulta o expresión para que el widget muestre los datos deseados
3. Elija un filtro si lo desea
4. Elija un método de agrupación o acumulación
5. Guarde el widget
6. Repita el procedimiento para todos los widgets que desee
7. Guarde la página del activo

También puede agregar variables a la página de activos personalizados que se pueden utilizar para afinar aún más los datos mostrados en widgets. Además de las variables habituales, cada tipo de activo puede usar un conjunto de variables "\$this" para identificar rápidamente recursos directamente relacionados con el activo actual, por ejemplo, todas las máquinas virtuales alojadas por el mismo hipervisor que aloja la máquina virtual actual.

Esta página de activos personalizados es única para cada usuario, así como para cada tipo de activo. Por ejemplo, si el usuario A crea una página de activos personalizada para una máquina virtual, esa página personalizada se mostrará para cualquier página de activos de máquina virtual, para ese usuario.

Los usuarios sólo pueden ver, editar o eliminar las páginas de activos personalizados que crean.

Las páginas de activos personalizados no se incluyen en la funcionalidad de exportación/importación de Insight.

### **Entender las variables "\$this"**

Las variables especiales de la página personalizable "datos adicionales" de un activo le permiten mostrar fácilmente información adicional directamente relacionada con el activo actual.

## Acerca de esta tarea

Para utilizar las variables « »\$this» en widgets de la página de inicio personalizable de su activo, siga estos pasos. En este ejemplo, añadiremos un widget de tabla.



las variables « »\$this» solo son válidas para la página de destino personalizable de un activo. No están disponibles para otros paneles de Insight. Las variables disponibles « »\$this» varían en función del tipo de activo.

## Pasos

1. Desplácese a una página de activos para obtener un activo de su elección. Para este ejemplo, vamos a elegir una página de activos de máquinas virtuales (VM). Consultar o buscar una máquina virtual y hacer clic en el enlace para ir a la página de activos de esa máquina virtual.


Se abre la página de activos para la máquina virtual.

2. Haga clic en la lista desplegable **Cambiar vista:** > **datos adicionales de la máquina virtual** para ir a la página de destino personalizable de ese activo.
3. Haga clic en el botón **Widget** y elija **widget de tabla**.

Se abre el widget Table para su edición. De forma predeterminada, todos los almacenamientos se muestran en la tabla.

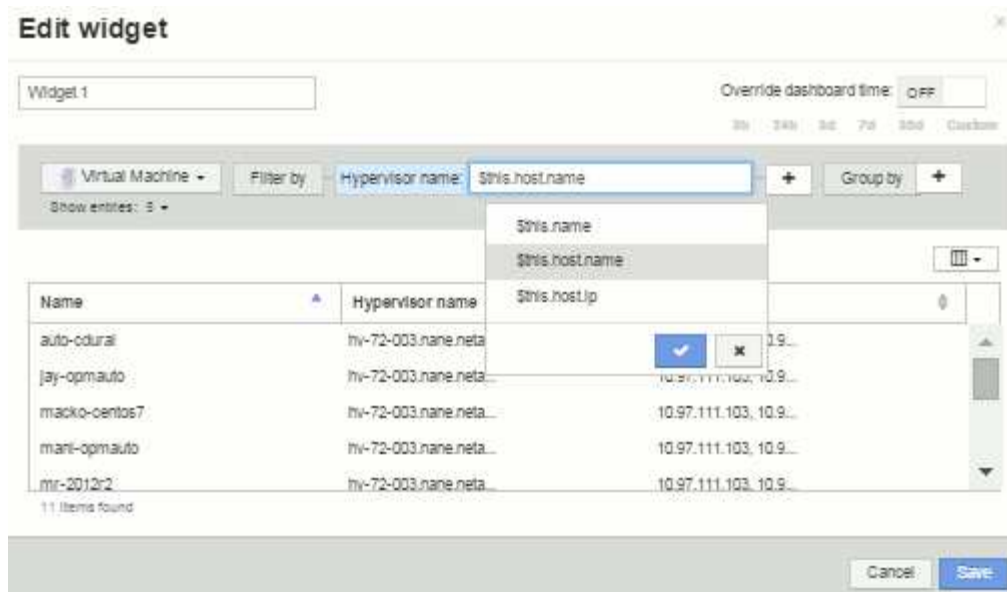
4. Queremos mostrar todas las máquinas virtuales. Haga clic en el selector de activos y cambie **almacenamiento a máquina virtual**.

Ahora todos los equipos virtuales se muestran en la tabla.

5. Haga clic en el botón **selector de columna\***  y agregue el campo **\*nombre del hipervisor** a la tabla.

El nombre del hipervisor se muestra para cada máquina virtual de la tabla.

6. Solo nos preocupamos por el hipervisor que aloja la máquina virtual actual. Haga clic en el botón **filtro por** del campo+ y seleccione **nombre de hipervisor**.
7. Haga clic en **Any** y seleccione la variable **\$this.host.name**. Haga clic en el botón de comprobación para guardar el filtro.



- Ahora la tabla muestra todas las máquinas virtuales alojadas por el hipervisor actual de la máquina virtual. Haga clic en **Guardar**.

## Resultados

La tabla que haya creado para esta página de activos de máquina virtual se mostrará en la página de activos de máquina virtual que muestre. El uso de la variable **\$this.host.name** en el widget significa que sólo se mostrará en la tabla el hipervisor del equipo virtual propiedad del activo actual.

## Equilibrado de recursos de red

Para resolver problemas de equilibrio, utilice las páginas de activos para encontrar los problemas e identificar volúmenes de alta capacidad que están infrautilizados.

### Pasos

- Abra la consola de activos en el explorador.
- En el mapa térmico de IOPS de máquinas virtuales, se observa el nombre de una máquina virtual en una impresión muy grande que a menudo informa de problemas.
- Haga clic en el nombre de la máquina virtual para mostrar la página del activo.
- Compruebe si hay mensajes de error en el resumen.
- Compruebe los gráficos de rendimiento y, en particular, los recursos principales correlacionados para localizar cualquier volumen que pueda estar en disputa.
- Añada volúmenes al gráfico de rendimiento para comparar los patrones de actividad y mostrar más páginas de activos de otros recursos implicados en el problema.
- Desplácese hasta la parte inferior de la página Asset para ver listas de todos los recursos asociados con la VM. Tenga en cuenta que cualquier VMDK funciona a alta capacidad. Es probable que esto cause la contención.
- Para resolver el problema de equilibrio, identifique un recurso que está infrautilizado para recibir la carga de un recurso sobreutilizado o quite una aplicación menos exigente del recurso utilizado.

## Examen del rendimiento de la red

Puede examinar el rendimiento de su entorno de almacenamiento e identificar recursos infrutilizados o sobreutilizados e identificar riesgos antes de que se conviertan en problemas.

Insight ayuda a resolver o evitar problemas de rendimiento y disponibilidad que se desvelan a través de los datos de almacenamiento recopilados.

Puede usar Insight para realizar estas tareas de gestión del rendimiento:

- Supervise el rendimiento en todo el entorno
- Identifique los recursos que influyen en el rendimiento de otros dispositivos

## La importancia de los puertos

El servidor de Insight Server y almacén de datos (DWH) puede requerir que varios puertos TCP estén libres para poder funcionar con fiabilidad. Algunos de estos puertos sólo se utilizan para procesos vinculados al adaptador localhost (127.0.0.1), pero siguen siendo necesarios para que los servicios principales funcionen de forma fiable. El número de puertos necesarios es un superconjunto de puertos que se utilizan en la red.

### Puertos de Insight Server

Los servidores Insight pueden tener servidores de seguridad de software instalados. Los "agujeros" que se tendrían que abrir serían como se describe a continuación.

**Entrada HTTPS 443:** Suponiendo que tenga la WebUI de Insight ejecutándose en TCP 443, debe exponer que para permitir a cualquiera de los siguientes consumidores:

- Usuarios de Insight de WebUI
- Unidades de adquisición remota que buscan conectarse al servidor de Insight
- Servidores OCI DWH con conectores a este servidor Insight.
- Cualquier interacción programática con la API DE REST de Insight

Nuestra recomendación general para cualquiera que desee implementar la protección con firewall en el nivel de host del servidor de Insight es permitir el acceso HTTPS a todos los bloques IP de la red corporativa.

**Inbound MySQL (TCP 3306).** Este puerto sólo debe estar expuesto a cualquier servidor Insight DWH con un conector

Aunque Insight tiene docenas de recopiladores de datos, todos están basados en encuestas: Insight hará que sus unidades de adquisición (AUS) inicien comunicación de salida a varios dispositivos. Mientras el firewall basado en host esté "con estado", de modo que permita el tráfico de retorno a través del firewall, los firewalls basados en host de Insight Server no deberían afectar a la adquisición de datos.

### Puertos de almacén de datos

Para servidores Insight DWH:

**HTTPS entrante 443:** Suponiendo que tenga la WebUI de Insight ejecutándose en TCP 443, debe exponer que permite a los siguientes consumidores:

- Usuarios administrativos de Insight del portal de administración de DWH

**HTTPS entrante (TCP 9300)** - esta es la interfaz de informes Cognos. Si va a tener usuarios que interactúan con la interfaz de informes de Cognos, debe exponerse de forma remota.

Podemos imaginar entornos en los que el DWH puede no necesitar estar expuesto; quizás los autores del informe simplemente hagan conexiones RDP con el servidor DWH, y crear y programar informes allí, mientras que todos los informes están programados para ser entregados a través de SMTP, o escritos en un sistema de archivos remoto.

**Inbound MySQL (TCP 3306).** Este puerto solo debe quedar expuesto si su organización tiene alguna integración basada en MySQL con datos DWH: ¿Está extrayendo datos de los distintos mercados de datos DWH para su incorporación a otras aplicaciones como CMDb, sistemas de pago por uso, etc.

## Análisis de rendimiento lento del PC

Si recibe llamadas de usuarios de la red quejándose de que sus equipos se ejecutan lentamente, debe analizar el rendimiento del host e identificar los recursos afectados.

### Antes de empezar

En este ejemplo, el llamante dio el nombre de host.

### Pasos

1. Abra Insight en su navegador.
2. Introduzca el nombre de host en el cuadro **Buscar activos** y haga clic en el nombre de host en los resultados de la búsqueda.

Se abrirá la página *Asset* del recurso.

3. En la página *Asset* del host, examine los gráficos de rendimiento en el centro de la página. Quizás sea conveniente mostrar diferentes tipos de datos además de latencia e IOPS que generalmente se seleccionan previamente. Haga clic en las casillas de verificación de otros tipos de datos, como rendimiento, memoria, CPU o procesamiento IP, según el tipo de dispositivo.
4. Para mostrar una descripción de un punto en un gráfico, coloque el puntero del ratón sobre el punto.
5. También es posible que desee cambiar el intervalo de tiempo con la selección en la parte superior de la página para que sea de 3 horas hasta 7 días o todos los datos disponibles.
6. Examine la lista de **recursos correlacionados principales** para ver si hay otros recursos con el mismo patrón de actividad que el recurso base.

El primer recurso de la lista es siempre el recurso base.

- a. Haga clic en un porcentaje vinculado junto a un recurso correlacionado para ver si el patrón de actividad correlacionado es para IOPS o CPU del recurso base y otro recurso.
  - b. Haga clic en la casilla de comprobación de un recurso correlacionado para añadir sus datos a los gráficos de rendimiento.
  - c. Haga clic en el nombre vinculado del recurso correlacionado para mostrar su página de activos.
7. Para una máquina virtual, como en este ejemplo, localice la agrupación de almacenamiento en **Top Concorreletal resources** y haga clic en el nombre de la agrupación de almacenamiento.



Analizar recursos correlacionados

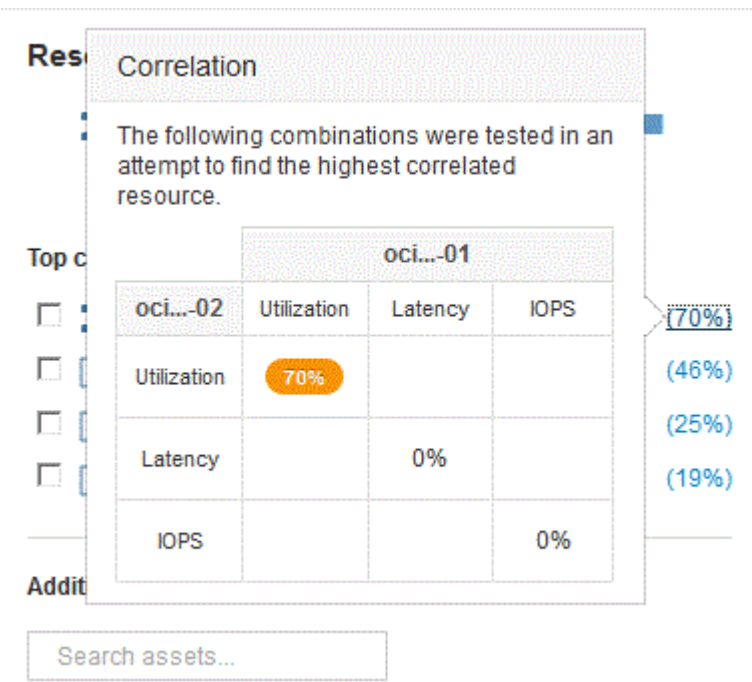
Cuando esté investigando problemas de rendimiento y abra *Asset page* para un dispositivo, debe utilizar la lista Top correlated resources para afinar los datos que se muestran en los gráficos de rendimiento. Un recurso con un porcentaje alto indica que el recurso tiene una actividad similar al recurso base.

Acerca de esta tarea

Está investigando un problema de rendimiento y ha abierto la página de activos de un dispositivo.

Pasos

- 1. En la lista \* recursos correlacionados principales\*, el primer recurso es el recurso base. Los recursos correlacionados de la lista se clasifican según el porcentaje de actividad correlacionada con el primer dispositivo. Haga clic en el porcentaje vinculado de correlación para ver los detalles. En este ejemplo, la correlación del 70 % está en utilización, por lo que tanto el recurso base como este recurso correlacionado tienen la misma utilización.



- 2. Para agregar un recurso correlacionado a los gráficos de rendimiento, active la casilla de verificación de la lista **principales recursos correlacionados** del recurso que desea agregar. De forma predeterminada, cada recurso proporciona los datos totales disponibles, pero sólo puede seleccionar datos de lectura o escritura en el menú de la casilla de verificación.

Cada recurso de los gráficos tiene un color diferente para que pueda comparar las mediciones de rendimiento de cada recurso. Sólo se traza el tipo de datos apropiado para las métricas de medición seleccionadas. Por ejemplo, los datos de CPU no incluyen métricas de lectura o escritura, por lo que solo están disponibles los datos totales.

- 3. Haga clic en el nombre vinculado del recurso correlacionado para mostrar su página de activos.
- 4. Si no ve un recurso enumerado en los recursos correlacionados principales que cree que debe ser considerado en el análisis, puede utilizar el cuadro **activos de búsqueda** para encontrar ese recurso.

## Supervisión del entorno Fibre Channel

Mediante el uso de las páginas de activos de Fibre Channel de OnCommand Insight, puede supervisar el rendimiento y el inventario de las estructuras de su entorno y conocer los cambios que puedan dar lugar a problemas.

### Páginas de activos de Fibre Channel

Las páginas de activos de Insight presentan información resumida sobre el recurso, su topología (el dispositivo y sus conexiones), gráficos de rendimiento y tablas de recursos asociados. Puede utilizar las páginas de activos Fabric, switch y puerto para supervisar el entorno Fibre Channel. Especialmente útil cuando se resuelve un problema de Fibre Channel es el gráfico de rendimiento de cada activo de puerto, que muestra el tráfico del puerto de contribuidor superior seleccionado. Además, también puede mostrar métricas de crédito de búfer a búfer y errores de puerto en este gráfico, donde Insight muestra un gráfico de rendimiento independiente para cada métrica.

### Políticas de rendimiento para métricas de puertos

Insight le permite crear políticas de rendimiento para supervisar la red y detectar diversos umbrales y alertas cuando se superen esos umbrales. Puede crear políticas de rendimiento para los puertos en función de las métricas de puertos disponibles. Cuando se produce una infracción de un umbral, Insight lo detecta y lo notifica en la página de activos asociados mostrando un círculo sólido rojo; por alerta de correo electrónico, si se configura; y en el panel de infracciones o en cualquier panel personalizado que informe de infracciones.

## Tiempo de vida (TTL) y datos de reducción de la muestra

A partir de OnCommand Insight 7.3, la retención de datos o el tiempo de vida (TTL) se ha incrementado a de 7 a 90 días. Dado que esto significa que se procesan muchos más datos para gráficos y tablas y la posibilidad de decenas de miles de puntos de datos, los datos se reducen antes de mostrarse.

Downsampling proporciona una aproximación estadística de sus datos en gráficos, lo que le proporciona una visión global eficiente de los datos sin tener que mostrar cada punto de datos, manteniendo al mismo tiempo una visión precisa de los datos recopilados.

### ¿Por qué es necesario reducir el muestreo?

Insight 7.3 aumenta el tiempo de vida (TTL) de los datos a 90 días. Esto significa un aumento en la cantidad de procesamiento necesario para preparar datos para su visualización en gráficos y gráficos. Para permitir que los gráficos se muestren de forma rápida y eficiente, los datos se reducen de forma que mantiene la forma general de un gráfico sin necesidad de procesar cada punto de datos para ese gráfico.



No se pierden datos reales durante el muestreo descendente. Puede elegir ver los datos reales del gráfico en lugar de los datos de muestra descendente siguiendo los pasos que se muestran a continuación.

### Cómo funciona la reducción de muestras

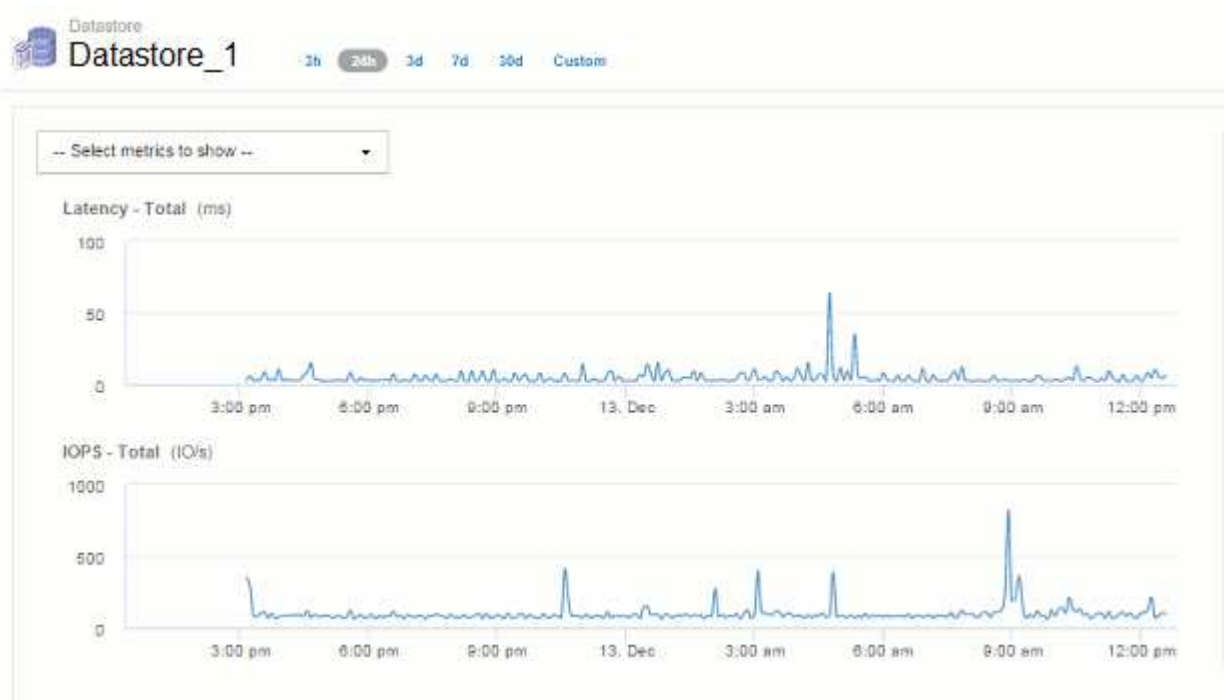
Los datos se reducen en las siguientes condiciones:

- Cuando el intervalo de tiempo seleccionado incluye 7 días de datos o menos, no se produce ninguna reducción de la muestra. Los gráficos muestran datos reales.

- Cuando el intervalo de tiempo seleccionado incluye más de 7 días de datos pero menos de 1,000 puntos de datos, no se produce ninguna reducción de muestreo. Los gráficos muestran datos reales.
- Cuando el intervalo de tiempo seleccionado incluye más de 7 días de datos y más de 1,000 puntos de datos, se reduce la muestra de los datos. Los gráficos muestran datos aproximados.

Los siguientes ejemplos muestran la acción de reducción de la muestra. En la primera ilustración se muestran los gráficos de latencia e IOPS en una página de activos de almacén de datos durante un periodo de 24 horas, tal y como se muestra seleccionando **24h** en el selector de tiempo de la página de activos. También puede ver los mismos datos seleccionando **personalizado** y ajustando el intervalo de tiempo al mismo periodo de 24 horas.

Dado que estamos eligiendo un intervalo de tiempo inferior a 7 días y tenemos menos de 1,000 puntos de datos para trazar, los datos mostrados son datos reales. No se produce ninguna reducción de la muestra.

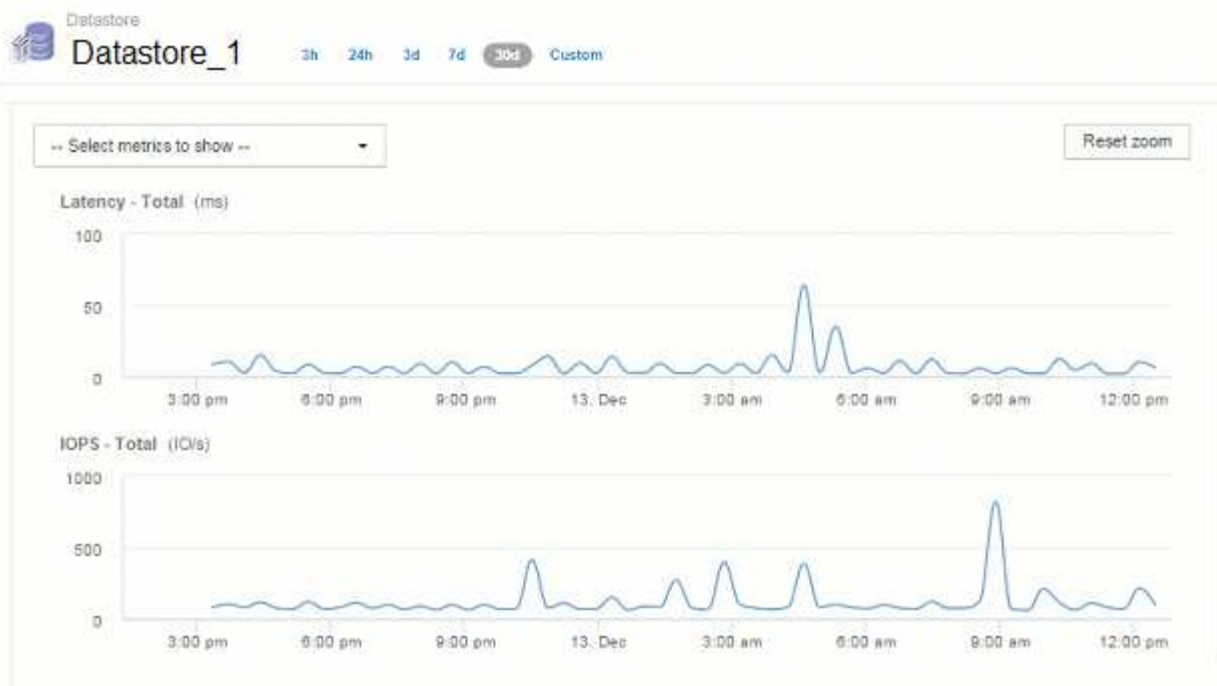


Sin embargo, si está viendo datos eligiendo **30d** en el selector de tiempo de página de activos, También se puede configurar un intervalo de tiempo personalizado de más de 7 días (o en el caso de que Insight haya recogido más de 1,000 muestras de datos durante el periodo seleccionado), los datos se reducen antes de mostrarse. Al ampliar un gráfico de muestra descendente, la pantalla continúa mostrando los datos aproximados.



Al ampliar un gráfico de muestra descendente, el zoom es un zoom digital. La pantalla continúa mostrando los datos aproximados.

Puede verlo en la siguiente ilustración, donde el intervalo de tiempo se establece por primera vez en 30d, y el gráfico se amplía para mostrar el mismo periodo de 24 horas como se ha indicado anteriormente.



Los gráficos de muestra descendente muestran el mismo período de 24 horas que los gráficos "reales" anteriores, por lo que las líneas siguen la misma forma general, lo que le permite detectar rápidamente picos o valles interesantes en sus datos de rendimiento.



Debido a la forma en que se aproximan los datos para la reducción de muestras, las líneas de la carta pueden estar ligeramente desactivadas al comparar las líneas de la muestra descendente vs datos reales, para permitir una mejor alineación en los gráficos. Sin embargo, la diferencia es mínima y no afecta a la precisión general de los datos mostrados.

### Infracciones en gráficos con muestreo inferior

Al ver gráficos con muestras descendentes, tenga en cuenta que no se muestran las infracciones. Para ver las violaciones, puede hacer una de estas dos cosas:

- Para ver los datos reales de ese intervalo de tiempo, seleccione personalizado en el selector de tiempo de página de activos e introduzca un intervalo de tiempo inferior a 7 días. Pase el ratón sobre cada punto rojo. La información sobre herramientas mostrará la infracción que se ha producido.
- Anote el intervalo de tiempo y busque las infracciones en el panel de infracciones.

### Eliminación del historial de inventario

A partir de la versión 7.3.2, Insight mantiene el historial de cambios del inventario (básico) durante 90 días. Las versiones anteriores de Insight mantuvieron todo el historial de cambios de inventario desde el momento de la instalación. Tras una actualización de una versión anterior de Insight, se reduce el historial de inventario antiguo a y, a continuación, se conserva a los 90 días.

Después de actualizar a la versión actual de OnCommand Insight, el historial se corta a los últimos 90 días. Insight corta la historia en fragmentos de 30 días que tienen una vez al día, comenzando por la más antigua, hasta que quedan 90 días de historia. A continuación, la historia se corta diariamente, para mantener sólo 90 días" de historia de cambio de inventario.

## Ruta NAS para máquinas virtuales

OnCommand Insight 7.3 admite rutas NAS para máquinas virtuales a recursos compartidos de almacenamiento. Estas rutas son similares a las rutas NAS para los hosts con los recursos compartidos de almacenamiento. Cuando se permite la dirección IP de una máquina virtual para acceder a un recurso compartido, se crea una ruta NAS.

Las rutas NAS para máquinas virtuales se muestran en la página de destino de los volúmenes internos. Esta página contiene un widget Storage Resources montado en invitado al que identifica los volúmenes internos a los que tienen acceso las máquinas virtuales.

- Las rutas NAS se crean cuando las máquinas virtuales tienen acceso a los recursos compartidos back-end. No se reconoce si los equipos virtuales acceden o no a los recursos compartidos.
- El cálculo de correlación se basa en las latencias y las IOPS, y no incluye casos en los que las máquinas virtuales tienen rutas NAS al almacenamiento back-end.
- El usuario puede consultar el recurso compartido por dirección IP del iniciador, pero no se admite la consulta por ruta.

La tabla Compute Resources del volumen interno ahora muestra también las máquinas virtuales con rutas NAS. Para cada equipo virtual, se proporcionan datos de CPU y memoria, utilización y rendimiento.

### Impacto en el almacén de datos

Los cambios en el almacén de datos que están presentes después de actualizar a OnCommand Insight 7.3 incluyen los siguientes:

- la tabla `dwh_Inventory.nas_logical` se elimina de la tienda de datos de inventario y se sustituye por una vista.

Se conservan todos los informes de Insight 7.2.x que contengan la tabla de rutas NFS.

- la tabla `dwh_Inventory.nas_cr_logical` se agrega al mercado de datos de inventario e incluye lo siguiente:
  - Recurso de computación
  - Volumen interno
  - Reducida
  - Recurso compartido NAS

### Capacidad como serie temporal

Con OnCommand Insight 7.3.1, la información de capacidad se registra y se registra como datos de series temporales.

Anteriormente, la información de capacidad adquirida de orígenes de datos ha sido exclusivamente datos "puntuales" (PIT), lo que significa que no se podía utilizar en gráficos como datos de series temporales. Ahora, los valores de capacidad de los activos se pueden utilizar como datos de series temporales de las siguientes formas:

- Gráfica en tablas, widgets, vistas de expertos y en cualquier lugar donde se muestren los datos de series temporales
- Se aplica a umbrales de rendimiento con infracciones mediante semántica existente

- Se utiliza en expresiones con otros contadores de rendimiento cuando sea apropiado

Tenga en cuenta que si actualiza una versión anterior de Insight, los valores de capacidad DE PIT anteriores utilizados en consultas o en filtros para paneles personalizados se sustituirán por los datos de capacidad de series temporales. Esto puede dar lugar a pequeños cambios en la forma en que se notifican o filtran los datos de capacidad en comparación con los datos equivalentes de versiones anteriores de Insight.

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.