Configurar Insight

OnCommand Insight

NetApp
April 01, 2024

Tabla de contenidos

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:

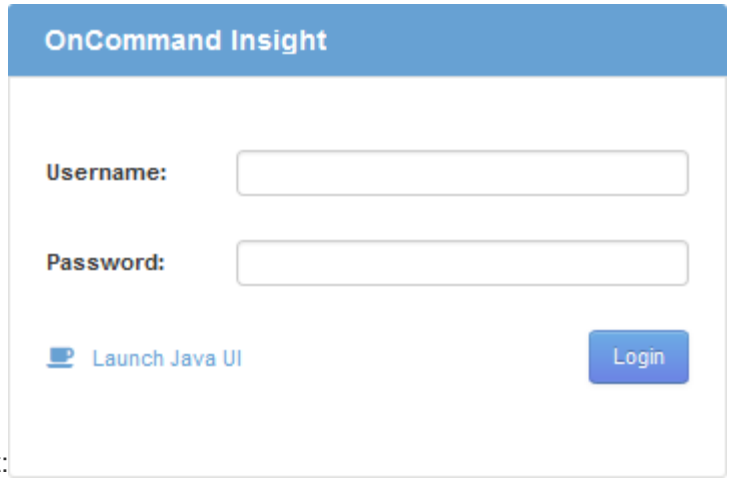
      `https://fqdn`

    - 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. `.lcn` 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
Cliente 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
siga

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

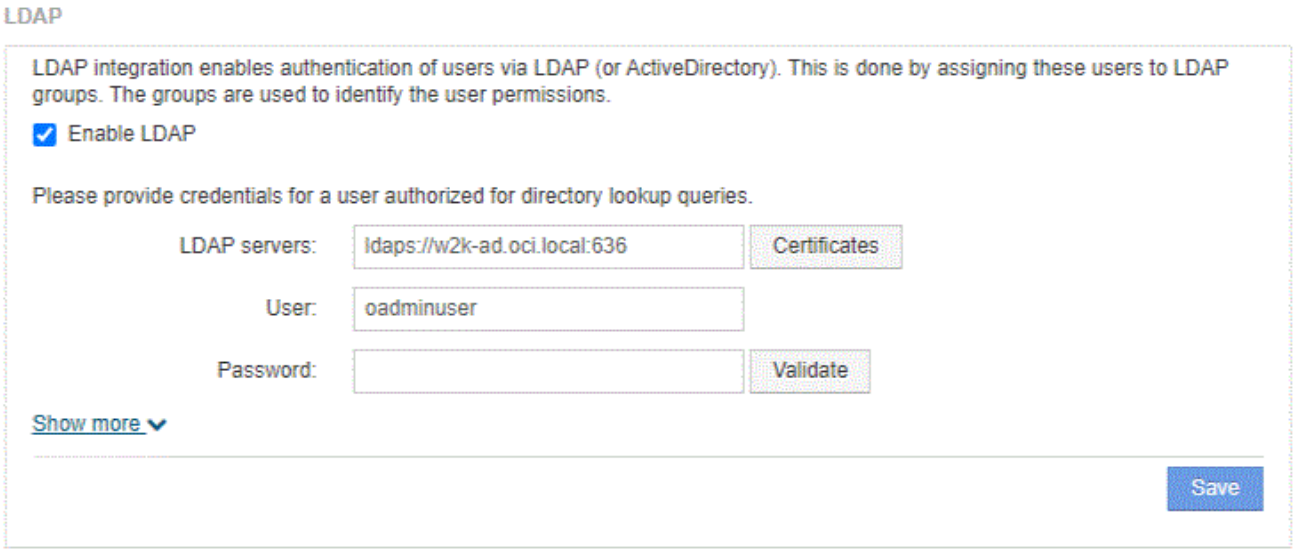
OnCommand Insight admite LDAP y LDAPS mediante el servidor de Microsoft Active Directory. Pueden funcionar implementaciones de LDAP adicionales pero no han sido aprobadas con Insight. Este procedimiento supone que está utilizando Microsoft Active Directory versión 2 o 3 LDAP (protocolo ligero de acceso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



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.

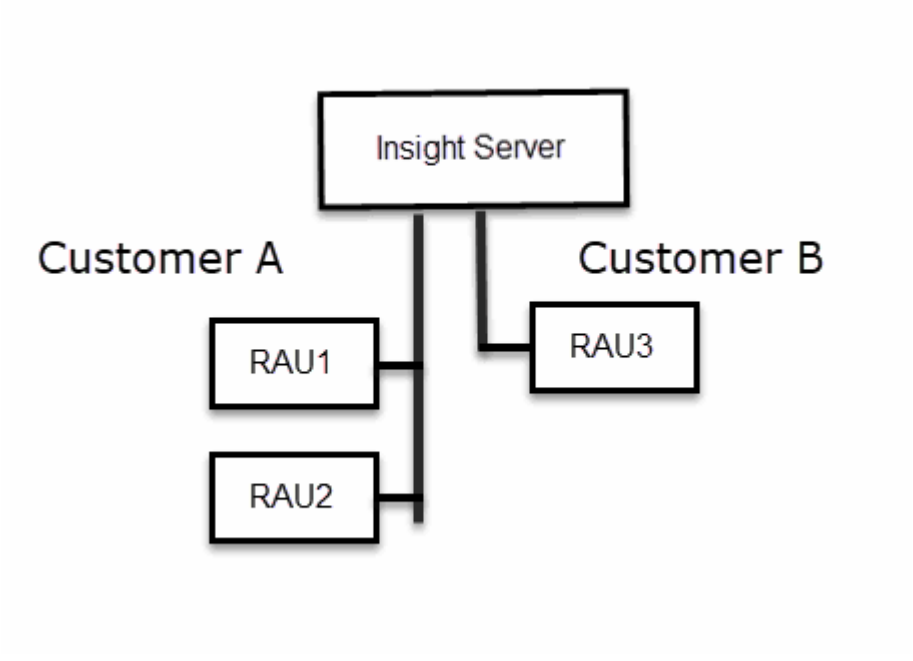
Consideraciones sobre la actualización y la instalación

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 SMPT.

- **Actualizar contraseña**

  Cambiar la contraseña de una cuenta de usuario específica.

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

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

+

- **Restablecer valores predeterminados**

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

- **Salida**

  Salga de la `securityadmin` herramienta.

Cambiar contraseñas de usuario interno de OnCommand Insight

Las directivas de seguridad pueden requerir cambiar las contraseñas en el entorno OnCommand Insight. Algunas de las contraseñas de un servidor existen en un servidor diferente del entorno, lo que requiere que cambie la contraseña en ambos servidores. Por ejemplo, al cambiar la contraseña de usuario de "'Inventory'" en Insight Server, debe coincidir con la contraseña de usuario "'Inventory'" en el conector del servidor del almacén de datos configurado para ese Insight Server.

Antes de empezar

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

Acerca de esta tarea

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

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

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

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

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

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

Contraseñas DE LAU	Cambios necesarios
adquisición	Insight Server, RAU

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

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

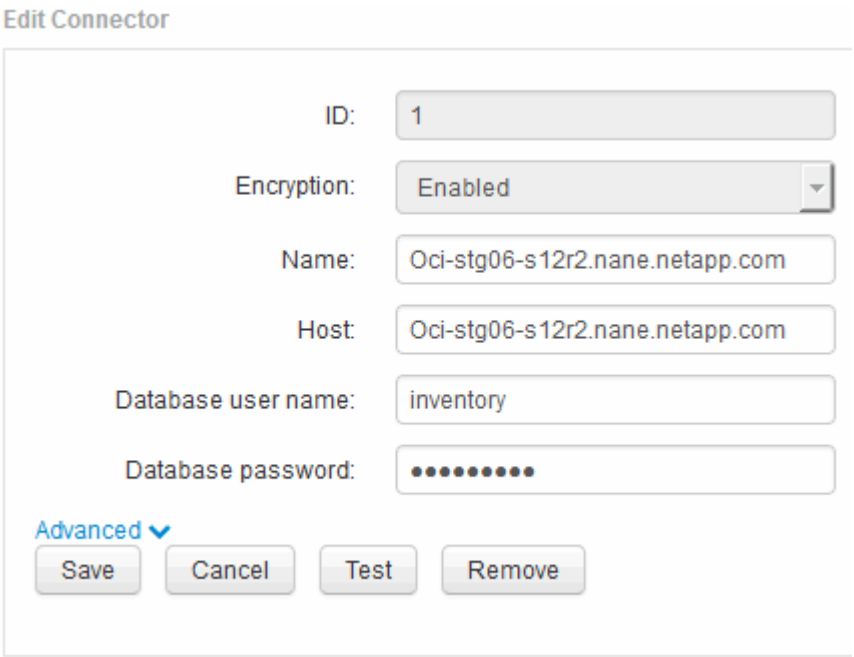
Antes de empezar

Debe iniciar sesión como administrador para realizar esta tarea.

Pasos

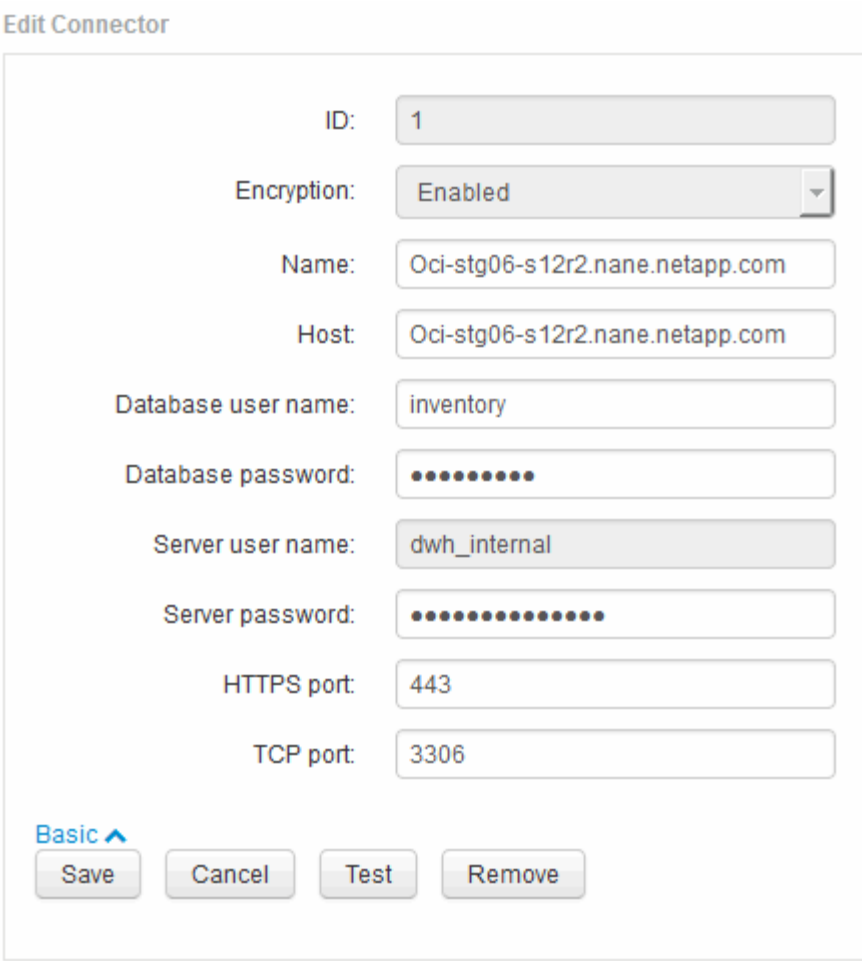
1. Inicie sesión en el portal del almacén de datos en https://hostname/dwh, Donde hostname es el nombre del sistema donde está instalado el almacén de datos OnCommand Insight.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

   Aparece la pantalla **Editar conector**.



3. Introduzca una nueva contraseña de "'Inventory'" para el campo **Contraseña de base de datos**.
4. Haga clic en **Guardar**
5. Para cambiar la contraseña "dwh_internal", haga clic en **Avanzado**

   Aparece la pantalla Editar conector avanzado.



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

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

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

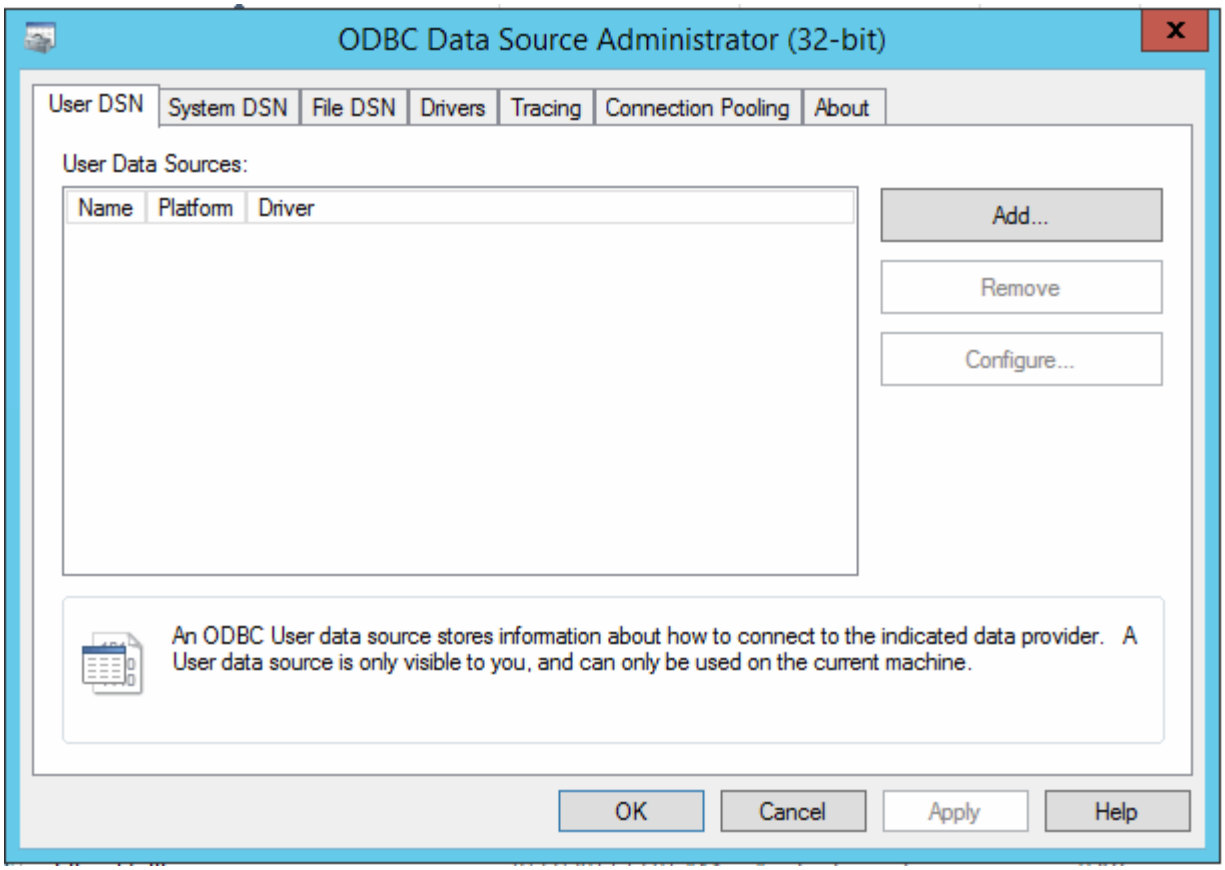
Antes de empezar

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

Pasos

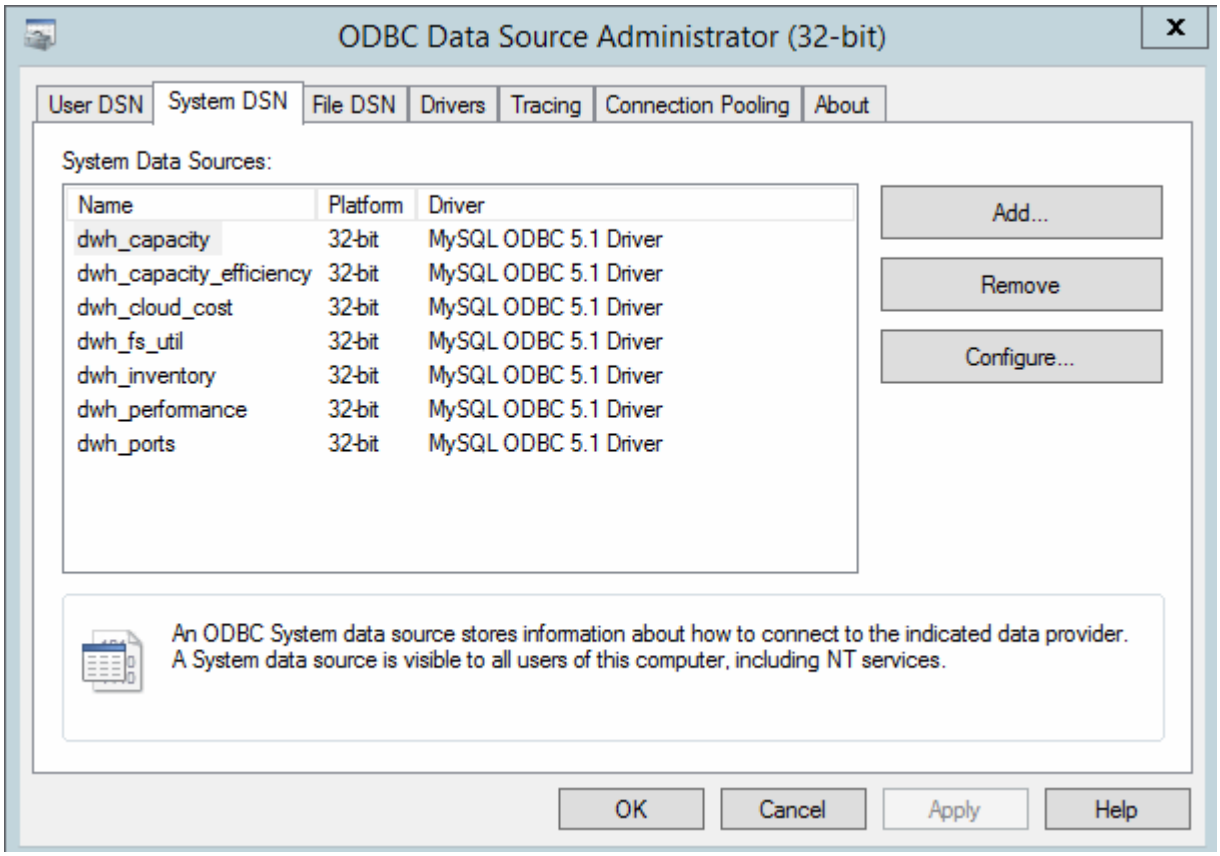
1. Realice un inicio de sesión remoto en el servidor que aloja ese almacén de datos.
2. Acceda a la herramienta de administración de ODBC en `C:\Windows\SysWOW64\odbcad32.exe`

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



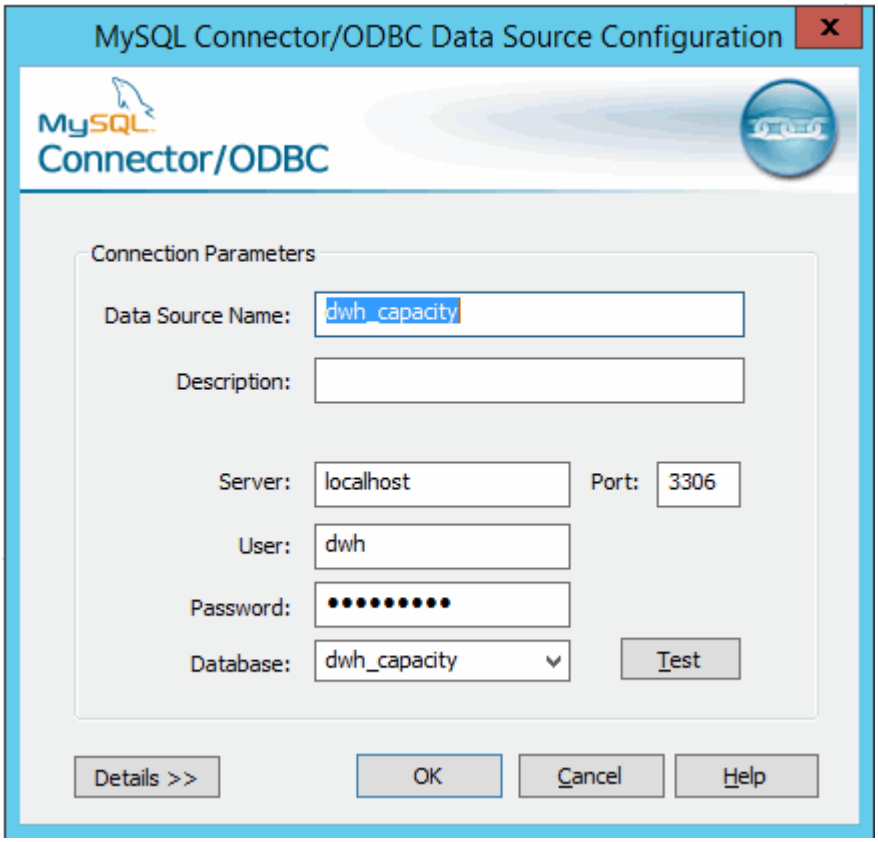
3. Haga clic en **DSN de sistema**

   Se muestran los orígenes de datos del sistema.



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

   Aparece la pantalla Configuración del origen de datos.



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

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 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"

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 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"

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. Fusionar 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 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

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 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"

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	<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 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"

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 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"

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 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANScreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   a. cd `"\Program Files\sanscreen\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 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. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y.. `..\SANScreen\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\sanscreen\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 subyectAltNames 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 l" 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"

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 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"

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	<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 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"

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 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"

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 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Crear una copia de seguridad de las carpetas «'certs'» y «'csk'» en `..\SANScreen\cognos\analytics\configuration`.
3. Genere una solicitud de cifrado de certificado desde Cognos. En una ventana Admin CMD, ejecute:
   a. cd "`\Program Files\sanscreen\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 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. Detenga Cognos utilizando la herramienta de configuración de IBM Cognos. Cierre Cognos.
2. Cree backups de `..\SANScreen\cognos\analytics\configuration` y.. `..\SANScreen\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\sanscreen\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 subyectAltNames 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 archivará 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.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 

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 Actions ▾. 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 Actions ▾ 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 dInsight 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 + Add 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 + Add.

   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 + Add 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 + 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**.
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 + Add.
   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> <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 [-uusername] [-ppassword]
[-aserver name or IP address] [-bbatch 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 More 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 Actions ▾ 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 Actions ▾ 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.

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.

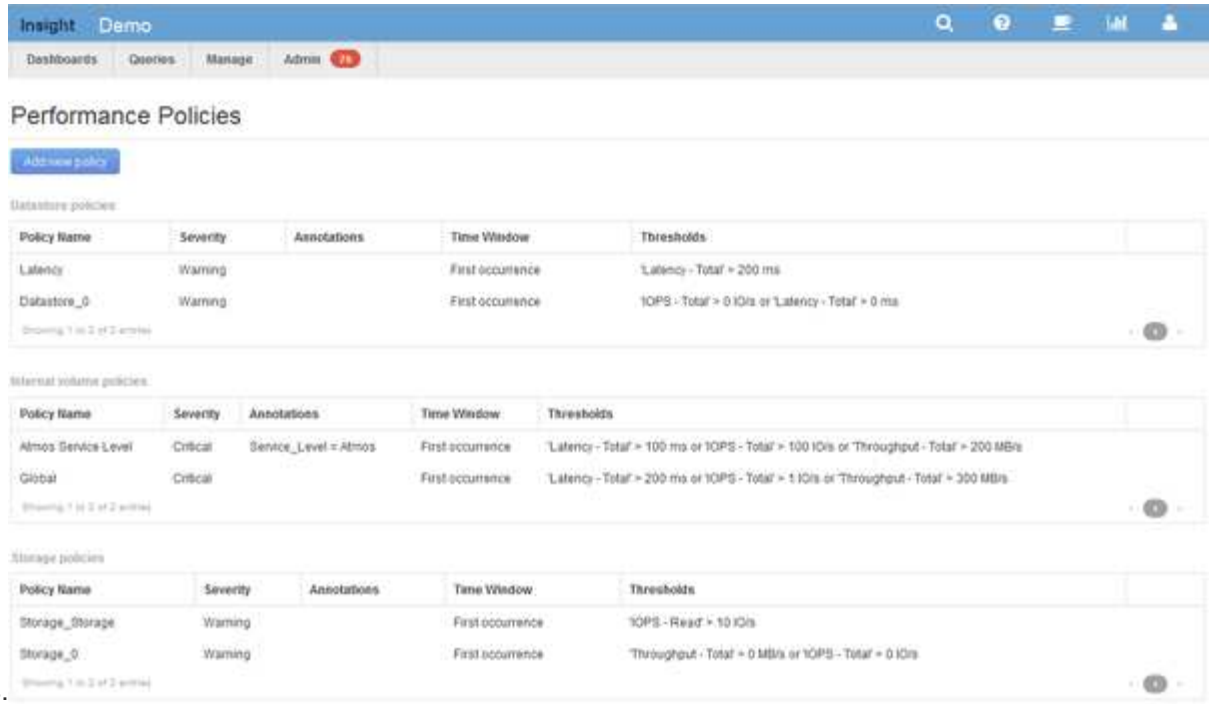
Crear políticas de rendimiento

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



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.

+