Finalización de las tareas posteriores a la actualización

OnCommand Insight

NetApp
April 01, 2024

This PDF was generated from https://docs.netapp.com/es-es/oncommand-insight/install-windows/installing-data-source-patches.html on April 01, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Finalización de las tareas posteriores a la actualización

Tras actualizar a la versión más reciente de Insight, debe completar las tareas adicionales.

Instalación de parches de origen de datos

Si procede, debe instalar los parches más recientes disponibles para los orígenes de datos para aprovechar las funciones y mejoras más recientes. Después de cargar un parche de origen de datos, puede instalarlo en todos los orígenes de datos del mismo tipo.

Antes de empezar

Debe haber contactado con el soporte técnico y obtener el `.zip` archivo que contiene las revisiones más recientes del origen de datos proporcionándoles la versión desde la que se está actualizando y la versión a la que desea actualizar.

Pasos

1. Coloque el archivo de revisión en el servidor de Insight.
2. En la barra de herramientas Insight, haga clic en **Admin**.
3. Haga clic en **parches**.
4. En el botón acciones, seleccione **aplicar parche**.
5. En el cuadro de diálogo **aplicar parche de origen de datos**, haga clic en **examinar** para localizar el archivo de parche cargado.
6. Revise los tipos de fuente de datos **Patch name**, **Description** y **impactados**.
7. Si el parche seleccionado es correcto, haga clic en **aplicar parche**.

   Con esta revisión se actualizan todos los orígenes de datos del mismo tipo. Insight obliga automáticamente a la adquisición a que se reinicie al agregar un origen de datos. La detección incluye la detección de cambios en la topología de red, incluida la adición o eliminación de nodos o interfaces.

8. Para forzar el proceso de detección manualmente, haga clic en **orígenes de datos** y haga clic en **sondeo de nuevo** junto al origen de datos para forzar la recopilación de datos inmediatamente.

   Si el origen de datos ya está en un proceso de adquisición, Insight ignora la solicitud de nuevo sondeo.

Reemplazar un certificado después de actualizar OnCommand Insight

Si se abre la interfaz de usuario web de OnCommand Insight después de una actualización, se genera una advertencia de certificación. Se muestra el mensaje de advertencia porque no hay un certificado autofirmado válido después de la actualización.

Para evitar que se muestre el mensaje de advertencia en el futuro, puede instalar un certificado autofirmado válido para reemplazar el certificado original.

Antes de empezar

El sistema debe satisfacer el nivel de bit de cifrado mínimo (1024 bits).

Acerca de esta tarea

La advertencia de certificación no afecta a la facilidad de uso del sistema. Cuando aparezca el mensaje, puede indicar que comprende el riesgo y, a continuación, proceder a utilizar Insight.

Pasos

1. 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"`

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

   Debe haber al menos un certificado en el almacén de claves, `ssl certificate`.

2. Elimine el `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Genere una nueva clave: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\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.

4. Generar un archivo de solicitud de certificado: `keytool -certreq -alias localhost -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.

5. Envíe el `c:\localhost.csr` Archivar a la entidad de certificación (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.

6. Importe el certificado aprobado: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

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

      El sistema muestra el siguiente mensaje: `Certificate reply was installed in keystore`

7. Reinicie el servicio del servidor SANscreen.

Resultados

El explorador web ya no informa sobre advertencias de certificados.

Aumentar la memoria de Cognos

Antes de restaurar la base de datos de Data Warehouse, debe aumentar la asignación de Java para Cognos de 768 MB a 2048 MB para reducir el tiempo de generación de informes.

Pasos

1. Abra una ventana de símbolo del sistema como administrador en el servidor de almacén de datos.
2. Desplácese hasta la `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directorio.
3. Escriba el siguiente comando: `cogconfigw`

   Aparece la ventana IBM Cognos Configuration.

> La aplicación de acceso directo de IBM Cognos Configuration apunta a. `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Si Insight está instalado en el directorio Archivos de programa (espacio entre), que es el valor predeterminado, en lugar de Archivos de programa (sin espacio), el `.bat` el archivo no funciona. Si esto ocurre, haga clic con el botón secundario del ratón en el acceso directo de la aplicación y cambie `cognosconfigw.bat` para `cognosconfig.exe` para corregir el acceso directo.

4. Desde el panel de navegación de la izquierda, expanda **entorno**, amplíe **IBM Cognos Services** y, a continuación, haga clic en **IBM Cognos**.
5. Seleccione **memoria máxima para Tomcat en MB** y cambie de 768 MB a 2048 MB.
6. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Guardar).

   Aparece un mensaje informativo para informarle de las tareas que Cognos está realizando.

7. Haga clic en **Cerrar**.
8. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Parada).
9. En la barra de herramientas de IBM Cognos Configuration, haga clic en (Iniciar).

Restauración de la base de datos del almacén de datos

Cuando realiza una copia de seguridad de la base de datos de Data Warehouse, Data Warehouse crea un `.zip` archivo que se puede usar más adelante para restaurar esa misma base de datos.

Acerca de esta tarea

Al restaurar la base de datos del almacén de datos, también puede restaurar la información de la cuenta de usuario desde la copia de seguridad. El motor de informes de Data Warehouse utiliza las tablas de administración de usuarios en una instalación sólo de Data Warehouse.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **copia de seguridad/Restaurar**.
3. En la sección **Restaurar base de datos e informes**, haga clic en **examinar** y busque `.zip` Archivo que contiene la copia de seguridad del almacén de datos.
4. Se recomienda dejar seleccionadas las dos opciones siguientes:
   - **Restaurar base de datos**

     Incluye la configuración del almacén de datos, los marts de datos, las conexiones y la información de la cuenta de usuario.

   - **Restaurar informes**

     Incluye informes personalizados, informes diseñados previamente, cambios en los informes diseñados previamente y configuración de informes realizada en Conexión de informes.

5. Haga clic en **Restaurar**.

   No salga del estado de restauración. Si lo hace, el estado de la restauración ya no aparecerá y no recibirá ninguna indicación cuando finalice la operación de restauración.

6. Para comprobar el proceso de actualización, consulte `dwh_upgrade.log` archivo, que se encuentra en la siguiente ubicación: `<install directory>\SANscreen\wildfly\standalone\log`.

   Cuando finalice el proceso de restauración, aparecerá un mensaje justo debajo del botón **Restaurar**. Si el

proceso de restauración se realiza correctamente, el mensaje indica que el proceso se ha realizado correctamente. Si el proceso de restauración falla, el mensaje indica la excepción específica que se produjo en ese caso. En este caso, póngase en contacto con el soporte técnico y entrételas `dwh_upgrade.log` archivo. Si se produce una excepción y la operación de restauración falla, la base de datos original se restablece automáticamente.

> Si la operación de restauración falla con un mensaje "'error al actualizar cognos content store'", restaure la base de datos de Data Warehouse sin sus informes (sólo base de datos) y utilice las copias de seguridad de informes XML para importar sus informes.

Restaurar informes personalizados de almacén de datos

Si procede, puede restaurar manualmente todos los informes personalizados de los que ha realizado la copia de seguridad antes de la actualización; sin embargo, sólo tendrá que hacerlo si pierde los informes si se han dañado.

Pasos

1. Abra el informe con un editor de texto y, a continuación, seleccione y copie su contenido.
2. Inicie sesión en el portal de informes en `https://fqdn/reporting`.
3. En la barra de herramientas almacén de datos, haga clic en Para abrir el portal de Insight Reporting.
4. En el menú Inicio, seleccione **Report Studio**.
5. Seleccione cualquier paquete.

   Aparecerá Report Studio.

6. Haga clic en **Crear nuevo**.
7. Seleccione **Lista**.
8. En el menú Herramientas, seleccione **Abrir informe desde Portapapeles**.

   Aparece el cuadro de diálogo **Abrir informe desde el Portapapeles**.

9. En el menú Archivo, seleccione **Guardar como** y guarde el informe en la carpeta Informes personalizados.
10. Abra el informe para verificar que se ha importado.

    Repita esta tarea para cada informe.

> Al cargar un informe, puede aparecer un "'error de análisis de expresión'". Esto significa que la consulta contiene una referencia al menos a un objeto que no existe, lo que significa que no hay ningún paquete seleccionado en la ventana origen para validar el informe. En este caso, haga clic con el botón derecho del ratón en una dimensión de data Mart en la ventana origen, seleccione paquete de informe, A continuación, seleccione el paquete asociado con el informe (por ejemplo, el paquete de inventario si se trata de un informe de inventario o uno de los paquetes de rendimiento si es un informe de rendimiento) para que Report Studio pueda validarlo y, a continuación, guardarlo.

Verificación de que el almacén de datos tiene datos históricos

Después de restaurar los informes personalizados, debe comprobar que Data Warehouse recopila datos históricos mediante la visualización de los informes personalizados.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En la barra de herramientas almacén de datos, haga clic en Para abrir el portal de Insight Reporting e iniciar sesión.
3. Abra la carpeta que contiene los informes personalizados (por ejemplo, Informes personalizados).
4. Haga clic en para abrir las opciones de formato de salida de este informe.
5. Seleccione las opciones que desee y haga clic en **Ejecutar** para asegurarse de que están rellenadas con datos históricos de almacenamiento, computación y cambio.

Restaurar el archivado de rendimiento

En el caso de sistemas que archivan el rendimiento, el proceso de actualización solo restaura siete días de datos archivados. Puede restaurar los datos de archivado restantes después de que se haya competido la actualización.

Acerca de esta tarea

Para restaurar el archivo de rendimiento, siga estos pasos.

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.

Comprobación de los conectores

Después de actualizar, desea probar los conectores para asegurarse de que tiene una conexión del almacén de datos OnCommand Insight al servidor OnCommand Insight.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **conectores**.

3. Seleccione el primer conector.

   Aparece la página Editar conector.

4. Haga clic en **Prueba**.
5. Si la prueba es correcta, haga clic en **Cerrar**; si falla, escriba el nombre del servidor Insight en el campo **Nombre** y su dirección IP en el campo **Host** y haga clic en **Prueba**.
6. Cuando haya una conexión correcta entre el almacén de datos y el servidor de Insight, haga clic en **Guardar**.

   Si no se realiza correctamente, compruebe la configuración de la conexión y asegúrese de que el servidor Insight no tiene ningún problema.

7. Haga clic en **Prueba**.

   Data Warehouse prueba la conexión.

Verificación de la programación de extraer, transformar y cargar

Después de actualizar, debe asegurarse de que el proceso extraer, transformar y cargar (ETL) está recuperando datos de las bases de datos OnCommand Insight, transformando los datos y guardarlos en los data marts.

Pasos

1. Inicie sesión en el portal del almacén de datos en `https://fqdn/dwh`.
2. En el panel de navegación de la izquierda, haga clic en **Programación**.
3. Haga clic en **Editar horario**.
4. Seleccione **Diario** o **Semanal** en la lista **Tipo**.

   Se recomienda programar ETL para que se ejecute una vez al día.

5. Compruebe que la hora seleccionada es la hora en la que desea que se ejecute el trabajo.

   Esto garantiza que el trabajo de generación se ejecute automáticamente.

6. Haga clic en **Guardar**.

Actualizar los modelos de disco

Después de la actualización, debe tener cualquier modelo de disco actualizado; sin embargo, si por algún motivo Insight no pudo detectar nuevos modelos de disco, puede actualizarlos manualmente.

Antes de empezar

Debe haber obtenido del soporte técnico de `.zip` archivo que contiene los parches más recientes del origen

de datos.

Pasos

1. Detenga el servicio Acq SANscreen.
2. Desplácese al siguiente directorio: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Mueva el movimiento actual `diskmodels.jar` archivo en una ubicación diferente.
4. Copie el nuevo `diskmodels.jar` en la `datasources.war` directorio.
5. Inicie el servicio Acq SANscreen.

Verificación de que se están ejecutando las herramientas de inteligencia empresarial

Si procede, debe verificar que las herramientas de inteligencia empresarial están en ejecución y recuperando los datos después de la actualización.

Compruebe que las herramientas de inteligencia empresarial como BMC Atrium y ServiceNow se ejecutan y pueden recuperar los datos. Esto incluye el conector BMC y soluciones que aprovechan REST.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.