



Actualizar OnCommand Insight

OnCommand Insight

NetApp
April 02, 2025

This PDF was generated from <https://docs.netapp.com/es-es/oncommand-insight/install-windows/upgrading-insight-to-version-7-3-12-or-later-windows.html> on April 02, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

| | |
|--|----|
| Actualizar OnCommand Insight | 1 |
| Actualización de Insight a la versión 7.3.12 o posterior: Windows | 1 |
| Información previa | 1 |
| ¿Qué hace la herramienta de migración de datos? | 1 |
| Antes de empezar | 1 |
| Ejecución de la herramienta de migración de datos | 1 |
| Errores de validación | 3 |
| Opciones de línea de comandos | 4 |
| Descripción general del proceso de actualización de OnCommand Insight | 5 |
| Lista de comprobación de actualización de OnCommand Insight | 6 |
| Descargue los paquetes de instalación de OnCommand Insight | 10 |
| Acerca de esta tarea | 10 |
| Pasos | 10 |
| Realizar un backup de las bases de datos | 11 |
| Copia de seguridad de la base de datos del almacén de datos | 11 |
| Realizar un backup de la base de datos de OnCommand Insight | 14 |
| Realizar una copia de seguridad de la configuración de seguridad | 15 |
| Acerca de esta tarea | 15 |
| Realizar copias de seguridad de informes personalizados de Data Warehouse | 15 |
| Pasos | 15 |
| Realizando la actualización de software | 15 |
| Renovar Insight | 16 |
| Actualizando almacén de datos | 16 |
| Actualización de servidores de unidades de adquisición remotas | 17 |
| Finalización de las tareas posteriores a la actualización | 18 |
| Instalación de parches de origen de datos | 18 |
| Reemplazar un certificado después de actualizar OnCommand Insight | 19 |
| Aumentar la memoria de Cognos | 21 |
| Restauración de la base de datos del almacén de datos | 22 |
| Restaurar informes personalizados de almacén de datos | 23 |
| Verificación de que el almacén de datos tiene datos históricos | 23 |
| Restaurar el archivado de rendimiento | 24 |
| Comprobación de los conectores | 24 |
| Verificación de la programación de extraer, transformar y cargar | 25 |
| Actualizar los modelos de disco | 25 |
| Verificación de que se están ejecutando las herramientas de inteligencia empresarial | 25 |
| Solucionar problemas de una actualización | 26 |
| No se puede iniciar Cognos desde el menú Inicio de Windows | 26 |
| "no es una aplicación win32 válida" mensaje de error | 26 |
| Las anotaciones no están presentes | 26 |
| Diferencias en los valores mostrados en los informes | 26 |
| Los datos no se muestran en los informes | 26 |

Actualizar OnCommand Insight

Normalmente, se debe realizar una actualización en todos los servidores Insight (servidor Insight, servidor de Data Warehouse, unidad de adquisición remota). Siempre debería consultar las notas de la versión para conocer los requisitos de actualización de una versión nueva de OnCommand Insight.

A menos que se indique lo contrario, los requisitos y procedimientos se aplican a la actualización de Insight 7.x a la versión actual de Insight. Si va a actualizar desde una versión anterior a la 7.0, póngase en contacto con su representante de cuenta.

Actualización de Insight a la versión 7.3.12 o posterior: Windows

Antes de actualizar OnCommand Insight 7.3.10 - 7.3.11 a la versión 7.3.12 o posterior, debe ejecutar la herramienta de migración de datos OCI.

Información previa

Las versiones 7.3.12 y posteriores de OnCommand Insight utilizan software subyacente que puede ser incompatible con versiones anteriores. Las versiones 7.3.12 y posteriores de Insight incluyen una **herramienta de migración de datos** para facilitar la actualización.



Ya no son compatibles las versiones 7.3.9 y anteriores de OnCommand Insight. Si ejecuta una de estas versiones, *debe* actualizar a Insight versión 7.3.10 o posterior (se recomienda encarecidamente utilizar la versión 7.3.11) antes de actualizar a la versión 7.3.12 o posterior.

¿Qué hace la herramienta de migración de datos?

La herramienta de migración realiza una comprobación de compatibilidad inicial y, a continuación, sigue una de las tres rutas de actualización diferentes. La ruta seleccionada se basa en la compatibilidad de los datos de la versión actual.



Antes de la actualización, debe ejecutar la herramienta de migración de datos y seguir los pasos recomendados.

Antes de empezar

- Se recomienda encarecidamente realizar una copia de seguridad del sistema OnCommand Insight antes de ejecutar la herramienta de migración de datos.
- Es necesario que el servicio Elasticsearch en el servidor esté en funcionamiento.
- La herramienta de migración de datos *debe* ejecutarse en la base de datos y en cualquier archivo de rendimiento antes de actualizar Insight.

Ejecución de la herramienta de migración de datos

1. Descargue la última versión de la herramienta de migración de datos (por ejemplo, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) en su servidor Insight, así como el archivo de instalación

de Insight correspondiente. Descomprima en una carpeta de trabajo. Las descargas se pueden encontrar en "[Sitio de soporte de NetApp](#)".

2. Abra una ventana de comandos y vaya a la carpeta de trabajo.
 - Abra PowerShell como administrador.
3. Ejecute la herramienta de migración de datos usando el siguiente comando:
 - `'.\SANSscreenDataMigrationTool.ps1'`
4. Siga las instrucciones según sea necesario. A continuación se muestra un ejemplo.

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
    the most recent of which is for 2021-05-13

Verifying migration component is present...
SANSscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

La herramienta de migración de datos comprobará la presencia de índices obsoletos en el sistema e informará si hay alguno. Si no hay ninguno, la herramienta se cerrará.

Es posible migrar algunos índices mientras se ejecuta el servicio de servidor SANSscreen. Es posible que otros sólo se migren cuando se detenga el servidor. Si no hay índices que puedan migrarse, la herramienta se cerrará. De lo contrario, siga las instrucciones que se le indiquen.

Una vez completada la herramienta de migración de datos, volverá a comprobar si hay índices obsoletos. Si se han migrado todos los índices, la herramienta le informará de que la actualización a OnCommand Insight 7.3.12 es compatible. Ya puede continuar con la actualización de Insight.

```

.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-127

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory: D:\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 5 obsolete indexes. Of these,
    5 indexes need to be migrated with OCI server stopped

Verifying migration component is present...
SANSscreen Server service is Stopped

Proceed with offline migration of 5 indexes (y or [n])?: y
Preparing to perform migration...
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;
backup; delete old; restore new; cleanup; done.
Execution time 0:00:15

Checking for obsolete (version 5) indexes...
No obsolete indexes found. Upgrade to 7.3.12+ is supported.

C:\Users\root\Desktop\SANSscreenDataMigrationTool-x64-7.3.12-127>

```

Si se le solicita que detenga el servicio SANSscreen, reinicie antes de actualizar Insight.

Errores de validación

En caso de que falle la validación de índices, la herramienta de migración le informará del problema antes de salir.

OnCommand Insight no está presente:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

Versión de Insight no válida:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

El servicio Elasticsearch no se está ejecutando:

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

Opciones de línea de comandos

La herramienta de migración de datos incluye algunos parámetros opcionales que afectan a su funcionamiento.

| Opción (Windows) | Función |
|------------------|--|
| -s. | Suprimir todas las indicaciones |
| -perf_archive | <p>Si se especifica, se reemplazarán las entradas de archivo existentes para cualquier fecha cuyos índices se migran. La ruta de acceso debe apuntar al directorio que contiene los archivos zip de la entrada de archivo.</p> <p>Se puede especificar un argumento de '-' para indicar que no hay ningún archivo de rendimiento que se va a actualizar.</p> <p>Si este argumento está presente, se suprimirá la petición de ubicación de archivado.</p> |
| -comprobar | Si está presente, el script se cerrará inmediatamente después de informar de los recuentos de índices. |
| -drirrun | Si está presente, el ejecutable de migración informará de las acciones que se realizarían (para migrar datos y actualizar entradas de archivo) pero no realizará las operaciones. |

Descripción general del proceso de actualización de OnCommand Insight

Antes de comenzar a actualizar Insight, es importante comprender el proceso de actualización. El proceso de actualización es el mismo para la mayoría de las versiones de Insight.



Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información.

El proceso de actualización de Insight incluye las siguientes tareas de alto nivel:

- Descarga de los paquetes de instalación
- Copia de seguridad de la base de datos del almacén de datos

Para evitar la posibilidad de informar de forma errónea de los datos, debe realizar una copia de seguridad de la base de datos de Data Warehouse antes de realizar una copia de seguridad de la base de datos de Insight.

- Realizar backups de la base de datos de Insight

Se realiza automáticamente un backup de la base de datos de Insight cuando se realiza una actualización sin movimiento. Se recomienda realizar una copia de seguridad de la base de datos antes de la actualización y colocar la copia de seguridad en una ubicación distinta a la del servidor de Insight. Durante

el proceso de actualización, Insight no recopila datos nuevos. Para minimizar la cantidad de datos que no se recopilan, debe iniciar el backup de base de datos en una hora o dos del tiempo de actualización planificado.

- Realice una copia de seguridad de la configuración de seguridad almacén de datos y Unidad de adquisición remota si la configuración se ha cambiado de la configuración predeterminada.

La configuración de seguridad no predeterminada se debe restaurar en el servidor de depósito de datos y RAU una vez finalizada la actualización y antes de restaurar la base de datos de almacén de datos en el sistema.

- Realizar una copia de seguridad de los informes personalizados de Data Warehouse

Al realizar una copia de seguridad de la base de datos de Data Warehouse, se incluyen informes personalizados. El archivo de copia de seguridad se crea en el servidor de almacén de datos. Se recomienda realizar una copia de seguridad de los informes personalizados en una ubicación distinta a la del servidor de almacén de datos.

- Desinstalar el almacén de datos y el software de la unidad de adquisición remota, si procede

El servidor de Insight tiene una actualización in situ; no es necesario desinstalar el software. La actualización in situ realiza backups de la base de datos, desinstala el software, instala la nueva versión y, a continuación, restaura la base de datos.

- Actualización del software en el servidor de Insight, el almacén de datos y las unidades de adquisición remota

Todas las licencias anteriormente aplicadas permanecen en el registro; no tiene que volver a aplicar estas licencias.

- Completar las tareas posteriores a la actualización

Lista de comprobación de actualización de OnCommand Insight

Se pueden usar las listas de comprobación proporcionadas para registrar el progreso cuando se prepara la actualización. Estas tareas tienen por objeto ayudar a mitigar el riesgo de que se produzcan fallos en la actualización y agilizar los esfuerzos de recuperación y restauración.

Lista de comprobación para preparar la actualización (obligatorio)



Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información.

| Condición | Completo |
|--|----------|
| Asegúrese de que dispone de permisos de administrador local de Windows, necesarios para realizar el proceso de actualización, en todos los servidores Insight. | |

| | |
|--|--|
| Si los servidores de Insight, Data Warehouse o Remote Acquisition Unit residen en plataformas de 32 bits, debe actualizar sus servidores a plataformas de 64 bits. A partir de Insight 7.x, las actualizaciones solo están disponibles para plataformas de 64 bits. | |
| <p>Asegúrese de que dispone de los permisos necesarios para modificar o deshabilitar el software antivirus en todos los servidores de su entorno. Para evitar un error de actualización debido al software de análisis antivirus activo, debe excluir el directorio de instalación de Insight (disk drive:\install directory\sanscreen desde el acceso al análisis antivirus durante la actualización. Después de actualizar todos los componentes, puede reactivar el software antivirus de forma segura; no obstante, asegúrese de configurar el análisis para que siga excluyéndose todo en el directorio de instalación de Insight.</p> <p>Además, debe excluir la carpeta IBM/DB2 (por ejemplo, C:\Archivos de programa\IBM\DB2) de la exploración antivirus tras la instalación.</p> | |

Lista de comprobación para preparar la actualización (mejores prácticas)

| Condición | Completo |
|---|----------|
| Planifique cuándo va a realizar la actualización, teniendo en cuenta que la mayoría de las actualizaciones requieren un mínimo de 4 a 8 horas; las empresas de mayor tamaño tomarán más tiempo. Los tiempos de actualización pueden variar en función de los recursos disponibles (arquitectura, CPU y memoria), el tamaño de las bases de datos y la cantidad de objetos supervisados en el entorno. | |
| Póngase en contacto con su representante de cuenta para obtener información sobre sus planes de actualización, proporcionar la versión de Insight que ha instalado y la versión a la que desea actualizar. | |
| Asegúrese de que los recursos actuales asignados a las unidades de Insight, almacén de datos y adquisición remota siguen cumpliendo las especificaciones recomendadas. Consulte las directrices de configuración recomendadas para todos los servidores. también puede ponerse en contacto con el representante de su cuenta para analizar las directrices de configuración. | |

| | |
|---|--|
| <p>Asegúrese de tener suficiente espacio en disco para el proceso de backup y restauración de base de datos. Los procesos de backup y restauración requieren aproximadamente cinco veces el espacio en disco utilizado por el archivo de copia de seguridad en los servidores de Insight y almacén de datos. Por ejemplo, un backup de 50 GB requiere de 250 a 300 GB de espacio libre en disco.</p> | |
| <p>Asegúrese de tener acceso a Firefox® o al navegador Chrome™ cuando realice una copia de seguridad de las bases de datos de Insight y Data Warehouse. No se recomienda Internet Explorer porque experimenta algunos problemas al cargar y descargar archivos de más de 4 GB.</p> | |
| <p>Elimine el .tmp Archivos en el servidor de Insight que se pueden encontrar en la siguiente ubicación: <install directory>\SANscreen\wildfly\standalone \tmp.</p> | |
| <p>Elimine orígenes de datos duplicados y retire los orígenes de datos fuera de servicio del cliente Insight. La eliminación de los orígenes de datos duplicados o retirados del servicio disminuye la cantidad de tiempo necesaria para realizar la actualización y mitiga la oportunidad de daños en los datos.</p> | |
| <p>Si ha modificado alguno de los informes predeterminados enviados con Insight, debe guardar los informes con otro nombre y, a continuación, guardarlos en la carpeta Informes de clientes para que no pierda el informe modificado al actualizar o restaurar el sistema.</p> | |
| <p>Si tiene informes personalizados o modificados de almacén de datos creados por usted o por servicios profesionales, cree una copia de seguridad de ellos exportándolos a XML y, a continuación, moviéndolos a la carpeta Informes de clientes. Asegúrese de que la copia de seguridad no se encuentra en el servidor de almacén de datos. Si no mueve los informes a las carpetas recomendadas, es posible que el proceso de actualización no realice el backup de estos informes. En versiones anteriores de Insight, si no se localizan los informes en las carpetas adecuadas, se podrían perder informes personalizados y modificados.</p> | |

| | |
|--|--|
| <p>Registre todos los ajustes en la utilidad de configuración de IBM Cognos, ya que no están incluidos en la copia de seguridad de Data Warehouse; debe reconfigurar estos ajustes después de la actualización. La utilidad se encuentra en <code>disk drive:\install directory\SANscreen\cognos\c10_64\bin64</code> directorio en el servidor de almacén de datos y lo ejecuta mediante <code>cogconfigw</code> Command.alternativamente, puede realizar una copia de seguridad completa de Cognos y, a continuación, importar toda su configuración. Consulte la documentación de IBM Cognos para obtener más información.</p> | |
|--|--|

Lista de comprobación para preparar la actualización (si procede)

| Condición | Completo |
|--|----------|
| <p>Si sustituyó los certificados autofirmados que creó la instalación de Insight debido a las advertencias de seguridad del explorador con certificados firmados por la autoridad de certificación interna, realice un backup del archivo keystore, que se encuentra en la siguiente ubicación: <code>disk drive:\install directory\SANscreen\wildfly\standalone\configuration</code> y restáurelo después de la actualización. Esto reemplaza los certificados autofirmados que Insight crea con los certificados firmados.</p> | |
| <p>Si se modificó alguno de sus orígenes de datos para su entorno y no está seguro de si estas modificaciones están disponibles en la versión de Insight a la que va a actualizar, realice una copia del siguiente directorio, que le ayudará a solucionar problemas de recuperación: <code>disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war</code>.</p> | |
| <p>Realice una copia de seguridad de todas las tablas y vistas de la base de datos personalizadas mediante <code>mysqldump</code> Herramienta de línea de comandos.la restauración de tablas de base de datos personalizadas requiere un acceso privilegiado a la base de datos. Póngase en contacto con el soporte técnico para obtener ayuda con la restauración de estas tablas.</p> | |

Asegúrese de que no existan scripts de integración personalizados, componentes de terceros necesarios para los orígenes de datos de Insight, backups o cualquier otro dato requerido en el disk drive:\install directory\sansscreen directorio, porque el proceso de actualización elimina el contenido de este directorio. Asegúrese de mover cualquiera de estas cosas del \sansscreen directorio en otra ubicación. Por ejemplo, si el entorno contiene scripts de integración personalizados, asegúrese de copiar el siguiente archivo en un directorio distinto del \sansscreen directorio:

```
\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt.
```

Descargue los paquetes de instalación de OnCommand Insight

Debe descargar los paquetes de instalación de Insight, almacén de datos y la unidad de adquisición remota (si corresponde) antes del día que elija actualizar. Tiempos de descarga de los paquetes (.msi ficheros) varían en función del ancho de banda disponible.

Acerca de esta tarea

Es posible descargar los paquetes de instalación mediante la interfaz de usuario web de Insight o mediante el enlace OnCommand Insight correspondiente desde <http://support.netapp.com/NOW/cgi-bin/software>.

Para descargar el paquete de instalación desde el servidor de Insight, haga lo siguiente:

Pasos

1. Abra la interfaz de usuario web de Insight abriendo un navegador web e introduciendo una de las siguientes opciones:
 - En el servidor de Insight: `https://localhost`
 - Desde cualquier ubicación: `https://IP Address:port` or `fqdn:port`

El número de puerto es 443 o el puerto que se configuró al instalar el servidor Insight. El número de puerto predeterminado es 443 si no se especifica el número de puerto en la URL.

2. Inicie sesión en Insight.
3. Haga clic en el icono Ayuda y seleccione **Buscar actualizaciones**.
4. Si se detecta una versión más reciente, siga las instrucciones del cuadro de mensaje.

Se llevará a la página InsightDescription de la nueva versión.

5. En la página **Descripción**, haga clic en **continuar**.
6. Cuando aparezca el contrato de licencia para usuario final (EULA), haga clic en **Aceptar**.
7. Haga clic en el enlace del paquete de instalación de cada componente (servidor Insight, almacén de datos, unidad de adquisición remota), etc.) y haga clic en **Guardar como** para guardar el paquete de instalación.

Antes de realizar la actualización, debe asegurarse de copiar los paquetes de instalación de Data Warehouse y Remote Acquisition Unit en discos locales en sus respectivos servidores.

8. Haga clic en **SUMA de COMPROBACIÓN** y anote los valores numéricos asociados con cada paquete de instalación.
9. Compruebe que los paquetes de instalación están completos y que no se han producido errores después de descargarlos.

Las transferencias de archivos incompletas pueden causar problemas en el proceso de actualización.

Para generar valores hash MD5 para los paquetes de instalación, puede utilizar una utilidad de terceros como la de Microsoft "[Verificador de integridad de archivo](#)" utilidad.

Realizar un backup de las bases de datos

Antes de actualizar, debe realizar una copia de seguridad de las bases de datos de Data Warehouse y OnCommand Insight. La actualización requiere una copia de seguridad de la base de datos de Data Warehouse para que pueda restaurar la base de datos más adelante en el proceso de actualización. La actualización in situ de Insight realiza un backup de la base de datos; sin embargo, debe realizar un backup de la base de datos antes de la actualización como práctica recomendada.



Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información.

Para evitar que los datos no se informen correctamente, debe realizar una copia de seguridad de la base de datos de Data Warehouse antes de realizar una copia de seguridad de la base de datos de Insight. Además, si tiene un entorno de prueba, se recomienda asegurarse de poder restaurar el backup antes de continuar con la actualización.

Copia de seguridad de la base de datos del almacén de datos

Puede realizar una copia de seguridad de la base de datos de Data Warehouse, que también incluye una copia de seguridad de Cognos, en un archivo y, posteriormente, restaurarla mediante el portal Data Warehouse. Dicha copia de seguridad le permite migrar a un servidor de Data Warehouse diferente o actualizar a una nueva versión 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, seleccione **copia de seguridad/Restaurar**.
3. Haga clic en **copia de seguridad** y seleccione su configuración de copia de seguridad:
 - a. Todos los Datamarts excepto Performance Datamart
 - b. Todos los Datamarts

Esta operación puede tardar 30 minutos o más.

+ almacén de datos crea un archivo de copia de seguridad y muestra su nombre.

4. Haga clic con el botón derecho del ratón en el archivo de copia de seguridad y guárdelo en la ubicación que desee.

Puede que no desee cambiar el nombre del archivo; sin embargo, debe almacenar el archivo fuera de la ruta de instalación del almacén de datos.

El archivo de copia de seguridad de Data Warehouse incluye MySQL de la instancia DWH; esquemas personalizados (MySQL DBS) y tablas; configuración LDAP; los orígenes de datos que conectan Cognos a la base de datos MySQL (no los orígenes de datos que conectan el servidor Insight a los dispositivos para adquirir datos); importar y exportar tareas que importaron o exportaron informes; informar de funciones de seguridad, grupos y espacios de nombres; cuentas de usuario; Cualquier informe modificado del Portal de informes y cualquier informe personalizado, independientemente del lugar donde se almacenen, incluso en el directorio Mis carpetas. No se realiza una copia de seguridad de los parámetros de configuración del sistema Cognos, como la configuración del servidor SMTP y la configuración de memoria personalizada Cognos.

Los esquemas predeterminados en los que se realiza una copia de seguridad de las tablas personalizadas incluyen los siguientes:

| |
|---------------------------|
| dwh_capacity |
| dwh_capacity_staging |
| dwh_dimensions |
| dwh_fs_util |
| dwh_inventory |
| dwh_inventory_staging |
| dwh_inventory_transitorio |
| dwh_management |
| dwh_performance |
| dwh_performance_staging |

| |
|----------------|
| dwh_ports |
| dwh_reports |
| dwh_sa_staging |
| |
| |
| |

Entre los esquemas en los que se excluyen las tablas personalizadas de la copia de seguridad se incluyen los siguientes:

| |
|------------------------|
| esquema_de_información |
| adquisición |
| modelo_cloud |
| datos_host |
| innodb |
| inventario |
| inventory_private |
| hora_inventario |
| registros |
| gestión |
| mysql |
| nas |
| rendimiento |
| esquema_rendimiento |
| performance_views |
| SANscreen |
| frote |

| |
|----------------------|
| garantía de servicio |
| prueba |
| tmp |
| banco de trabajo |
| |
| |
| |
| |

En cualquier backup iniciado manualmente, un `.zip` se crea un archivo que contiene los siguientes archivos:

- Un backup diario `.zip` Archivo, que contiene definiciones de informe de Cognos
- Una copia de seguridad de informes `.zip` Archivo, que contiene todos los informes en Cognos, incluidos los del directorio Mis carpetas
- Un archivo de copia de seguridad de la base de datos de Data Warehouse además de copias de seguridad manuales, que puede realizar en cualquier momento, Cognos crea una copia de seguridad diaria (generada automáticamente cada día a un archivo llamado `DailyBackup.zip`) que incluye las definiciones de informe. La copia de seguridad diaria incluye las carpetas y paquetes principales que se suministran con el producto. El directorio Mis carpetas y cualquier directorio que cree fuera de las carpetas superiores del producto no están incluidos en la copia de seguridad de Cognos.



Debido a la forma en que Insight nombra los archivos en `.zip` archivo, algunos programas de descompresión muestran que el archivo está vacío al abrirse. Siempre que la `.zip` el archivo tiene un tamaño mayor que 0 y no termina con un `.bad` extensión, la `.zip` el archivo es válido. Puede abrir el archivo con otro programa de descompresión como 7-Zip o WinZip®.

Realizar un backup de la base de datos de OnCommand Insight

Realice una copia de seguridad de la base de datos de Insight para asegurarse de tener una copia de seguridad reciente si se produce un problema después de la actualización. Durante la fase de backup y restauración, no se recogerán datos de rendimiento; por lo tanto, el backup debe producirse lo más cerca posible del tiempo de actualización.

Pasos

1. Abra Insight en su navegador.
2. Haga clic en **Admin > solución de problemas**.
3. En la página **solución de problemas**, haga clic en **copia de seguridad**.

El tiempo para realizar un backup de la base de datos puede variar en función de los recursos disponibles (arquitectura, CPU y memoria), el tamaño de la base de datos y la cantidad de objetos supervisados en su entorno.

Una vez finalizada la copia de seguridad, se le preguntará si desea descargar el archivo.

4. Descargue el archivo de copia de seguridad.

Realizar una copia de seguridad de la configuración de seguridad

Cuando los componentes de Insight utilizan una configuración de seguridad no predeterminada, debe realizar una copia de seguridad de la configuración de seguridad y, a continuación, restaurar la configuración en todos los componentes una vez instalado el nuevo software. La configuración de seguridad debe restaurarse antes de restaurar la copia de seguridad de la base de datos del almacén de datos.


Acerca de esta tarea

Utilice la `securityadmin` para crear una copia de seguridad de la configuración y restaurar la configuración guardada. Para obtener más información, busque `securityadmin` En el centro de documentación de OnCommand Insight: <http://docs.netapp.com/oci-73/index.jsp>

Realizar copias de seguridad de informes personalizados de Data Warehouse

Si creó informes personalizados y no dispone de `.xml` archivos de origen para ellos, debe realizar una copia de seguridad de estos informes antes de la actualización. A continuación, debe copiarlos en un servidor que no sea el servidor de almacén de datos.

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 informes e iniciar sesión.
3. Seleccione **Archivo > Abrir**.
4. Seleccione la carpeta en la que se encuentra el informe, selecciónelo y, a continuación, haga clic en **Abrir**.
5. Seleccione **Herramientas > Copiar informe al portapapeles**.
6. Abra un editor de texto, pegue el contenido del informe y guarde el archivo como `report_name.txt`, donde `report_name` es el nombre del informe.
7. Almacene los informes en un servidor que no sea el servidor de almacén de datos.

Realizando la actualización de software

Una vez completadas todas las tareas de requisitos previos, podrá actualizar todos los componentes de Insight a una nueva versión descargando y ejecutando el paquete de instalación correspondiente en cada servidor.

Renovar Insight

Una vez completadas todas las tareas de requisitos previos, inicie sesión en Insight Server y ejecute el paquete de instalación para completar la actualización. El proceso de actualización desinstala el software existente, instala el nuevo software y, a continuación, reinicia el servidor.

Antes de empezar

El paquete de instalación de Insight debe estar ubicado en el servidor.



Debe hacer una copia de seguridad del almacén antes de actualizar OnCommand Insight.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información.

Pasos

1. Inicie sesión en el servidor de Insight con una cuenta que tenga permisos de administrador local de Windows.
2. Busque el paquete de instalación de Insight (SANscreenServer-x64-version_number-build_number.msi) Usando el Explorador de Windows y haga doble clic en él.

Aparece el asistente de configuración de OnCommand InsightSetup.

3. Mueva la ventana de progreso lejos del centro de la pantalla y lejos de la ventana del asistente **Configuración** para que no se oculte ningún error generado de la vista.
4. Siga las instrucciones del asistente de configuración.

Se recomienda dejar todos los valores predeterminados seleccionados.

Después de terminar

Para verificar si la actualización se ha realizado correctamente o si se han generado errores, compruebe el registro de actualización en la siguiente ubicación: <install directory>\SANscreen\wildfly\standalone\log.

Actualizando almacén de datos

Después de completar todas las tareas de requisitos previos, puede iniciar sesión en el servidor de almacén de datos y ejecutar el paquete de instalación para completar la actualización.

Acerca de esta tarea

El almacén de datos (DWH) no admite la actualización en línea. Siga estos pasos para actualizar a la nueva versión del software DWH.



Debe hacer una copia de seguridad del almacén antes de actualizar DWH.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información.

Pasos

Al actualizar el almacén de datos, debe realizar las siguientes acciones:

1. Después de instalar DWH 7,3.16, restaure el almacén y la base de datos en este orden:
 - a. Almacén
 - b. Base de datos
2. Inicie sesión en el servidor DWH utilizando una cuenta que tenga permisos de administrador local de Windows.
3. Realice una copia de seguridad de la base de datos y los informes de DWH mediante la interfaz del portal de DWH.
4. Haga una copia de seguridad del almacén. Consulte ["Securityadmin"](#) la documentación.
5. Desinstale el software DWH del servidor.
6. Reinicie el servidor para eliminar componentes de la memoria.
7. Instale la nueva versión de DWH en el servidor.

La instalación dura aproximadamente 2 horas. Se recomienda dejar todos los valores predeterminados seleccionados.

8. Restaure el almacén en el servidor DWH.
9. Restaurar la base de datos DWH en el servidor.

Después de terminar

Después de actualizar, debe restaurar la base de datos de Data Warehouse, que puede tardar tanto tiempo como más que la actualización.



Durante una actualización de OnCommand Insight, no es extraño que un cliente cambie a un Insight Server diferente. Si ha cambiado el servidor Insight, después de restaurar la base de datos del almacén de datos, los conectores existentes señalarán a la dirección IP o el nombre de host del servidor anterior. Se recomienda eliminar el conector y crear uno nuevo para evitar posibles errores.

Conservando la configuración personalizada de Cognos durante una actualización de Data Warehouse

La configuración personalizada de Cognos, como la configuración de correo electrónico SMTP no predeterminada, no se realiza automáticamente una copia de seguridad como parte de una actualización de Data Warehouse. Debe documentar manualmente y restaurar la configuración personalizada después de una actualización.

Antes de actualizar Data Warehouse, prepare una lista de comprobación con cualquier configuración personalizada de Cognos que desee conservar y revise la lista antes de actualizar el sistema. Una vez finalizada la actualización, puede restaurar los valores manualmente para devolverlos a los ajustes de la configuración original.

Actualización de servidores de unidades de adquisición remotas

Después de completar todas las tareas de requisitos previos, puede iniciar sesión en el servidor de la unidad de adquisición remota y ejecutar el paquete de instalación para

completar la actualización. Debe realizar esta tarea en todos los servidores de adquisición remotos del entorno.

Antes de empezar

- Debe haber actualizado OnCommand Insight.
- El paquete de instalación de OnCommand Insight debe estar ubicado en el servidor.



Debe realizar una copia de seguridad del almacén antes de actualizar.

Consulte "[Herramienta securityadmin](#)" las instrucciones para obtener más información sobre el almacén.

Pasos

1. Inicie sesión en el servidor de la unidad de adquisición remota mediante una cuenta que tenga permisos de administrador local de Windows.
2. Haga una copia de seguridad del almacén.
3. Busque el paquete de instalación de Insight (RAU-x64-version_number-build_number.msi) Usando el Explorador de Windows y haga doble clic en él.

Aparece el asistente de configuración de OnCommand Insight.

4. Mueva la ventana de progreso del asistente de instalación lejos del centro de la pantalla y lejos de la ventana del asistente de instalación para que no se oculte ningún error generado.
5. Siga las instrucciones del asistente de configuración.

Se recomienda dejar todos los valores predeterminados seleccionados.

Después de terminar

- Para verificar si la actualización se ha realizado correctamente o si se han generado errores, compruebe el registro de actualización en la siguiente ubicación: <install_directory>\SANscreen\bin\log.
- Utilice la `securityadmin` para restaurar la seguridad guardada

configuración. Para obtener más información, busque `securityadmin` en OnCommand Insight

Centro de documentación: <http://docs.netapp.com/oci-73/index.jsp>

- Borre la caché y el historial del navegador para garantizar que recibe los datos más recientes del servidor.

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"`

Consulte "[Securityadmin](#)" la documentación para obtener más información sobre la configuración o el cambio de la contraseña del almacén de claves.

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>\SANSscreen\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 entrételes `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 rellenas 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 completado 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.

Solucionar problemas de una actualización

Si se encuentran problemas después de una actualización de OnCommand Insight, es posible que sea útil revisar la información para la solución de problemas relacionada con algunos problemas posibles.

No se puede iniciar Cognos desde el menú Inicio de Windows

La existencia de un espacio antes `\SANscreen\cognos` en el nombre de la ruta es un problema. Consulte lo siguiente en la Comunidad de casos de éxito de clientes de NetApp para obtener más información: <https://forums.netapp.com/thread/62721>.

"no es una aplicación win32 válida" mensaje de error

Esto es un problema con Microsoft Windows. Para resolver este problema, debe colocar comillas alrededor de la ruta de acceso de imagen en el Registro. En la siguiente documentación, se ofrece más información: <https://support.microsoft.com/en-us/kb/812486/en-us>.

Las anotaciones no están presentes

Cuando un trabajo ETL de almacén de datos consulta las anotaciones de una instancia de Insight, a veces recibe una respuesta vacía (resultado de 0) en error. Este error da lugar a anotaciones para determinados objetos que se mueven entre los Estados «'presentes'» y «'no presentes'» del almacén de datos. En la siguiente sección, se ofrece más información: <https://forums.netapp.com/docs/DOC-44167>

Diferencias en los valores mostrados en los informes

Antes de 7.0, los informes se basaban en números enteros. Ahora están basados en decimales; por lo tanto, después de actualizar, puede notar un aumento o disminución en cómo se muestran los valores.

Los datos no se muestran en los informes

En 7.0.1 se cambiaron varios nombres de modelos (por ejemplo, Symmetrix se cambió a Symmetrix VMAX). Como resultado, si un informe contiene un filtro para "Tymmetrix", no verá ningún dato al ejecutar el informe. Para cambiar el informe, debe abrir el informe con Query Explorer en Report Studio, buscar el nombre del modelo, reemplazarlo con el nuevo nombre del modelo y guardar el informe.

Información de copyright

Copyright © 2025 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.