Completing post-upgrade tasks

OnCommand Insight

NetApp
October 24, 2024

Table of Contents

Completing post-upgrade tasks

After you upgrade to the latest version of Insight, you must complete additional tasks.

Installing data source patches

If applicable, you should install the latest patches available for your data sources to take advantage of the latest features and enhancements. After uploading a data source patch, you can install it on all of the data sources of the same type.

Before you begin

You must have contacted technical support and obtained the `.zip` file that contains the latest data source patches by providing them with the version you are upgrading from and the version you want to upgrade to.

Steps

1. Place the patch file on the Insight server.
2. On the Insight toolbar, click **Admin**.
3. Click **Patches**.
4. From the Actions button, select **Apply patch**.
5. In the **Apply data source patch** dialog box, click **Browse** to locate the uploaded patch file.
6. Review the **Patch name**, **Description**, and **Impacted data source types**.
7. If the selected patch is correct, click **Apply Patch**.

   All data sources of the same type are updated with this patch. Insight automatically forces acquisition to restart when you add a data source. Discovery includes the detection of changes in network topology including the addition or deletion of nodes or interfaces.

8. To force the discovery process manually, click **Data Sources** and click **Poll Again** next to the data source to force it to collect data immediately.

   If the data source is already in an acquisition process, Insight ignores the poll again request.

Replacing a certificate after upgrading OnCommand Insight

Opening the OnCommand Insight web UI after an upgrade results in a certification warning. The warning message is displayed because a valid self-signed certificate is not available after the upgrade. To prevent the warning message from being displayed in the future, you can install a valid self-signed certificate to replace the original certificate.

Before you begin

Your system must satisfy the minimum encryption bit level (1024 bits).

About this task

The certification warning does not impact the usability of the system. At the message prompt, you can indicate that you understand the risk, and then proceed to use Insight.

Steps

1. List the contents of the keystore:
   ```
   C:\Program Files\SANscreen\java64\bin>keytool.exe
   -list -v -keystore "c:\Program
   Files\SANscreen\wildfly\standalone\configuration\server.keystore"
   ```

   See the SecurityAdmin documentation for more information about setting or changing the password for the keystore.

   There should be at least one certificate in the keystore, `ssl certificate`.

2. Delete the `ssl certificate`:
   ```
   keytool -delete -alias ssl certificate -keystore
   c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore
   ```

3. Generate a new key:
   ```
   keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize
   2048 -keystore
   "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"
   ```

   a. When prompted for first and last names, enter the fully qualified domain name (FQDN) that you intend to use.

   b. Provide the following information about your organization and organizational structure:

      - Country: two-letter ISO abbreviation for your country (for example, US)
      - State or Province: name of the state or province where your organization’s head office is located (for example, Massachusetts)
      - Locality: name of the city where your organization’s head office is located (for example, Waltham)
      - Organizational name: name of the organization that owns the domain name (for example, NetApp)
      - Organizational unit name: name of the department or group that will use the certificate (for example, Support)
      - Domain Name/ Common Name: the FQDN that is used for DNS lookups of your server (for example, www.example.com) The system responds with information similar to the following: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`

   c. Enter `Yes` when the Common Name (CN) is equal to the FQDN.

   d. When prompted for the key password, enter the password, or press the Enter key to use the existing keystore password.

4. Generate a certificate request file:
   ```
   keytool -certreq -alias localhost -keystore
   "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"
   -file c:\localhost.csr
   ```

   The `c:\localhost.csr` file is the certificate request file that is newly generated.

5. Submit the `c:\localhost.csr` file to your certification authority (CA) for approval.

   Once the certificate request file is approved, you want the certificate returned to you in `.der` format. The file might or might not be returned as a `.der` file. The default file format is `.cer` for Microsoft CA services.

6. Import the approved certificate: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. When prompted for a password, enter the keystore password.

      The system displays the following message: `Certificate reply was installed in keystore`
7. Restart the SANscreen Server service.

Results

The web browser no longer reports certificate warnings.

Increasing Cognos memory

Before you restore the Data Warehouse database, you should increase the Java allocation for Cognos from 768 MB to 2048 MB to decrease report generation time.

Steps

1. Open a command prompt window as administrator on the Data Warehouse server.
2. Navigate to the `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directory.
3. Type the following command: `cogconfigw`

   The IBM Cognos Configuration window displays.

   > ⓘ The IBM Cognos Configuration shortcut application points to `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. If Insight is installed in the Program Files (space between) directory, which is the default, instead of ProgramFiles (no space), the `.bat` file will not work. If this occurs, right click the application shortcut and change `cognosconfigw.bat` to `cognosconfig.exe` to fix the shortcut.

4. From the navigation pane on the left, expand **Environment**, expand **IBM Cognos services**, and then click **IBM Cognos**.
5. Select **Maximum memory for Tomcat in MB** and change 768 MB to 2048 MB.
6. On the IBM Cognos Configuration toolbar, click 💾 (Save).

   An informational message displays to inform you of the tasks Cognos is performing.
7. Click **Close**.
8. On the IBM Cognos Configuration toolbar, click ■ (Stop).
9. On the IBM Cognos Configuration toolbar, click ▶(Start).

Restoring the Data Warehouse database

When you back up the Data Warehouse database, Data Warehouse creates a `.zip` file that you can later use to restore that same database.

About this task

When you restore the Data Warehouse database, you can restore user account information from the backup as well. User management tables are used by the Data Warehouse report engine in a Data Warehouse only installation.

Steps

1. Log in to the Data Warehouse Portal at `https://fqdn/dwh`.
2. From the navigation pane on the left, click **Backup/Restore**.
3. In the **Restore Database and Reports** section, click **Browse** and locate the `.zip` file that holds the Data Warehouse backup.
4. It is a best practice to leave both of the following options selected:
   - **Restore database**

     Includes Data Warehouse settings, data marts, connections, and user account information.
   - **Restore reports**

     Includes custom reports, predesigned reports, changes to predesigned reports that you made, and reporting settings you made in the Reporting Connection.
5. Click **Restore**.

   Do not navigate away from the restore status. If you do, the restore status is no longer displays and you receive no indication when the restore operation is complete.
6. To check the upgrade process, view the `dwh_upgrade.log` file, which is in the following location: `<install directory>\SANscreen\wildfly\standalone\log`.

   After the restore process finishes, a message appears just below the **Restore** button. If the restore process is successful, the message indicates success. If the restore process fails, the message indicates the specific exception that occurred to cause the failure. In this case, contact technical support and provide them with `dwh_upgrade.log` file. If an exception occurs and the restore operation fails, the original database is automatically reset.

   ⓘ If the restore operation fails with a “Failed upgrading cognos content store” message, restore the Data Warehouse database without its reports (database only) and use your XML report backups to import your reports.

Restoring custom Data Warehouse reports

If applicable, you can manually restore any custom reports you backed up before the upgrade; however, you only need to do this if you lose reports of if they have become corrupted.

Steps

1. Open your report with a text editor, and then select and copy its contents.

2. Log in to the Reporting portal at `https://fqdn/reporting`.
3. On the Data Warehouse toolbar, click 📊 to open the Insight Reporting portal.
4. From the Launch menu, select **Report Studio**.
5. Select any package.

   Report Studio displays.

6. Click **Create new**.
7. Select **List**.
8. From the Tools menu, select **Open Report from Clipboard**.

   The **Open Report from Clipboard** dialog box displays.

9. From the File menu, select **Save As** and save the report to the Custom Reports folder.
10. Open the report to verify that it was imported.

    Repeat this task for each report.

> ⓘ You may see an “Expression parsing error” when you load a report. This means that the query contains a reference to at least one object that does not exist, which means there is no package selected in the Source window to validate the report against. In this case, right-click on a data mart dimension in the Source window, select Report Package, and then select the package associated with the report (for example, the inventory package if it is an inventory report or one of the performance packages if it’s a performance report) so Report Studio can validate it and then you can save it.

Verifying that Data Warehouse has historical data

After restoring your custom reports, you should verify that Data Warehouse is collecting historical data by viewing your custom reports.

Steps

1. Log in to the Data Warehouse portal at `https://fqdn/dwh`.
2. On the Data Warehouse toolbar, click 📊 to open the Insight Reporting portal and log in.
3. Open the folder that contains your custom reports (for example, Custom Reports).
4. Click ▶ to open the output format options for this report.
5. Select the options you want and click **Run** to ensure that they are populated with storage, compute, and switch historical data.

Restoring the performance archive

For systems that perform performance archiving, the upgrade process only restores seven days of archive data. You can restore the remaining archive data after the upgrade is competed.

About this task

To restore the performance archive, follow these steps.

Steps

1. On the toolbar, click **Admin** > **Troubleshooting**
2. In the Restore section, under **Load performance archive**, click **Load**.

   Archive loading is handled in the background. Loading the full archive can take a long time as each day's archived performance data is populated into Insight. The status of the archive loading is displayed in the archive section of this page.

Testing the connectors

After you upgrade, you want to test the connectors to ensure that you have a connection from the OnCommand Insight Data Warehouse to the OnCommand Insight server.

Steps

1. Log in to the Data Warehouse Portal at `https://fqdn/dwh`.
2. From the navigation pane on the left, click **Connectors**.
3. Select the first connector.

   The Edit Connector page displays.

4. Click **Test**.
5. If the test is successful, click **Close**; if it fails, enter the name of the Insight server in the **Name** field and its IP address in the **Host** field and click **Test**.
6. When there is a successful connection between the Data Warehouse and the Insight server, click **Save**.

   If it does not succeed, check the connection configuration and ensure the Insight server does not have any issues.

7. Click **Test**.

   Data Warehouse tests the connection.

Verifying the Extract, Transform, and Load scheduling

After you upgrade, you should ensure that the Extract, Transform, and Load (ETL) process is retrieving data from the OnCommand Insight databases, transforming the data, and saving it into the data marts.

Steps

1. Log in to the Data Warehouse portal at `https://fqdn/dwh`.

2. From the navigation pane on the left, click **Schedule**.
3. Click **Edit schedule**.
4. Select **Daily** or **Weekly** from the **Type** list.

   It is recommended to schedule ETL to run once a day.

5. Verify that the time selected is the time at which you want the job to run.

   This ensures that the build job runs automatically.

6. Click **Save**.

Updating disk models

After upgrading, you should have any updated disk models; however, if for some reason Insight failed to discover new disk models, you can manually update them.

Before you begin

You must have obtained from technical support the `.zip` file that contains the latest data source patches.

Steps

1. Stop the SANscreen Acq service.
2. Navigate to the following directory: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Move the current `diskmodels.jar` file to a different location.
4. Copy the new `diskmodels.jar` file into the `datasources.war` directory.
5. Start the SANscreen Acq service.

Verifying that business intelligence tools are running

If applicable, you should verify that your business intelligence tools are running and retrieving data after the upgrade.

Verify that business intelligence tools like BMC Atrium and ServiceNow are running and able to retrieve data. This includes the BMC connector and solutions that leverage REST.

Copyright information

Trademark information