Upgrading OnCommand Insight

OnCommand Insight

NetApp
October 24, 2024

Table of Contents

Upgrading OnCommand Insight

Normally, an upgrade must be performed on all of the Insight servers (Insight server, Data Warehouse server, Remote acquisition unit). You should always consult the Release Notes for the upgrade requirements for a new release of OnCommand Insight.

Unless otherwise indicated, the requirements and procedures apply to upgrading from Insight 7.x to the current version of Insight. If you are upgrading from a version prior to 7.0, contact your account representative.

Upgrading Insight to version 7.3.12 or later - Windows

Prior to upgrading from OnCommand Insight 7.3.10 - 7.3.11 to version 7.3.12 or later, you must run the OCI Data Migration Tool.

Background

OnCommand Insight versions 7.3.12 and later utilize underlying software that may be incompatible with previous versions. Insight versions 7.3.12 and later include a **Data Migration Tool** to assist with upgrading.

OnCommand Insight versions 7.3.9 and earlier are no longer supported. If you are running one of these versions, you *must* upgrade to Insight version 7.3.10 or later (7.3.11 is strongly recommended) prior to upgrading to 7.3.12 or later.

What Does The Data Migration Tool Do?

The migration tool performs an initial compatibility check and then follows one of three different upgrade paths. The path selected is based on the data compatibility of your current version.

Prior to upgrading, you must run the Data Migration Tool and follow the recommended steps.

Before you Begin

- It is strongly recommended to back up your OnCommand Insight system prior to running the Data Migration Tool.
- The Elasticsearch service on the server needs to be up and running.
- The Data Migration Tool *must* be run for the database and any performance archives before you upgrade Insight.

Running the Data Migration Tool

1. Download the latest version of the Data Migration Tool (for example, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) to your Insight server, as well as the appropriate Insight installer file. Unzip into a working folder. Downloads can be found on the NetApp Support Site.
2. Open a command window and navigate to your working folder.
    - Open Powershell as Administrator.
3. Run the data migration tool using the following command:
    - `.\*SANScreenDataMigrationTool.ps1*`

4. Follow the instructions as needed. The following is an example.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen 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\SANscreen\
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...
SANscreen Server service is Running

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

The Data Migration Tool will check for the presence of obsolete indexes on your system and report if any are found. If none are present the tool will exit.

Some indexes may be migrated while the SANscreen Server service is running. Others may only be migrated when the server is stopped. If there are no indexes that may be migrated the tool will exit. Otherwise follow the instructions as prompted.

After the Data Migration Tool completes it will recheck for obsolete indexes. If all indexes have been migrated, the tool will inform you that upgrade to OnCommand Insight 7.3.12 is supported. You can now proceed with upgrading Insight.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen 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:\SANscreen\
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...
SANscreen 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\SANScreenDataMigrationTool-x64-7.3.12-127>
```

If you were prompted to stop the SANScreen service, restart it before upgrading Insight.

Validation failures

In the event that index validation fails, the migration tool will inform you of the problem before quitting.

OnCommand Insight is not present:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool V1.0

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

Invalid Insight version:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen 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
```

Elasticsearch service is not running:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen 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\SANscreen\
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
```

Command-line options

The Data Migration Tool includes some optional parameters that affect its operation.

Option (Windows)	Function

-s	Suppress all prompts
-perf_archive	If specified, existing archive entries for any date whose index(es) are migrated will be replaced. The path should point to the directory containing the archive entry zip files. An argument of '-' may be specified to indicate there is no performance archive to be updated. If this argument is present, the prompt for the archive location will be suppressed.
-check	If present, the script will exit immediately after reporting the index counts.
-dryrun	If present, then the migration executable will report the actions that would be taken (to migrate data and update archive entries) but will not perform the operations.

Overview of the OnCommand Insight upgrade process

Before you begin upgrading Insight, it is important to understand the upgrade process. The upgrade process is the same for most versions of Insight.

You must back up the vault prior to upgrading OnCommand Insight.

See the SecurityAdmin Tool instructions for more information.

The upgrade process for Insight includes the following high-level tasks:

- Downloading the installation packages
- Backing up the Data Warehouse database

  To avoid the possibility of misreporting data, you must back up the Data Warehouse database before you back up the Insight database.

- Backing up the Insight database

  The Insight database is automatically backed up when you perform the in-place upgrade. It is a best practice to back up the database before the upgrade, and place the backup in a location other than on the Insight server. During the upgrade process, Insight does not collect new data. To minimize the amount of data that is not collected, you must start the database backup within an hour or two of your planned upgrade time.

- Back up the Data Warehouse and Remote Acquisition Unit security configuration if the configuration has been changed from the default configuration.

  The non-default security configuration must be restored to the Data Warehouse and RAU server after the

upgrade is complete and before the Data Warehouse database is restored to the system.

- Backing up any custom Data Warehouse reports

  When you back up the Data Warehouse database, custom reports are included. The backup file is created on the Data Warehouse server. It is a recommended best practice to back up the custom reports to a location other than the Data Warehouse server.

- Uninstalling the Data Warehouse and the Remote Acquisition Unit software, if applicable

  The Insight server has an in-place upgrade; you do not have to uninstall the software. The in-place upgrade backs up the database, uninstalls the software, installs the new version, and then restores the database.

- Upgrading the software on the Insight server, Data Warehouse, and Remote Acquisition Unit(s)

  All previously applied licenses remain in the registry; you do not have to reapply these licenses.

- Completing the post-upgrade tasks

OnCommand Insight upgrade checklist

You can use the provided checklists to record your progress as you prepare for the upgrade. These tasks are intended to help mitigate the risk for upgrade failures and to expedite recovery and restoration efforts.

Checklist for preparing for the upgrade (required)

You must back up the vault prior to upgrading OnCommand Insight.

See the SecurityAdmin Tool instructions for more information.

Condition	Complete?
Ensure that you have Windows local administrator permissions, which are required to perform the upgrade process, on all Insight servers.	
If your Insight, Data Warehouse, or Remote Acquisition Unit servers reside on 32-bit platforms, you must upgrade your servers to 64-bit platforms. As of Insight 7.x, upgrades are only available for 64-bit platforms.	

Ensure that you have the necessary permissions to modify or disable the antivirus software on all the servers in your environment. To prevent an upgrade failure due to active virus scan software, you must exclude the Insight installation directory (`disk drive:\install directory\sanscreen` from access to antivirus scanning during the upgrade. After you upgrade all of the components, you can safely reactivate the antivirus software; however, ensure that you configure the scan to still exclude everything in the Insight installation directory. Additionally, you must also exclude the IBM/Db2 folder (for example *C:\Program Files\IBM\DB2*) from anti-virus scanning following installation.	

Checklist for preparing for the upgrade (best practice)

Condition	Complete?
Plan when you are going to upgrade, taking into consideration that most upgrades take a minimum of 4 to 8 hours; larger enterprises will take longer. Upgrade times might vary depending on your available resources (architecture, CPU, and memory), the size of your databases, and the number of objects monitored in your environment.	
Contact your account representative about your upgrade plans and provide the version of Insight you have installed and what version you would like to upgrade to.	
Ensure that your current resources allocated to the Insight, Data Warehouse, and Remote Acquisition Unit(s) still meet recommended specifications. See the recommend sizing guidelines for all servers.Alternatively, you can contact your account representative to discuss sizing guidelines.	
Ensure that you have enough disk space for the database backup and restore process. The backup and restore processes require approximately five times the disk space used by the backup file on the Insight and Data Warehouse servers. For example, a 50 GB backup requires 250 to 300 GB of free disk space.	

Ensure that you have access to Firefox® or the Chrome™ browser when you back up the Insight and Data Warehouse databases. Internet Explorer is not recommended, because it experiences some issues when uploading and downloading files larger than 4 GB.	
Delete the `.tmp` files on the Insight server, which you can find in the following location: `<install directory>\SANscreen\wildfly\standalone\tmp`.	
Remove duplicate data sources and decommissioned data sources from the Insight client. Removing decommissioned or duplicate data sources decreases the amount of time required to perform the upgrade and mitigates the opportunity for data corruption.	
If you have modified any of the default reports shipped with Insight, you should save the reports with a different name and then save them to the Customer Reports folder so that you do not lose your modified report when you upgrade or restore the system.	
If you have any custom or modified Data Warehouse reports created by you or professional services, create a backup of them by exporting them to XML and then moving them to the Customer Reports folder. Ensure that the backup is not located on the Data Warehouse server. If you do not move your reports to the recommended folders, these reports might not be backed up by the upgrade process. For earlier versions of Insight, failure to locate reports in the appropriate folders may result in the loss of custom and modified reports.	
Record all settings in the IBM Cognos Configuration utility, because these are not included in the Data Warehouse backup; you have to reconfigure these settings after the upgrade. The utility is located in the `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directory on the Data Warehouse server and you run it using the `cogconfigw` command.Alternatively, you can perform a complete backup of Cognos and then import all of your settings. Refer to the IBM Cognos documentation for more information.	

Checklist for preparing for the upgrade (if applicable)

Condition	Complete?
If you have replaced the self-signed certificates that the Insight installation created due to browser security warnings with certificates signed by your internal certificate authority, back up your keystore file, which is in the following location: `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` and restore it after the upgrade. This replaces the self-signed certificates that Insight creates with your signed certificates.	
If any of your data sources were modified for your environment and you are unsure if these modifications are available in the Insight version to which you are upgrading, make a copy of the following directory, which will help you troubleshoot if there are recovery issues: `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`.	
Back up all custom database tables and views using the `mysqldump` command line tool.Restoring custom database tables requires privileged database access. Contact technical support for assistance with restoring these tables.	
Ensure that no custom integration scripts, third-party components required for Insight data sources, backups, or any other required data is stored in the `disk drive:\install directory\sanscreen` directory, because the contents of this directory is deleted by the upgrade process.Ensure that you move any of these things from the `\sanscreen` directory to another location. For example, if your environment contains custom integration scripts, ensure that you copy the following file to a directory other than the `\sanscreen` directory: `\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`.	

Downloading the OnCommand Insight installation packages

You should download the installation packages for Insight, Data Warehouse, and the Remote Acquisition Unit (if applicable) prior to the day that you choose to upgrade. Download times for the packages (`.msi` files) vary based on your available bandwidth.

About this task

You can download the installation packages using the Insight webUI or by navigating to the appropriate OnCommand Insight link from http://support.netapp.com/NOW/cgi-bin/software.

To download the installation package from within the Insight server, do the following:

Steps

1. Open the Insight web UI by opening a web browser and entering one of the following:
   - On the Insight server: `https://localhost`
   - From any location: `https://IP Address:port or fqdn:port`

     The port number is either 443 or the port that was configured when the Insight server was installed. The port number defaults to 443 if you do not specify the port number in the URL.
2. Log in to Insight.
3. Click on the Help icon and select **Check for updates**.
4. If a newer version is detected, follow the instructions in the message box.

   You will be taken to the InsightDescription page for the newer version.
5. On the **Description** page, click **Continue**.
6. When the end-user license agreement (EULA) is displayed, click **Accept**.
7. Click the installation package link for each component (Insight server, Data Warehouse, Remote Acquisition Unit), etc.) and click **Save as** to save the installation package.

   Before you upgrade, you should ensure that you copy the Data Warehouse and Remote Acquisition Unit installation packages to disks that are local to their respective servers.
8. Click **CHECKSUM**, and make a note of the numerical values that are associated with each installation package.
9. Verify that the installation packages are complete and without error after you download them.

   Incomplete file transfers can cause issues with the upgrade process.

   To generate MD5 hash values for the installation packages, you can use a third-party utility like Microsoft'sFile ChecksumIntegrity Verifier utility.

Backing up the databases

Before you upgrade, you should back up both the Data Warehouse and OnCommand Insight databases. Upgrading requires a backup of the Data Warehouse database so that you can restore the database later in the upgrade process. The in-place upgrade for Insight backs up the database; however, you should back up the database before the upgrade as a best practice.

You must back up the vault prior to upgrading OnCommand Insight.

See the SecurityAdmin Tool instructions for more information.

To avoid misreporting data, you should back up the Data Warehouse database prior to backing up the Insight database. Additionally, if you have a test environment, it is recommended that you ensure you can restore the backup before you continue with the upgrade.

Backing up the Data Warehouse database

You can back up the Data Warehouse database, which also includes a Cognos backup, to a file and later restore it using the Data Warehouse portal. Such a backup enables you to migrate to a different Data Warehouse server or upgrade to a new Data Warehouse version.

Steps

1. Log in to the Data Warehouse Portal at `https://fqdn/dwh`.
2. From the navigation pane on the left, select **Backup/Restore**.
3. Click **Backup** and select your backup configuration:

   a. All Datamarts except Performance Datamart

   b. All Datamarts

   This operation can take 30 minutes or more.

   + Data Warehouse creates a backup file and displays its name.

4. Right-click the backup file and save it to a location you want.

   You might not want to change the file name; however, you should store the file outside the Data Warehouse installation path.

   The Data Warehouse backup file includes the DWH instance's MySQL; custom schemas (MySQL DBs) and tables; LDAP configuration; the data sources that connect Cognos to the MySQL database (not the data sources that connect the Insight server to devices to acquire data); import and export tasks that imported or exported reports; reporting security roles, groups, and namespaces; user accounts; any modified Reporting Portal reports; and any custom reports, regardless of where they are stored, even in the My Folders directory. Cognos system configuration parameters, such as SMTP server setting, and Cognos custom memory settings are not backed up.

   The default schemas where custom tables are backed up include the following:

dwh_capacity
dwh_capacity_staging
dwh_dimensions
dwh_fs_util

dwh_inventory
dwh_inventory_staging
dwh_inventory_transient
dwh_management
dwh_performance
dwh_performance_staging
dwh_ports
dwh_reports
dwh_sa_staging

Schemas where custom tables are excluded from backup include the following:

information_schema
acquisition
cloud_model
host_data
innodb
inventory
inventory_private
inventory_time
logs
management
mysql
nas

performance
performance_schema
performance_views
sanscreen
scrub
serviceassurance
test
tmp
workbench

In any backup initiated manually, a `.zip` file is created that contains these files:

- A daily backup `.zip` file, which contains Cognos report definitions
- A reports backup `.zip` file, which contains all the reports in Cognos, including those in the My Folders directory
- A Data Warehouse database backup file In addition to manual backups, which you can perform at any time, Cognos creates a daily backup (automatically generated each day to a file called `DailyBackup.zip`) that includes the report definitions. The daily backup includes the top folders and packages shipped with the product. The My Folders directory and any directories that you create outside the product's top folders are not included in the Cognos backup.

Due to the way Insight names the files in the `.zip` file, some unzip programs show that the file is empty when opened. As long as the `.zip` file has a size greater than 0 and does not end with a `.bad` extension, the `.zip` file is valid. You can open the file with another unzip program like 7-Zip or WinZip®.

Backing up the OnCommand Insight database

Back up the Insight database to ensure that you have a recent backup if an issue occurs after the upgrade. During the backup and restore phase, performance data will not be collected; thus, the backup should occur as close as possible to the upgrade time.

Steps

1. Open Insight in your browser.
2. Click **Admin** > **Troubleshooting**.

3. On the **Troubleshooting** page, click **Backup**.

   The time to back up the database might vary depending on your available resources (architecture, CPU, and memory), the size of your database, and the number of objects monitored in your environment.

   When the backup is complete, you are asked if you want to download the file.

4. Download the backup file.

Backing up the security configuration

When your Insight components are using a non-default security configuration, you must back up the security configuration and then restore the configuration on all components after the new software is installed. The security configuration must be restored before the Data Warehouse database backup is restored.

About this task

You use the `securityadmin` tool to create a backup of the configuration and to restore the saved configuration. For more information, search for `securityadmin` in the OnCommand Insight Documentation Center: http://docs.netapp.com/oci-73/index.jsp

Backing up custom Data Warehouse reports

If you created custom reports and you do not have the `.xml` source files for them, then you should back up these reports before the upgrade. You should then copy them to a server other than the Data Warehouse server.

Steps

1. Log in to the Data Warehouse portal at `https://fqdn/dwh`.
2. On the Data Warehouse toolbar, click  to open the Reporting Portal and log in.
3. Select **File** > **Open**.
4. Select the folder that the report is located in, select the report, and then click **Open**.
5. Select **Tools** > **Copy report to clipboard**.
6. Open a text editor, paste the contents of the report, and save the file as `report_name.txt`, where `report _name` is the name of the report.
7. Store the reports on a server other than the Data Warehouse server.

Performing the software upgrade

After you complete all prerequisite tasks, you can upgrade all of the Insight components to a new release by downloading and running the applicable installation package on each server.

Upgrading Insight

After you complete all prerequisite tasks, you log in to the Insight server and run the installation package to complete the upgrade. The upgrade process uninstalls the existing software, installs the new software, and then reboots the server.

Before you begin

The Insight installation package must be located on the server.

You must back up the vault prior to upgrading OnCommand Insight.

See the SecurityAdmin Tool instructions for more information.

Steps

1. Log in to the Insight server using an account that has Windows local administrator permissions.
2. Locate the Insight installation package (`SANscreenServer-x64-version_number-build_number.msi`) using Windows Explorer and double-click it.

   The OnCommand InsightSetup wizard displays.
3. Move the progress window away from the center of the screen and away from the **Setup** wizard window so that any generated errors are not hidden from view.
4. Follow the setup wizard prompts.

   It is a best practice to leave all the defaults selected.

After you finish

To verify if the upgrade is successful or if errors are generated, check the upgrade log in the following location: `<install directory>\SANscreen\wildfly\standalone\log`.

Upgrading Data Warehouse

After you complete all prerequisite tasks, you can log in to the Data Warehouse server and run the installation package to complete the upgrade.

About this task

Inline upgrade is not supported by the Data Warehouse (DWH). Use the following steps to upgrade to the new version of DWH software.

You must back up the vault prior to upgrading DWH.

See the SecurityAdmin Tool instructions for more information.

Steps

When upgrading the Data Warehouse, you must perform the following actions:

1. After you install DWH 7.3.16, restore the vault and database in this order:
   a. Vault
   b. Database
2. Log in to the DWH server using an account that has Windows local administrator permissions.
3. Back up the DWH DB and Reports using the DWH portal interface.
4. Back up the vault. See the SecurityAdmin documentation.
5. Uninstall the DWH software from the server.
6. Reboot the server to remove components from memory.
7. Install the new version of DWH on the server.

   The installation takes approximately 2 hours. It is a best practice to leave all the defaults selected.

8. Restore the vault to the DWH server.
9. Restore the DWH database to the server.

After you finish

After you upgrade, you must restore the Data Warehouse database, which can take as long or longer than the upgrade.

> During an OnCommand Insight upgrade, it is not uncommon for a customer to switch to a different Insight server. If you have changed your Insight server, after you restore the data warehouse database the existing connectors will point to the previous server IP address or hostname. It is a best practice to delete the connector and create a new one, to avoid possible errors.

Preserving custom Cognos settings during a Data Warehouse upgrade

Custom Cognos settings, such as non-default SMTP email settings, are not automatically backed up as part of a Data Warehouse upgrade. You need to manually document and then restore the custom settings following an upgrade.

Prior to upgrading Data Warehouse, prepare a checklist with any custom Cognos settings that you want to preserve, and review the list prior to upgrading the system. After the upgrade is complete, you can restore the values manually to return them to the settings in the original configuration.

Upgrading remote acquisition unit servers

After you complete all prerequisite tasks, you can log in to the remote acquisition unit server and run the installation package to complete the upgrade. You must perform this task on all remote acquisition servers in your environment.

Before you begin

- You must have upgraded OnCommand Insight.
- The OnCommand Insight installation package must be located on the server.

You must back up the vault prior to upgrading.

See the SecurityAdmin Tool instructions for more information about the vault.

Steps

1. Log in to the remote acquisition unit server using an account that has Windows local administrator permissions.
2. Back up the vault.
3. Locate the Insight installation package (`RAU-x64-version_number-build_number.msi`) using Windows Explorer and double-click it.

   The OnCommand Insight Setup Wizard displays.
4. Move the installation wizard progress window away from the center of the screen and away from the installation wizard window so that any generated errors are not hidden from view.
5. Follow the Setup Wizard prompts.

   It is a best practice to leave all the defaults selected.

After you finish

- To verify if the upgrade is successful or if errors are generated, check the upgrade log in the following location: `<install directory>\SANscreen\bin\log`.
- Use the `securityadmin` tool to restore the saved security

  configuration. For more information, search for securityadmin in the OnCommand Insight

  Documentation Center: http://docs.netapp.com/oci-73/index.jsp
- Clear your browser's cache and history to ensure that you are receiving the latest data from the server.

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.

Troubleshooting an upgrade

If you encounter issues after an OnCommand Insight upgrade, you might find it helpful to review the troubleshooting information related to some possible issues.

Unable to start Cognos from the Windows Start menu

The existence of a space before `\SANscreen\cognos` in the path name is an issue. See the following in the NetApp Customer Success Community for more information: https://forums.netapp.com/thread/62721.

“Not a valid win32 application” error message

This is an issue with Microsoft Windows. To resolve this issue, you must put quotation marks around the image path in the registry. See the following documentation for more information: https://support.microsoft.com/en-us/kb/812486/en-us.

Annotations are not present

When a Data Warehouse ETL job queries for annotations from an Insight instance, it sometimes receives an empty response (a 0 result) in error. This error results in annotations for certain objects moving back and forth between a “present” and “not present” state in Data Warehouse. See the following for more information: https://forums.netapp.com/docs/DOC-44167

Differences in values displayed in reports

Prior to 7.0, reports were integer-based. They are now decimal-based; therefore, after you upgrade, you may notice a increase or decrease in how the values display.

Data does not display in reports

In 7.0.1, several model names were changed (for example, Symmetrix was changed to Symmetrix VMAX). As a result, if a report contains a filter for “Symmetrix”, you will not see any data when you run the report. To

change the report, you must open the report with Query Explorer in Report Studio, search for the model name, replace it with the new model name, and save the report.

Copyright information

Trademark information