Setting up Insight

OnCommand Insight

NetApp
June 10, 2024

Table of Contents

Setting up Insight

To set up Insight, you must activate Insight licenses, set up your data sources, define users and notifications, enable backups, and perform any required advanced configuration steps.

After the OnCommand Insight system is installed, you must perform these setup tasks:

- Install your Insight licenses.
- Set up your data sources in Insight.
- Set up user accounts.
- Configure your email.
- Define your SNMP, email, or syslog notifications if needed.
- Enable automatic weekly backups of your Insight database.
- Perform any advanced configuration steps required, including defining annotations and thresholds.

Accessing the web UI

After you install OnCommand Insight, you must install your licenses and then set up Insight to monitor your environment. To do this, you use a web browser to access the Insight web UI.

Steps

1. Do one of the following:
    - Open Insight on the Insight server:

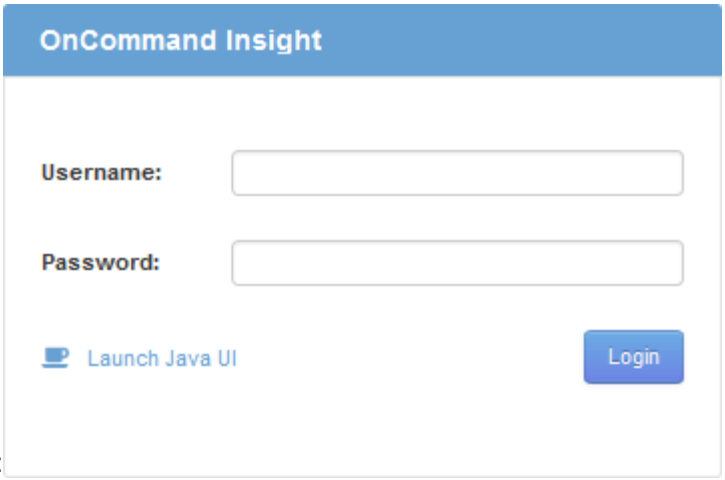
      `https://fqdn`

    - Open Insight from any other location:

      `https://fqdn:port`

      The port number is either 443 or another port configured when the Insight server was installed. The port number defaults to 443 if you do not specify it in the URL.

The OnCommand Insight dialog box displays:



2. Enter your user name and password and click **Login**.

   If the licenses have been installed, the data source setup page displays.

> An Insight browser session that is inactive for 30 minutes is timed out and you are automatically logged out of the system. For added security, it is recommended to close your browser after logging out of Insight.

Installing your Insight licenses

After you receive the license file containing the Insight license keys from NetApp, you can use the setup features to install all of your licenses at the same time.

About this task

Insight license keys are stored in a `.txt` or `.lcn` file.

Steps

1. Open the license file in a text editor and copy the text.
2. Open Insight in your browser.
3. On the Insight toolbar, click **Admin**.
4. Click **Setup**.
5. Click the **Licenses** tab.
6. Click **Update License**.
7. Copy the license key text into the **License** text box.
8. Select the **Update (most common)** operation.
9. Click **Save**.
10. If you are using the Insight consumption licensing model, you must check the box to **Enable sending usage information to NetApp** in the **Send usage information** section. Proxy must be properly configured and enabled for your environment.

After you finish

After installing the licenses, you can perform these configuration tasks:

- Configure data sources.
- Create OnCommand Insight user accounts.

OnCommand Insight licenses

OnCommand Insight operates with licenses that enable specific features on the Insight Server.

- **Discover**

  Discover is the basic Insight license that supports inventory. You must have a Discover license to use OnCommand Insight, and the Discover license must be paired with at least one of the Assure, Perform, or Plan licenses.

- **Assure**

  An Assure license provides support for assurance functionality, including global and SAN path policy, and violation management. An Assure license also enables you to view and manage vulnerabilities.

- **Perform**

  A Perform license supports performance monitoring on asset pages, dashboard widgets, queries, and so on, as well as managing performance policies and violations.

- **Plan**

  A Plan license supports planning functions, including resource usage and allocation.

- **Host Utilization pack**

  A Host Utilization license supports file system utilization on hosts and virtual machines.

- **Report Authoring**

  A Report Authoring license supports additional authors for reporting. This license requires the Plan license.

OnCommand Insight modules are licensed for annual term or perpetual:

- By terabyte of monitored capacity for Discover, Assure, Plan, Perform modules
- By number of hosts for Host Utilization pack
- By number of additional units of Cognos pro-authors required for Report Authoring

License keys are a set of unique strings that are generated for each customer. You can obtain license keys from your OnCommand Insight representative.

Your installed licenses control the following options that are available in the software:

- **Discover**

Acquire and manage inventory (Foundation)

Monitor changes and manage inventory policies

- **Assure**

  View and manage SAN path policies and violations

  View and manage vulnerabilities

  View and manage tasks and migrations

- **Plan**

  View and manage requests

  View and manage pending tasks

  View and manage reservation violations

  View and manage port balance violations

- **Perform**

  Monitor performance data, including data in dashboard widgets, asset pages, and queries

  View and manage performance policies and violations

The following tables provide details of the features that are available with and without the Perform license for admin users and non-admin users.

Feature (admin)	With Perform license	Without Perform license
Application	Yes	No performance data or charts
Virtual machine	Yes	No performance data or charts
Hypervisor	Yes	No performance data or charts
Host	Yes	No performance data or charts
Datastore	Yes	No performance data or charts
VMDK	Yes	No performance data or charts
Internal volume	Yes	No performance data or charts
Volume	Yes	No performance data or charts
Storage pool	Yes	No performance data or charts

Disk	Yes	No performance data or charts
Storage	Yes	No performance data or charts
Storage node	Yes	No performance data or charts
Fabric	Yes	No performance data or charts
Switch port	Yes	No performance data or charts; “Port Errors” shows “N/A”
Storage port	Yes	Yes
NPV port	Yes	No performance data or charts
Switch	Yes	No performance data or charts
NPV switch	Yes	No performance data or charts
Qtrees	Yes	No performance data or charts
Quota	Yes	No performance data or charts
Path	Yes	No performance data or charts
Zone	Yes	No performance data or charts
Zone member	Yes	No performance data or charts
Generic device	Yes	No performance data or charts
Tape	Yes	No performance data or charts
Masking	Yes	No performance data or charts
ISCSI sessions	Yes	No performance data or charts
ICSI network portals	Yes	No performance data or charts
Search	Yes	Yes
Admin	Yes	Yes
Dashboard	Yes	Yes

Widgets	Yes	Partially available (only asset, query, and admin widgets are available)
Violations dashboard	Yes	Hidden
Assets dashboard	Yes	Partially available (storage IOPS and VM IOPS widgets are hidden)
Manage performance policies	Yes	Hidden
Manage annotations	Yes	Yes
Manage annotation rules	Yes	Yes
Manage applications	Yes	Yes
Queries	Yes	Yes
Manage business entities	Yes	Yes

Feature	User - with Perform license	Guest - with Perform license	User - without Perform license	Guest - without Perform license
Assets dashboard	Yes	Yes	Partially available (storage IOPS and VM IOPS widgets are hidden)	Partially available (storage IOPS and VM IOPS widgets are hidden)
Custom dashboard	View only (no create, edit, or save options)	View only (no create, edit, or save options)	View only (no create, edit, or save options)	View only (no create, edit, or save options)
Manage performance policies	Yes	Hidden	Hidden	Hidden
Manage annotations	Yes	Hidden	Yes	Hidden
Manage applications	Yes	Hidden	Yes	Hidden
Manage business entities	Yes	Hidden	Yes	Hidden
Queries	Yes	View and edit only (no save option)	Yes	View and edit only (no save option)

Setting up and managing user accounts

User accounts, user authentication, and user authorization can be defined and managed in either of two ways: in Microsoft Active Directory (Version 2 or 3) LDAP (Lightweight Directory Access Protocol) server, or in an internal OnCommand Insight user database. Having a different user account for each person provides a way of controlling the access rights, individual preferences, and accountability. Use an account that has Administrator privileges for this operation.

Before you begin

You must have completed the following tasks:

- Install your OnCommand Insight licenses.
- Allocate a unique user name for each user.
- Determine what passwords to use.
- Assign the correct user roles.

Security best practices dictate that administrators configure the host operating system to prevent the interactive login of non-administrator/standard users.

Steps

1. Open Insight in your browser.
2. On the Insight toolbar, click **Admin**.
3. Click **Setup**.
4. Select the **Users**tab.
5. To create a new user, click the **Actions** button and select **Add user**.

   You enter the **Name**, **Password**, **Email** address, and select one of the user **Roles** as Administrator, User, or Guest.

6. To change a user's information, select the user from the list and click the **Edit user account** symbol to the right of the user description.
7. To remove a user from the OnCommand Insight system, select the user from the list and click **Delete user account** to the right of the user description.

Results

When a user logs in to OnCommand Insight, the server first attempts to authenticate through LDAP, if LDAP is enabled. If OnCommand Insight cannot locate the user on the LDAP server, it searches in the local Insight database.

Insight user roles

Each user account is assigned one of the three possible permission levels.

- Guest permits you to log into Insight and to view the various pages.
- User permits all guest-level privileges, as well as access to Insight operations such as defining policy and identifying generic devices. The User account type does not allow you to perform data source operations, nor to add or edit any user accounts other than your own.
- Administrator permits you to perform any operation, including adding new users and managing data sources.

Best Practice: Limit the number of users with Administrator permissions by creating most accounts for users or guests.

Configuring Insight for LDAP(s)

OnCommand Insight must be configured with Lightweight Directory Access Protocol (LDAP) settings as they are configured in your corporate LDAP domain.

Before configuring Insight for use with LDAP or secure LDAP (LDAPs), make note of the Active Directory configuration in your corporate environment. Insight settings must match those in your organization's LDAP domain configuration. Review the concepts below before configuring Insight for use with LDAP, and check with your LDAP domain administrator for the proper attributes to use in your environment.

For all Secure Active Directory (i.e. LDAPS) users, you must use the AD server name exactly as it is defined in the certificate. You can not use IP address for secure AD login.

OnCommand Insight supports LDAP and LDAPS via Microsoft Active Directory server or Azure AD. Additional LDAP implementations may work but have not been qualified with Insight. The procedures in these guides assume that you are using Microsoft Active Directory Version 2 or 3 LDAP (Lightweight Directory Access Protocol).

User Principal Name attribute:

The LDAP User Principal Name attribute (userPrincipalName) is what Insight uses as the username attribute. User Principal Name is guaranteed to be globally unique in an Active Directory (AD) forest, but in many large organizations, a user's principal name may not be immediately obvious or known to them. Your organization might use an alternative to the User Principal Name attribute for primary user name.

Following are some alternative values for the User Principal Name attribute field:

- **sAMAccountName**

  This user attribute is the legacy pre-Windows 2000 NT username - this is what most users are accustomed to logging into their personal Windows machine. This is not guaranteed to be globally unique throughout an AD forest.

  sAMAccountName is case-sensitive for the User Principal Name attribute.

- **mail**

  In AD environments with MS Exchange, this attribute is the primary e-mail address for the end user. This should be globally unique throughout an AD forest, (and also familiar for end users), unlike their userPrincipalName attribute. The mail attribute will not exist in most non-MS Exchange environments.

- **referral**

An LDAP referral is a domain controller's way of indicating to a client application that it does not have a copy of a requested object (or, more precisely, that it does not hold the section of the directory tree where that object would be, if in fact it exists) and giving the client a location that is more likely to hold the object. The client in turn uses the referral as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the referred-to domain controller to generate yet another referral, although it usually does not take long to discover that the object does not exist and to inform the client.

sAMAccountName is generally preferred over User Principal Name. sAMAccountName is unique in the domain (though it may not be unique in the domain forest), but it is the string domain users typically use for login (For example,*netapp\username*).The Distinguished Name is the unique name in the forest, but is generally not known by the users.

On the Windows system part of the same domain, you can always open a command prompt and type SET to find the proper domain name (USERDOMAIN=). The OCI login name will then be `USERDOMAIN\sAMAccountName`.

For the domain name **mydomain.x.y.z.com**, use `DC=x,DC=y,DC=z,DC=com` in the Domain field in Insight.

Ports:

The default port for LDAP is 389, and the default port for LDAPs is 636

Typical URL for LDAPs: `ldaps://<ldap_server_host_name>:636`

Logs are at:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

By default, Insight expects the values noted in the following fields. If these change in your Active Directory environment, be sure to change them in the Insight LDAP configuration.

Role attribute
memberOf
Mail attribute
mail
Distinguished Name attribute
distinguishedName
Referral
follow

Groups:

To authenticate users with different access roles in the OnCommand Insight and DWH servers, you must

create groups in Active Directory and enter those group names in OnCommand Insight and DWH servers. The group names below are examples only; the names you configure for LDAP in Insight must match the ones set up for your Active Directory environment.

Insight Group	Example
Insight server administrator group	insight.server.admins
Insight administrators group	insight.admins
Insight users group	insight.users
Insight guests group	insight.guests
Reporting administrator group	insight.report.admins
Reporting pro authors group	insight.report.proauthors
Reporting authors group	insight.report.business.authors
Reporting consumers group	insight.report.business.consumers
Reporting recipients group	insight.report.recipients

Configuring user definitions using LDAP

To configure OnCommand Insight (OCI) for user authentication and authorization from an LDAP server, you must be defined in the LDAP server as the OnCommand Insight server administrator.

Before you begin

You must know the user and group attributes that have been configured for Insight in your LDAP domain.

For all Secure Active Directory (i.e. LDAPS) users, you must use the AD server name exactly as it is defined in the certificate. You can not use IP address for secure AD login.

About this task

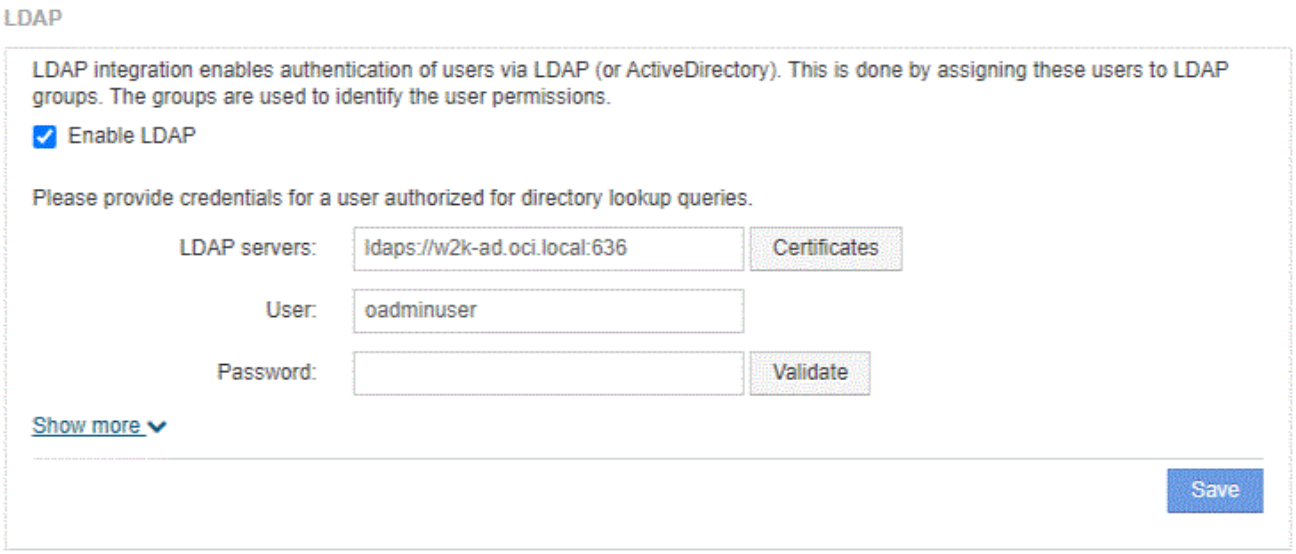
OnCommand Insight supports LDAP and LDAPS via Microsoft Active Directory server. Additional LDAP implementations may work but have not been qualified with Insight. This procedure assumes that you are using Microsoft Active Directory Version 2 or 3 LDAP (Lightweight Directory Access Protocol).

LDAP users display along with the locally defined users in the **Admin** > **Setup** › **Users** list.

Steps

1. On the Insight toolbar, click **Admin**.
2. Click **Setup**.

3. Click the **Users** tab.
4. Scroll to the LDAP section, as shown here.



5. Click **Enable LDAP** to allow the LDAP user authentication and authorization.
6. Fill in the fields:
   - `LDAP servers`: Insight accepts a comma-separated list of LDAP URLs. Insight attempts to connect to the provided URLs without validating for LDAP protocol.

     To import the LDAP certificates, click **Certificates** and automatically import or manually locate the certificate files.

     The IP address or DNS name used to identify the LDAP server is typically entered in this format:

     ```
     ldap://<ldap-server-address>:port
     ```

     or, if using the default port:

     ```
     ldap://<ldap-server-address>
     ```

     When entering multiple LDAP servers in this field, ensure that the correct port number is used in each entry.

   - `User name`: Enter the credentials for a user authorized for directory lookup queries on the LDAP servers.
   - `Password`: Enter the password for the above user. To confirm this password on the LDAP server, click **Validate**.
7. If you want to define this LDAP user more precisely, click **Show more** and fill in the fields for the listed attributes.

   These settings must match the attributes configured in your LDAP domain. Check with your Active Directory administrator if you are unsure of the values to enter for these fields.

- **Admins group**

  LDAP group for users with Insight Administrator privileges. Default is `insight.admins`.

- **Users group**

  LDAP group for users with Insight User privileges. Default is `insight.users`.

- **Guests group**

  LDAP group for users with Insight Guest privileges. Default is `insight.guests`.

- **Server admins group**

  LDAP group for users with Insight Server Administrator privileges. Default is `insight.server.admins`.

- **Timeout**

  Length of time to wait for a response from the LDAP server before timing out, in milliseconds. default is 2,000, which is adequate in all cases and should not be modified.

- **Domain**

  LDAP node where OnCommand Insight should start looking for the LDAP user. Typically this is the top-level domain for the organization. For example:

  ```
  DC=<enterprise>,DC=com
  ```

- **User principal name attribute**

  Attribute that identifies each user in the LDAP server. Default is `userPrincipalName`, which is globally unique. OnCommand Insight attempts to match the contents of this attribute with the username that has been supplied above.

- **Role attribute**

  LDAP attribute that identifies the user's fit within the specified group. Default is `memberOf`.

- **Mail attribute**

  LDAP attribute that identifies the user's email address. Default is `mail`. This is useful if you want to subscribe to reports available from OnCommand Insight. Insight picks up the user's email address the first time each user logs in and does not look for it after that.

  If the user's email address changes on the LDAP server, be sure to update it in Insight.

- **Distinguished name attribute**

  LDAP attribute that identifies the user's distinguished name. default is `distinguishedName`.

8. Click **Save**.

Changing user passwords

A user with administrator privileges can change the password for any OnCommand Insight user account defined on the local server.

Before you begin

The following items must have been completed:

- Notifications to anyone who logs into the user account you are modifying.
- New password to be used after this change.

About this task

When using this method, you cannot change the password for a user who is validated through LDAP.

Steps

1. Log in with administrator privileges.
2. On the Insight toolbar, click **Admin**.
3. Click **Setup**.
4. Click the **Users** tab.
5. Locate the row that displays the user account you want to modify.
6. To the right of the user information, click **Edit user account**.
7. Enter the new **Password** and then enter it again in the verification field.
8. Click **Save**.

Editing a user definition

A user with administrator privileges can edit a user account to change the email address or roles for OnCommand Insight or DWH and reporting functions.

Before you begin

Determine the type of user account (OnCommand Insight, DWH or a combination) that needs to be changed.

About this task

For LDAP users, you can only modify the email address using this method.

Steps

1. Log in with administrator privileges.
2. On the Insight toolbar, click **Admin**.
3. Click **Setup**.
4. Click the **Users** tab.
5. Locate the row that displays the user account you want to modify.

6. To the right of the user information, click the **Edit user account** icon.
7. Make the necessary changes.
8. Click **Save**.

Deleting a user account

Any user with Administrator privileges can delete a user account, either when it is no longer used (for a local user definition) or to force OnCommand Insight to rediscover the user information the next time the user logs in (for an LDAP user).

Steps

1. Log into OnCommand Insight with Administrator privileges.
2. On the Insight toolbar, click **Admin**.
3. Click **Setup**.
4. Click the **Users** tab.
5. Locate the row that displays the user account you want to delete.
6. To the right of the user information, click the **Delete user account "x"** icon.
7. Click **Save**.

Setting a Login Warning Message

OnCommand Insight allows administrators to set a custom text message that is displayed when users log in.

Steps

1. To set the message in the OnCommand Insight Server:
   a. Navigate to **Admin › Troubleshooting › Advanced Troubleshooting › Advanced Settings**.
   b. Enter your login message in the text area.
   c. Click the **Client displays login warning message** checkbox.
   d. Click **Save**.

      The message will display upon login for all users.
2. To set the message in the Data Warehouse (DWH) and Reporting (Cognos):
   a. Navigate to **System Information** and click the **Login Warning** tab.
   b. Enter your login message in the text area.
   c. Click **Save**.

      The message will display upon DWH and Cognos Reporting login for all users.

Insight Security

The 7.3.1 release of OnCommand Insight introduced security features that allow Insight environments to operate with enhanced security. The features include improvements to encryption, password hashing, and the ability to change internal user passwords and key pairs that encrypt and decrypt passwords. You can manage these features on all servers in the Insight environment.

The default installation of Insight includes a security configuration where all sites in your environment share the same keys and the same default passwords. To protect sensitive data, NetApp recommends you change the default keys and the Acquisition user password after an installation or upgrade.

Data source encrypted passwords are stored in the Insight Server database. The Server has a public key and encrypts passwords when a user enters them in a WebUI data source configuration page. The Server does not have the private keys required to decrypt the data source passwords stored in the Server database. Only Acquisition Units (LAU, RAU) have the data source private key required to decrypt data source passwords.

Rekeying servers

Using default keys introduces security vulnerability in your environment. By default, data source passwords are stored encrypted in the Insight database. They are encrypted using a key that is common to all Insight installations. In a default configuration, an Insight database sent to NetApp includes passwords that could theoretically be decrypted by NetApp.

Changing the Acquisition user password

Using the default 'Acquisition' user password introduces security vulnerability into your environment. All Acquisition Units use the “Acquisition” user to communicate with the Server. RAUs with default passwords can theoretically connect to any Insight server using default passwords.

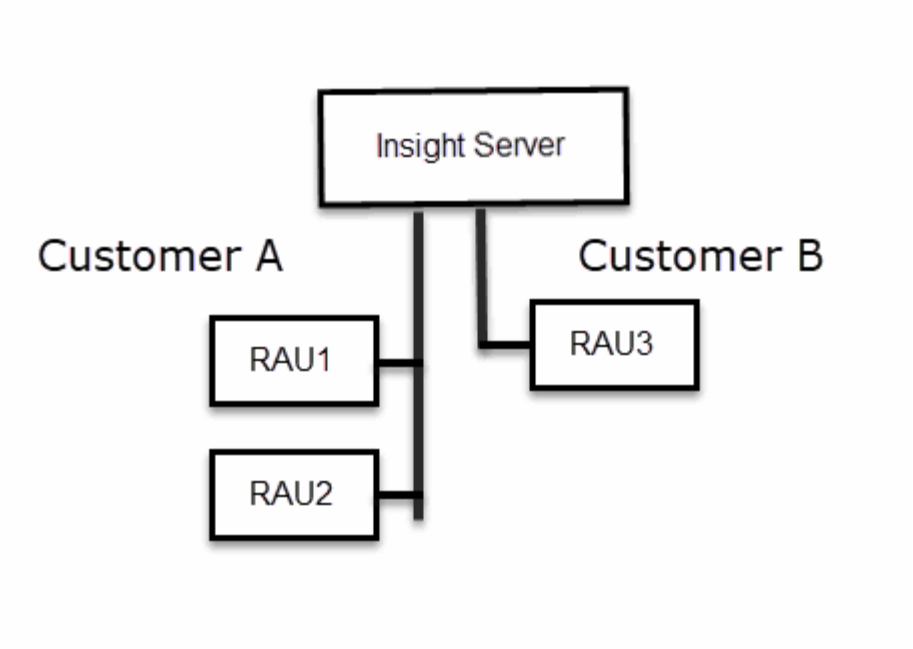
Upgrade and installation considerations

When your Insight system contains non-default security configurations (you have rekeyed or changed passwords), you must back up your security configurations. Installing new software, or in some cases upgrading software, reverts your system to a default security configuration. When your system reverts to the default configuration, you must restore the non-default configuration in order for the system to operate correctly.

Managing keys in a complex service provider environment

A service provider can host multiple OnCommand Insight customers collecting data. The keys protect customer data from unauthorized access by multiple customers on the Insight server. Each customer’s data is protected by their specific key pairs.

This implementation of Insight could be configured as shown in the following illustration.



You need to create individual keys for each customer in this configuration. Customer A requires identical keys for both RAUs. Customer B requires a single set of keys.

The steps you would take to change encryption keys for Customer A:

1. Perform a remote login to the server hosting RAU1.
2. Start the security admin tool.
3. Select Change Encryption Key to replace the default keys.
4. Select Backup to create a backup zip file of the security configuration.
5. Perform a remote login to the server hosting RAU2.
6. Copy the backup zip file of the security configuration to RAU2.
7. Start the security admin tool.
8. Restore the security backup from RAU1 to the current server.

The steps you would take to change encryption keys for Customer B:

1. Perform a remote login to the server hosting RAU3.
2. Start the security admin tool.
3. Select Change Encryption Key to replace the default keys.
4. Select Backup to create a backup zip file of the security configuration.

Managing security on the Insight server

The `securityadmin` tool allows you to manage security options on the Insight server. Security management includes changing passwords, generating new keys, saving and restoring security configurations you create, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Steps

1. Perform a remote login to the Insight server.
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     The system requests login credentials.
3. Enter the user name and password for an account with “Admin” credentials.
4. Select **Server**.

   The following server configuration options are available:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change the server encryption key on one server - Create a backup of the vault - Restore the vault backup to the second server
   - **Change Encryption Key**

     Change the server encryption key that is used to encrypt or decrypt proxy user passwords, SMTP user passwords, LDAP user passwords, and so on.

     When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.
   - **Update Password**

     Change password for the internal accounts that are used by Insight. The following options are displayed:

- _internal
- acquisition
- cognos_admin
- dwh_internal
- hosts
- inventory
- root

> Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Reset to Defaults**

  Resets keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

1. Chose the option you want to change and follow the prompts.

Managing security on the local acquisition unit

The `securityadmin` tool allows you to manage security options on the local acquisition user (LAU). Security management includes managing keys and passwords, saving and restoring security configurations you create or restoring configurations to the default settings.

Before you begin

You must have `admin` privileges to perform security configuration tasks.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Steps

1. Perform a remote login to the Insight server.
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`

- Linux - `/bin/oci-securityadmin.sh -i`

  The system requests login credentials.

3. Enter the user name and password for an account with “Admin” credentials.
4. Select **Local Acquisition Unit** to reconfigure the Local Acquisition Unit security configuration.

   The following options are displayed:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`

   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on the LAU - Create a backup of the vault - Restore the vault backup to each of the RAUs

   - **Change Encryption Keys**

     Change the AU encryption keys used to encrypt or decrypt device passwords.

     When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.

   - **Update Password**

     Change password for 'acquisition' user account.

     Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

   - **Reset to Defaults**

     Resets acquisition user password and acquisition user encryption keys to default values, Default values are those provided during installation.

   - **Exit**

     Exit the `securityadmin` tool.

5. Chose the option you want configure and follow the prompts.

Managing security on an RAU

The `securityadmin` tool allows you to manage security options on RAUs. You might need to backup or restore a vault configuration, change encryption keys, or update passwords for the acquisition units.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

One scenario for updating the security configuration for the LAU, RAU is to update the 'acquisition' user password when the password for that user has been changed on the server. All of the RAUs, and the LAU use the same password as that of the server 'acquisition' user to communicate with the server.

The 'acquisition' user only exists on the Insight server. The RAU or LAU logs in as that user when they connect to the server.

Use the following steps to manage security options on an RAU:

Steps

1. Perform a remote login to the server running the RAU
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     The system requests login credentials.
3. Enter the user name and password for an account with “Admin” credentials.

   The system displays the menu for the RAU.

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on one server - Create a backup of the vault - Restore the vault backup to the second server

- **Change Encryption Keys**

  Change the RAU encryption keys used to encrypt or decrypt device passwords.

  > When you change encryption keys, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Update Password**

  Change password for 'acquisition' user account.

  > Some accounts need to be synchronized when passwords are changed. For example, if you change the password for the 'acquisition' user on the server, you need to change the password for the 'acquisition' user on the LAU, RAU, and DWH to match. Also, when you change passwords, you should backup your new security configuration so that you can restore it after an upgrade or installation.

- **Reset to Defaults**

  Resets encryption keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

Managing security on the Data Warehouse

The `securityadmin` tool allows you to manage security options on the Data Warehouse server. Security management includes updating internal passwords for internal users on the DWH server, creating backups of the security configuration, or restoring configurations to the default settings.

About this task

You use the `securityadmin` tool to manage security:

- Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Steps

1. Perform a remote login to the Data Warehouse server.
2. Start the security admin tool in interactive mode:
   - Windows - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     The system requests login credentials.

3. Enter the user name and password for an account with “Admin” credentials.

   The system displays the security admin menu for the Data Warehouse:

   - **Backup**

     Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the default location:

     - Windows - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`

   - **Restore**

     Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

     > Restore can be used to synchronize passwords and keys on multiple servers, for example: - Change encryption keys on one server - Create a backup of the vault - Restore the vault backup to the second server
     >
     > +

   - **Change encryption keys**

     Change the DWH encryption key used to encrypt or decrypt passwords such as connector passwords and SMPT passwords.

   - **Update Password**

     Change password for a specific user account.

     - _internal
     - acquisition
     - cognos_admin
     - dwh
     - dwh_internal
     - dwhuser
     - hosts
     - inventory
     - root

     > When you change the dwhuser, hosts, inventory, or root passwords, you have the option to use SHA-256 password hashing. This options requires that all clients accessing the accounts use SSL connections.

   - **Reset to Defaults**

     Resets encryption keys and passwords to default values. Default values are those provided during installation.

- **Exit**

  Exit the `securityadmin` tool.

Changing OnCommand Insight internal user passwords

Security policies might require you to change the passwords in your OnCommand Insight environment. Some of the passwords on one server exist on a different server in the environment, requiring that you change the password on both servers. For example, when you change the “inventory” user password on the Insight Server you must match the “inventory” user password on the Data Warehouse server Connector configured for that Insight Server.

Before you begin

> You should understand the dependencies of the user accounts before you change passwords. Failing to update passwords on all required servers will result in communication failures between the Insight components.

About this task

The following table lists the internal user passwords for the Insight Server and lists the Insight components that have dependent passwords that need to match the new password.

Insight Server Passwords	Required changes
_internal	
acquisition	LAU, RAU
dwh_internal	Data Warehouse
hosts	
inventory	Data Warehouse
root	

The following table lists the internal user passwords for the Data Warehouse and lists the Insight components that have dependent passwords that need to match the new password.

Data Warehouse Passwords	Required changes
cognos_admin	
dwh	

dwh_internal (Changed using the Server Connector configuration UI)	Insight server
dwhuser	
hosts	
inventory (Changed using the Server Connector configuration UI)	Insight server
root	

Changing passwords in the DWH Server Connection Configuration UI

The following table lists the user password for the LAU and lists the Insight components that have dependent passwords that need to match the new password.

LAU Passwords	Required changes
acquisition	Insight Server, RAU

Changing the “inventory” and “dwh_internal” passwords using the Server Connection Configuration UI

If you need to change the “inventory” or “dwh_internal” passwords to match those on the Insight server you use the Data Warehouse UI.

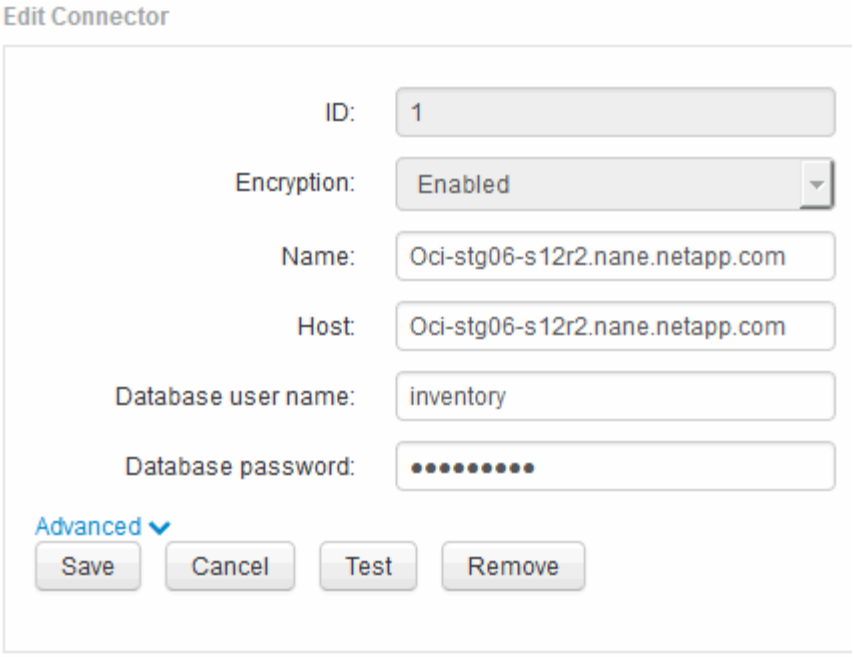
Before you begin

You must be logged in as administrator to perform this task.

Steps

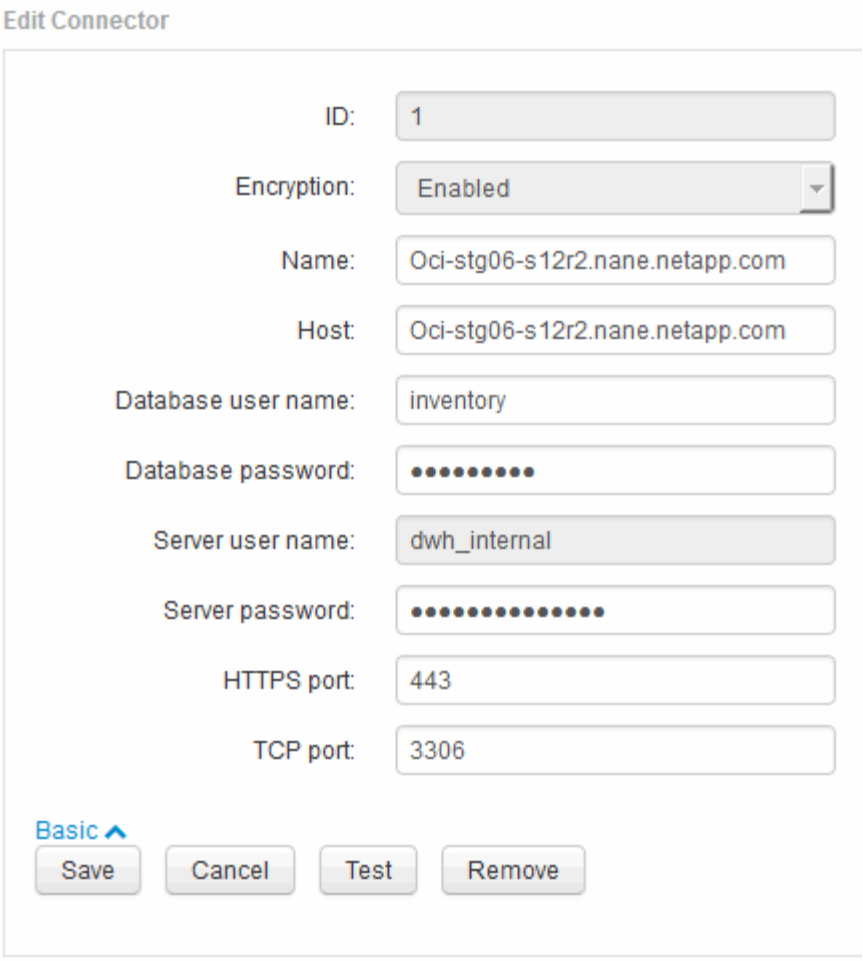
1. Log in to the Data Warehouse Portal at https://hostname/dwh, where hostname is the name of the system where OnCommand Insight Data Warehouse is installed.
2. From the navigation pane on the left, click **Connectors**.

   The **Edit Connector** screen is displayed.



3. Enter a new “inventory” password for the **Database password** field.
4. Click **Save**
5. To change the “dwh_internal” password, click **Advanced.**

   The Edit Connector Advanced screen is displayed.



6. Enter the new password in the **Server password** field:
7. Click save.

Changing the dwh password using the ODBC Administration tool

When you change the password on for the dwh user on the Insight server, the password must also be changed on the Data Warehouse server. You use the ODBC Data Source Administrator tool to change the password on the Data Warehouse.

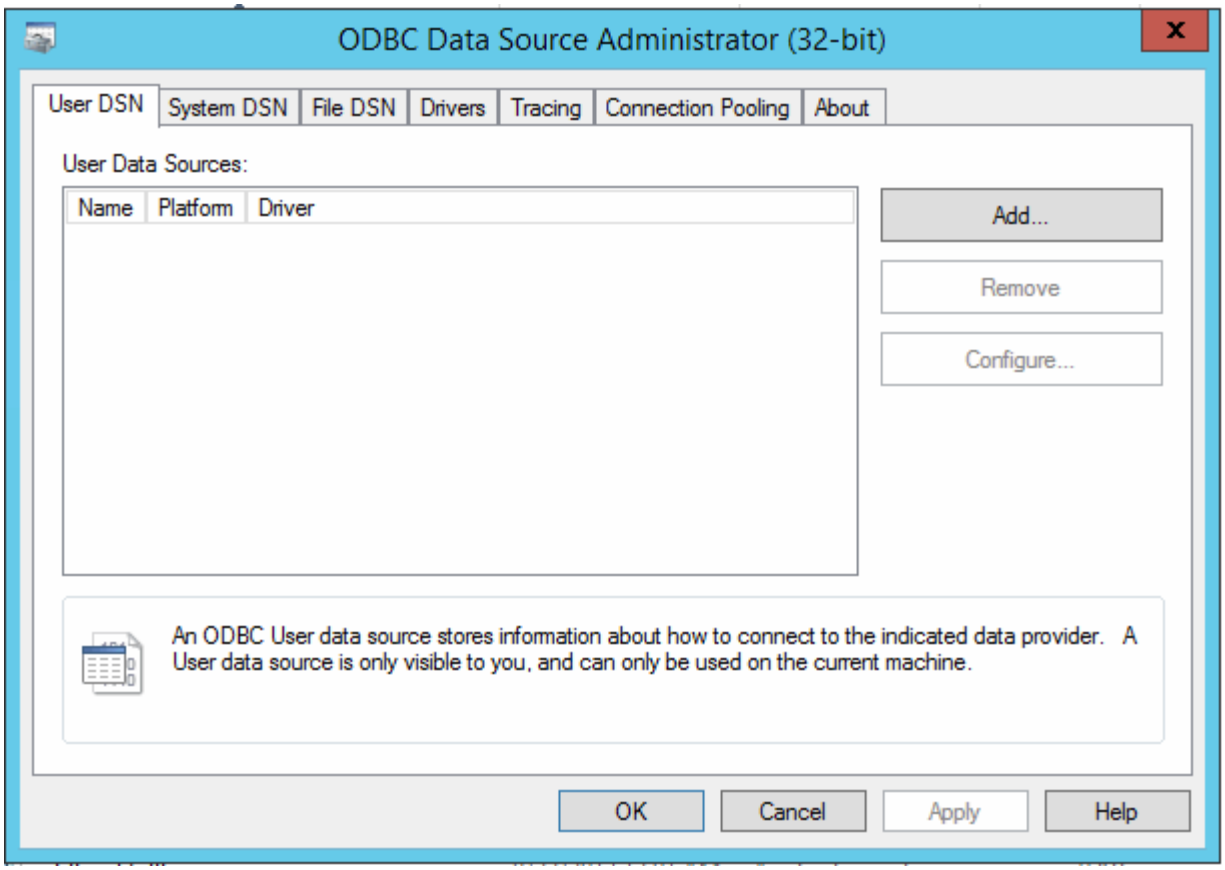
Before you begin

You must perform a remote login to the Data Warehouse server using an account with administrator privileges.

Steps

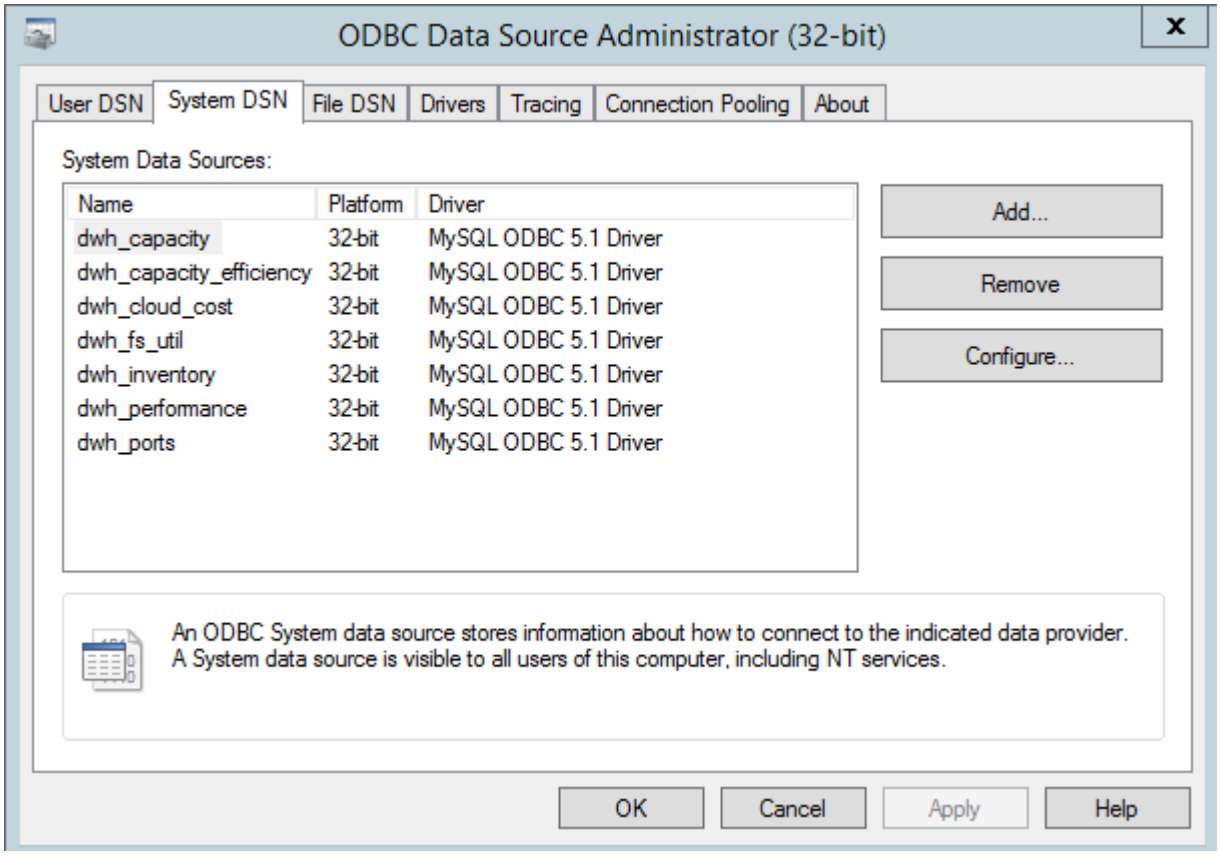
1. Perform a remote login to the server hosting that Data Warehouse.
2. Access the ODBC Administration tool at `C:\Windows\SysWOW64\odbcad32.exe`

   The system displays the ODBC Data Source Administrator screen.



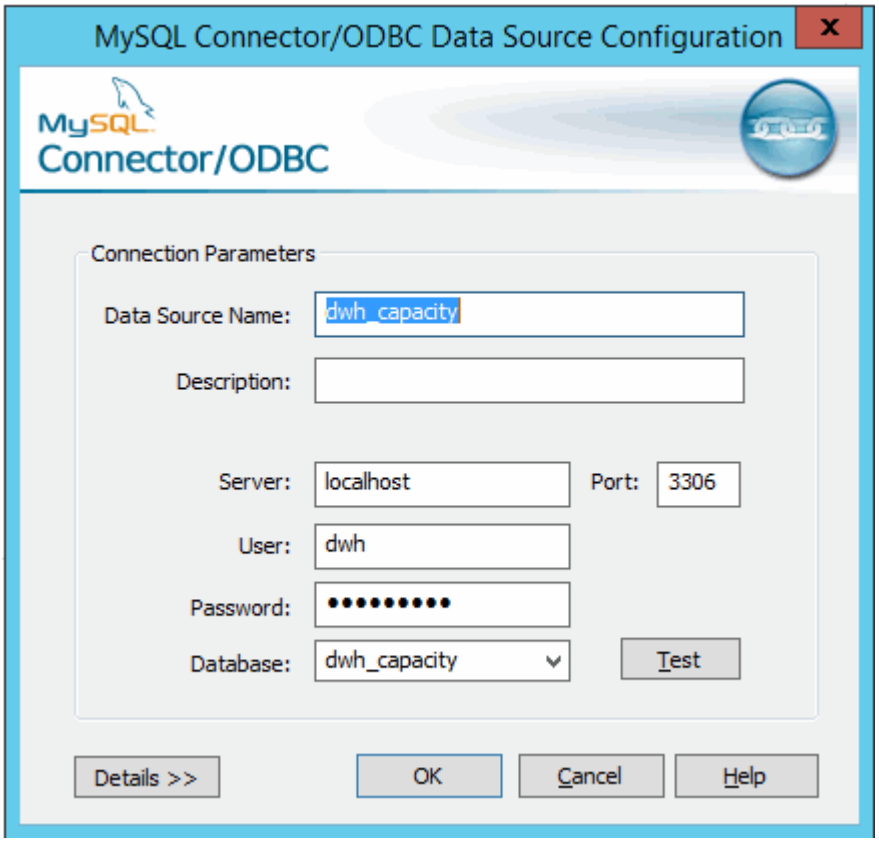
3. Click **System DSN**

   The system data sources are displayed.



4. Select an OnCommand Insight Data Source from the list.
5. Click **Configure**

   The Data Source Configuration screen is displayed.



6. Enter the new password in the **Password** field.

Smart Card and certificate login support

OnCommand Insight supports use of Smart Cards (CAC) and certificates to authenticate users logging in to the Insight servers. You must configure the system to enable these features.

After configuring the system to support CAC and certificates, navigating to a new session of OnCommand Insight results in the browser displaying a native dialog providing the user with a list of personal certificates to choose from. These certificates are filtered based on the set of personal certificates that have been issued by CAs trusted by the OnCommand Insight server. Most often, there is a single choice. By default, Internet Explorer skips this dialog if there is only one choice.

For CAC users, smart cards contain multiple certificates, only one of which can match the trusted CA. The CAC certificate for `identification` should be used.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Configuring hosts for Smart Card and certificate login

You must make modifications to the OnCommand Insight host configuration to support Smart Card (CAC) and certificate logins.

Before you begin

- LDAP must be enabled on the system.
- The LDAP `User principal account name` attribute must match the LDAP field that contains a user's ID.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Use the `regedit` utility to modify registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:
   a. Change the JVM_Option `DclientAuth=false` to `DclientAuth=true`.
2. Back up the keystore file: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Open a command prompt specifying `Run as administrator`

4. Delete the self-generated certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Generate a new certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Generate a certificate signing request (CSR): `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. After the CSR is returned in step 6, import the certificate, then export the certificate in Base-64 format and place it in `"C:\temp" named servername.cer`.
8. Extract the certificate from the keystore:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extract a private key from the p12 file: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Merge the Base-64 certificate that you exported in step 7 with the private key: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Import the merged certificate into the keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Import the root certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Import the root certificate into the server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Import the intermediate certificate: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"`

    Repeat this step for all intermediate certificates.

15. Specify the domain in LDAP to match this example.

1. Restart the server.

Configuring a client to support Smart Card and certificate login

Client machines require middleware and modifications to browsers to enable the use of Smart Cards and for certificate login. Customers who are already using Smart Cards should not require additional modifications to their client machines.

Before you begin

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

The following are the common client configuration requirements:

- Installing Smart Card middleware, such as ActivClient (see http://militarycac.com/activclient.htm)
- Modifying the IE browser (see http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdf)
- Modifying the Firefox browser (see https://militarycac.com/firefox2.htm)

Enabling CAC on a Linux server

Some modifications are required to enable CAC on a Linux OnCommand Insight server.

Steps

1. Navigate to `/opt/netapp/oci/conf/`
2. Edit `wildfly.properties` and change the value of `CLIENT_AUTH_ENABLED` to "True"
3. Import the “root certificate” that exists under `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. Restart the server

Configuring Data Warehouse for Smart Card and certificate login

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins.

Before you begin

- LDAP must be enabled on the system.
- The LDAP `User principal account name` attribute must match the LDAP field that contains a user's government ID number.

  The common name (CN) stored on government-issued CACs is normally in the following format: `first.last.ID`. For some LDAP fields, such as `sAMAccountName`, this format is too long. For these fields, OnCommand Insight extracts only the ID number from the CNs.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Use regedit to modify registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Change the JVM_Option `-DclientAuth=false` to `-DclientAuth=true`.

   For Linux, modify the `clientAuth` parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Add certificate authorities (CAs) to the Data Warehouse trustore:

   a. In a command window, go to `..\SANscreen\wildfly\standalone\configuration`.

   b. Use the `keytool` utility to list the trusted CAs: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      The first word in each line indicates the CA alias.

   c. If necessary, supply a CA certificate file, usually a `.pem` file. To include customer's CAs with Data Warehouse trusted CAs go to `..\SANscreen\wildfly\standalone\configuration` and use the `keytool` import command: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      my_alias is usually an alias that would easily identify the CA in the`keytool -list` operation.

3. On the OnCommand Insight server, the `wildfly/standalone/configuration/standalone-full.xml` file needs to be modified by updating verify-client to "REQUESTED" in

`/subsystem=undertow/server=default-server/https-listener=default-https`to enable CAC. Log in to the Insight server and run the appropriate command:

OS	Script
Windows	<install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

After executing the script, wait until the reload of the wildfly server is complete before proceeding to the next step.

4. Restart the OnCommand Insight server.

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.5 through 7.3.9)

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins for the Cognos server.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.5 through 7.3.9.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Add certificate authorities (CAs) to the Cognos trustore.
   a. In a command window, go to `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Use the `keytool` utility to list the trusted CAs: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      The first word in each line indicates the CA alias.

c. If no suitable files exist, supply a CA certificate file, usually a `.pem` file.

d. To include customer's CAs with OnCommand Insight trusted CAs, go to `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Use the `keytool` utility to import the `.pem` file: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` is usually an alias that would easily identify the CA in the`keytool -list` operation.

f. When prompted for a password, enter `NoPassWordSet`.

g. Answer `yes` when prompted to trust the certificate.

2. To enable CAC mode, execute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. To disable CAC mode, execute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.10 and later)

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins for the Cognos server.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Add certificate authorities (CAs) to the Cognos trustore.
   a. In a command window, go to `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Use the `keytool` utility to list the trusted CAs: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   The first word in each line indicates the CA alias.

c. If no suitable files exist, supply a CA certificate file, usually a `.pem` file.

d. To include customer's CAs with OnCommand Insight trusted CAs, go to `..\SANscreen\cognos\analytics\configuration\certs\`.

e. Use the `keytool` utility to import the `.pem` file: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` is usually an alias that would easily identify the CA in the`keytool -list` operation.

f. When prompted for a password, enter `NoPassWordSet`.

g. Answer `yes` when prompted to trust the certificate.

2. To enable CAC mode, do the following:

a. Configure CAC logout page, using the following steps:

- Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
- (Only for 7.3.10 and 7.3.11) Click Manage -> Configuration -> System -> Security
- (Only for 7.3.10 and 7.3.11) Enter cacLogout.html against Logout Redirect URL -> Apply
- Close browser.

b. Execute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Start IBM Cognos service. Wait for Cognos service to start.

3. To disable CAC mode, do the following:

a. Execute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Start IBM Cognos service. Wait for Cognos service to start.

c. (Only for 7.3.10 and 7.3.11) Unconfigure CAC logout page, using the following steps:

- Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
- Click Manage -> Configuration -> System -> Security
- Enter cacLogout.html against Logout Redirect URL -> Apply
- Close browser.

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.5 to 7.3.9)

You can add SSL certificates to enable enhanced authentication and encryption for your Data Warehouse and Cognos environment.

Before you begin

This procedure is for systems running OnCommnand Insight 7.3.5 through 7.3.9.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

You must have admin privileges to perform this procedure.

Steps

1. Create a backup of `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Create a backup of the “certs” and “csk” folders under `..\SANScreen\cognos\analytics\configuration`.
3. Generate a Certificate Encryption Request from Cognos. In an Admin CMD window, run:
   a. cd `“\Program Files\sanscreen\cognos\analytics\bin”`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. Open the `c:\temp\encryptRequest.csr` file and copy the generated content.
5. Send the encryptRequest.csr to the certificate authority (CA) to obtain an SSL certificate.

   Make sure to add additional attributes such as “SAN:dns=FQDN (For example, hostname.netapp.com)” to add the SubjectAltName. Google Chrome version 58 and later complains if the SubjectAltName is missing from the certificate.

6. Download the chain certificates by including root certificate by using PKCS7 format

   This will download fqdn.p7b file

7. Get a cert in .p7b format from your CA. Use a name that marks it as the certificate for the Cognos Webserver.
8. ThirdPartyCertificateTool.bat fails to import the entire chain, so multiple steps are required to export all certificates. Split the chain by exporting them individually as follows:
   a. Open the .p7b certificate in “Crypto Shell Extensions”.
   b. Browse in the left pane to “Certificates”.
   c. Right-click on root CA > All Tasks > Export.
   d. Select Base64 output.

e. Enter a file name identifying it as the root certificate.

f. Repeat steps 8a through 8c to export all of the certificates separately into .cer files.

g. Name the files intermediateX.cer and cognos.cer.

9. Ignore this step if you have only one CA certificate, otherwise merge both root.cer and intermediateX.cer into one file.

   a. Open intermediate.cer with NotePad and copy the content.

   b. Open root.cer with NotePad and save the content from 9a.

   c. Save the file as CA.cer.

10. Import the certificates into the Cognos keystore using the Admin CMD prompt:

    a. cd “Program Files\sanscreen\cognos\analytics\bin”

    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer

       This will set CA.cer as root Certificate Authority.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

       This will set Cognos.cer as encryption certificate which is signed by CA.cer.

11. Open the IBM Cognos Configuration.

    a. Select Local Configuration-→ Security -→ Cryptography -→ Cognos

    b. Change “Use third party CA?” to True.

    c. Save the configuration.

    d. Restart Cognos

12. Export the latest Cognos certificate into cognos.crt using the Admin CMD prompt:

    a. "D:\Program Files\SANscreen\java\bin\keytool.exe" -exportcert -file “c:\temp\cognos.crt” -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoPassWordSet -alias encryption

13. Import the “c:\temp\cognos.crt” into dwh trustore to establish SSL communication between Cognos and DWH, using the Admin CMD prompt window.

    a. "D:\Program Files\SANscreen\java\bin\keytool.exe" -importcert -file “c:\temp\cognos.crt” -keystore "D:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -storepass changeit -alias cognoscert

14. Restart the SANscreen service.

15. Perform a backup of DWH to make sure DWH communicates with Cognos.

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.10 and later)

You can add SSL certificates to enable enhanced authentication and encryption for your Data Warehouse and Cognos environment.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

You must have admin privileges to perform this procedure.

Steps

1. Stop Cognos using the IBM Cognos Configuration tool. Close Cognos.
2. Create backups of the `..\SANScreen\cognos\analytics\configuration` and `..\SANScreen\cognos\analytics\temp\cam\freshness` folders.
3. Generate a Certificate Encryption Request from Cognos. In an Admin CMD window, run:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Note: here -H and -I are to add subjectAltNames like dns and ipaddress.
4. Open the `c:\temp\encryptRequest.csr` file and copy the generated content.
5. Input the encryptRequest.csr content and generate certificate using CA signing portal.
6. Download the chain certificates by including root certificate by using PKCS7 format

   This will download fqdn.p7b file
7. Get a cert in .p7b format from your CA. Use a name that marks it as the certificate for the Cognos Webserver.
8. ThirdPartyCertificateTool.bat fails to import the entire chain, so multiple steps are required to export all certificates. Split the chain by exporting them individually as follows:
   a. Open the .p7b certificate in "Crypto Shell Extensions".
   b. Browse in the left pane to "Certificates".
   c. Right-click on root CA > All Tasks > Export.
   d. Select Base64 output.
   e. Enter a file name identifying it as the root certificate.
   f. Repeat steps 8a through 8e to export all of the certificates separately into .cer files.

g. Name the files intermediateX.cer and cognos.cer.

9. Ignore this step if you have only one CA certificate, otherwise merge both root.cer and intermediateX.cer into one file.
   a. Open root.cer with NotePad and copy the content.
   b. Open intermediate.cer with NotePad and append the content from 9a (intermediate first and root next).
   c. Save the file as chain.cer.
10. Import the certificates into the Cognos keystore using the Admin CMD prompt:
    a. cd “Program Files\sanscreen\cognos\analytics\bin”
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Open the IBM Cognos Configuration.
    a. Select Local Configuration-→ Security -→ Cryptography -→ Cognos
    b. Change “Use third party CA?” to True.
    c. Save the configuration.
    d. Restart Cognos
12. Export the latest Cognos certificate into cognos.crt using the Admin CMD prompt:
    a. cd "`C:\Program Files\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias encryption
13. Back up the DWH server trustore at `..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Import the “c:\temp\cognos.crt” into DWH trustore to establish SSL communication between Cognos and DWH, using the Admin CMD prompt window.
    a. cd "`C:\Program Files\SANscreen"
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass changeit -alias cognos3rdca
15. Restart the SANscreen service.
16. Perform a backup of DWH to make sure DWH communicates with Cognos.
17. The following steps should be performed even when only the “ssl certificate” is changed and the default Cognos certificates are left unchanged. Otherwise Cognos may complain about the new SANscreen certificate or be unable to create a DWH backup.
    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`
    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass changeit -alias “ssl certificate”`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    Typically, these steps are performed as part of the Cognos certificate import process described in How to

import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Configuring Data Warehouse for Smart Card and certificate login

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins.

Before you begin

- LDAP must be enabled on the system.
- The LDAP `User principal account name` attribute must match the LDAP field that contains a user's government ID number.

  The common name (CN) stored on government-issued CACs is normally in the following format: `first.last.ID`. For some LDAP fields, such as `sAMAccountName`, this format is too long. For these fields, OnCommand Insight extracts only the ID number from the CNs.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Use regedit to modify registry values in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Change the JVM_Option `-DclientAuth=false` to `-DclientAuth=true`.

   For Linux, modify the `clientAuth` parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Add certificate authorities (CAs) to the Data Warehouse trustore:

   a. In a command window, go to `..\SANscreen\wildfly\standalone\configuration`.

   b. Use the `keytool` utility to list the trusted CAs: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      The first word in each line indicates the CA alias.

c. If necessary, supply a CA certificate file, usually a `.pem` file. To include customer's CAs with Data Warehouse trusted CAs go to `..\SANscreen\wildfly\standalone\configuration` and use the `keytool` import command: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   my_alias is usually an alias that would easily identify the CA in the`keytool -list` operation.

3. On the OnCommand Insight server, the `wildfly/standalone/configuration/standalone-full.xml` file needs to be modified by updating verify-client to "REQUESTED" in `/subsystem=undertow/server=default-server/https-listener=default-https`to enable CAC. Log in to the Insight server and run the appropriate command:

OS	Script
Windows	<install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat
Linux	/opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   After executing the script, wait until the reload of the wildfly server is complete before proceeding to the next step.

4. Restart the OnCommand Insight server.

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.5 through 7.3.9)

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins for the Cognos server.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.5 through 7.3.9.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Add certificate authorities (CAs) to the Cognos trustore.
   a. In a command window, go to `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Use the `keytool` utility to list the trusted CAs: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      The first word in each line indicates the CA alias.

   c. If no suitable files exist, supply a CA certificate file, usually a `.pem` file.
   d. To include customer's CAs with OnCommand Insight trusted CAs, go to `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Use the `keytool` utility to import the `.pem` file: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` is usually an alias that would easily identify the CA in the`keytool -list` operation.

   f. When prompted for a password, enter `NoPassWordSet`.
   g. Answer `yes` when prompted to trust the certificate.
2. To enable CAC mode, execute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. To disable CAC mode, execute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.10 and later)

You must modify the OnCommand Insight Data Warehouse configuration to support Smart Card (CAC) and certificate logins for the Cognos server.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Steps

1. Add certificate authorities (CAs) to the Cognos trustore.
   a. In a command window, go to `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Use the `keytool` utility to list the trusted CAs: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      The first word in each line indicates the CA alias.

   c. If no suitable files exist, supply a CA certificate file, usually a `.pem` file.
   d. To include customer's CAs with OnCommand Insight trusted CAs, go to `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Use the `keytool` utility to import the `.pem` file: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` is usually an alias that would easily identify the CA in the`keytool -list` operation.

   f. When prompted for a password, enter `NoPassWordSet`.
   g. Answer `yes` when prompted to trust the certificate.
2. To enable CAC mode, do the following:
   a. Configure CAC logout page, using the following steps:
      - Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
      - (Only for 7.3.10 and 7.3.11) Click Manage -> Configuration -> System -> Security
      - (Only for 7.3.10 and 7.3.11) Enter cacLogout.html against Logout Redirect URL -> Apply
      - Close browser.
   b. Execute `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
   c. Start IBM Cognos service. Wait for Cognos service to start.
3. To disable CAC mode, do the following:
   a. Execute `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Start IBM Cognos service. Wait for Cognos service to start.

c. (Only for 7.3.10 and 7.3.11) Unconfigure CAC logout page, using the following steps:

- Logon to Cognos portal (user must be part of System Administrators group i.e. cognos_admin)
- Click Manage -> Configuration -> System -> Security
- Enter cacLogout.html against Logout Redirect URL -> Apply
- Close browser.

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.5 to 7.3.9)

You can add SSL certificates to enable enhanced authentication and encryption for your Data Warehouse and Cognos environment.

Before you begin

This procedure is for systems running OnCommnand Insight 7.3.5 through 7.3.9.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

You must have admin privileges to perform this procedure.

Steps

1. Create a backup of `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Create a backup of the “certs” and “csk” folders under `..\SANScreen\cognos\analytics\configuration`.
3. Generate a Certificate Encryption Request from Cognos. In an Admin CMD window, run:
   a. cd `“\Program Files\sanscreen\cognos\analytics\bin”`
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. Open the `c:\temp\encryptRequest.csr` file and copy the generated content.

5. Send the encryptRequest.csr to the certificate authority (CA) to obtain an SSL certificate.

   Make sure to add additional attributes such as “SAN:dns=FQDN (For example, hostname.netapp.com)” to add the SubjectAltName. Google Chrome version 58 and later complains if the SubjectAltName is missing from the certificate.

6. Download the chain certificates by including root certificate by using PKCS7 format

   This will download fqdn.p7b file

7. Get a cert in .p7b format from your CA. Use a name that marks it as the certificate for the Cognos Webserver.
8. ThirdPartyCertificateTool.bat fails to import the entire chain, so multiple steps are required to export all certificates. Split the chain by exporting them individually as follows:
   a. Open the .p7b certificate in “Crypto Shell Extensions”.
   b. Browse in the left pane to “Certificates”.
   c. Right-click on root CA > All Tasks > Export.
   d. Select Base64 output.
   e. Enter a file name identifying it as the root certificate.
   f. Repeat steps 8a through 8c to export all of the certificates separately into .cer files.
   g. Name the files intermediateX.cer and cognos.cer.
9. Ignore this step if you have only one CA certificate, otherwise merge both root.cer and intermediateX.cer into one file.
   a. Open intermediate.cer with NotePad and copy the content.
   b. Open root.cer with NotePad and save the content from 9a.
   c. Save the file as CA.cer.
10. Import the certificates into the Cognos keystore using the Admin CMD prompt:
    a. cd “Program Files\sanscreen\cognos\analytics\bin”
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\CA.cer

       This will set CA.cer as root Certificate Authority.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

       This will set Cognos.cer as encryption certificate which is signed by CA.cer.

11. Open the IBM Cognos Configuration.
    a. Select Local Configuration-→ Security -→ Cryptography -→ Cognos
    b. Change “Use third party CA?” to True.
    c. Save the configuration.
    d. Restart Cognos
12. Export the latest Cognos certificate into cognos.crt using the Admin CMD prompt:
    a. "D:\Program Files\SANscreen\java\bin\keytool.exe" -exportcert -file “c:\temp\cognos.crt” -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoPassWordSet -alias encryption

13. Import the “c:\temp\cognos.crt” into dwh trustore to establish SSL communication between Cognos and DWH, using the Admin CMD prompt window.
    a. "D:\Program Files\SANscreen\java\bin\keytool.exe" -importcert -file “c:\temp\cognos.crt” -keystore "D:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -storepass changeit -alias cognoscert
14. Restart the SANscreen service.
15. Perform a backup of DWH to make sure DWH communicates with Cognos.

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.10 and later)

You can add SSL certificates to enable enhanced authentication and encryption for your Data Warehouse and Cognos environment.

Before you begin

This procedure is for systems running OnCommand Insight 7.3.10 and later.

For the most up to date CAC and Certificate instructions, see the following Knowledgebase articles (Support login required):

- How to configure Common Access Card (CAC) authentication for OnCommand Insight
- How to configure Common Access Card (CAC) authentication for OnCommand Insight Data Warehouse
- How to create and import a Certificate Authority (CA) signed certificate into OnComand Insight and OnCommand Insight Data Warehouse 7.3.x
- How to create a Self Signed Certificate within OnCommand Insight 7.3.X installed on a Windows Host
- How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

About this task

You must have admin privileges to perform this procedure.

Steps

1. Stop Cognos using the IBM Cognos Configuration tool. Close Cognos.
2. Create backups of the `..\SANScreen\cognos\analytics\configuration` and `..\SANScreen\cognos\analytics\temp\cam\freshness` folders.
3. Generate a Certificate Encryption Request from Cognos. In an Admin CMD window, run:
    a. cd `“\Program Files\sanscreen\cognos\analytics\bin”`
    b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d “CN=server.domain.com,O=NETAPP,C=US” -H “server.domain.com” -I “ipaddress”`. Note: here -H and -I are to add subjectAltNames like dns and ipaddress.

4. Open the `c:\temp\encryptRequest.csr` file and copy the generated content.
5. Input the encryptRequest.csr content and generate certificate using CA signing portal.
6. Download the chain certificates by including root certificate by using PKCS7 format

   This will download fqdn.p7b file

7. Get a cert in .p7b format from your CA. Use a name that marks it as the certificate for the Cognos Webserver.
8. ThirdPartyCertificateTool.bat fails to import the entire chain, so multiple steps are required to export all certificates. Split the chain by exporting them individually as follows:
   a. Open the .p7b certificate in “Crypto Shell Extensions”.
   b. Browse in the left pane to “Certificates”.
   c. Right-click on root CA > All Tasks > Export.
   d. Select Base64 output.
   e. Enter a file name identifying it as the root certificate.
   f. Repeat steps 8a through 8e to export all of the certificates separately into .cer files.
   g. Name the files intermediateX.cer and cognos.cer.
9. Ignore this step if you have only one CA certificate, otherwise merge both root.cer and intermediateX.cer into one file.
   a. Open root.cer with NotePad and copy the content.
   b. Open intermediate.cer with NotePad and append the content from 9a (intermediate first and root next).
   c. Save the file as chain.cer.
10. Import the certificates into the Cognos keystore using the Admin CMD prompt:
    a. cd “Program Files\sanscreen\cognos\analytics\bin”
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. Open the IBM Cognos Configuration.
    a. Select Local Configuration-→ Security -→ Cryptography -→ Cognos
    b. Change “Use third party CA?” to True.
    c. Save the configuration.
    d. Restart Cognos
12. Export the latest Cognos certificate into cognos.crt using the Admin CMD prompt:
    a. cd "`C:\Program Files\SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias encryption
13. Back up the DWH server trustore at`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Import the “c:\temp\cognos.crt” into DWH trustore to establish SSL communication between Cognos and DWH, using the Admin CMD prompt window.

a. cd "`C:\Program Files\SANscreen"

b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass changeit -alias cognos3rdca

15. Restart the SANscreen service.
16. Perform a backup of DWH to make sure DWH communicates with Cognos.
17. The following steps should be performed even when only the “ssl certificate” is changed and the default Cognos certificates are left unchanged. Otherwise Cognos may complain about the new SANscreen certificate or be unable to create a DWH backup.

    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass changeit -alias “ssl certificate”`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    Typically, these steps are performed as part of the Cognos certificate import process described in How to import a Cognos Certificate Authority (CA) signed certificate into OnCommand DataWarehouse 7.3.3 and later

Importing SSL certificates

You can add SSL certificates to enable enhanced authentication and encryption for enhancing the security of your OnCommand Insight environment.

Before you begin

You must ensure that your system meets the minimum required bit level (1024 bits).

About this task

Before you attempt to perform this procedure, you should back up the existing `server.keystore` file, and name the backup `server.keystore.old`. Corrupting or damaging the `server.keystore` file may result in an inoperable Insight server after the Insight server is restarted. If you create a backup, you can revert to the old file if problems occur.

Steps

1. Create a copy of the original keystore file: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. 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"`

    a. When prompted for a password, enter `changeit`.

    The system displays the contents of the keystore. There should be at least one certificate in the keystore,

"ssl certificate".

3. Delete the "ssl certificate": `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Generate a new key: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. 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.
5. Generate a certificate request file: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

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

   Most organizations' CAs use a chain of trust model, including a root CA, which is often offline. It has signed the certificates for only a few child CAs, known as intermediate CAs.

   You must obtain the public key (certificates) for the entire chain of trust—the certificate for the CA that signed the certificate for the OnCommand Insight server, and all the certificates between that signing CA up to and including the organizational root CA.

   In some organizations, when you submit a signing request, you might receive one of the following:

   - A PKCS12 file that contains your signed certificate and all the public certificates in the chain of trust
   - A `.zip` file that contains individual files (including your signed certificate) and all the public certificates in the chain of trust

- Only your signed certificate

  You must obtain the public certificates.

7. Import the approved certificate for server.keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. When prompted, enter the keystore password.

      The following message is displayed: `Certificate reply was installed in keystore`

8. Import the approved certificate for server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. When prompted, enter the trustore password.

      The following message is displayed: `Certificate reply was installed in trustore`

9. Edit the `SANscreen\wildfly\standalone\configuration\standalone-full.xml` file:

   Substitute the following alias string: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. For example:

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir"
   keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
   02.muccbc.hq.netapp.com" key-
   password="${VAULT::HttpsRealm::key_password::1}"/>
   ```

10. Restart the SANscreen server service.

    Once Insight is running, you can click the padlock icon to view the certificates that are installed on the system.

    If you see a certificate containing "Issued To" information that matches "Issued By" information, you still have a self-signed certificate installed. The Insight installer-generated self-signed certificates have a 100-year expiration.

    NetApp cannot guarantee that this procedure will remove digital certificate warnings. NetApp cannot control how your end user workstations are configured. Consider the following scenarios:

    - Microsoft Internet Explorer and Google Chrome both utilize Microsoft's native certificate functionality on Windows.

      This means that if your Active Directory administrators push your organization's CA certificates into the end user's certificate trustores, the users of these browsers will see certificate warnings disappear when the OnCommand Insight self-signed certificates have been replaced with the one signed by the internal CA infrastructure.

    - Java and Mozilla Firefox have their own certificate stores.

      If your system administrators do not automate ingesting the CA certificates into these applications' trusted certificates stores, using the Firefox browser might continue to generate certificate warnings

because of an untrusted certificate, even when the self-signed certificate has been replaced. Getting your organization's certificate chain installed into the trustore is an additional requirement.

Setting up weekly backups for your Insight database

You might want to set up automatic weekly backups for your Insight database to protect your data. These automatic backups overwrite the files in the specified backup directory.

About this task

Best practice: When you are setting up the weekly backup of the OCI database, you need to store the backups on a different server than Insight is using, in case that server fails. Do not store any manual backups in the weekly backup directory because each weekly backup overwrites the files in the directory.

The backup file will contain the following:

- Inventory data
- Up to 7 days of performance data

Steps

1. On the Insight toolbar, click **Admin** > **Setup**.
2. Click the **Backup & Archive** tab.
3. In the Weekly Backup section, select **Enable weekly backup**.
4. Enter the path to the **Backup location**. This can be on the on the local Insight server or on a remote server that is accessible from the Insight server.

   The backup location setting is included in the backup itself, so if you restore the backup on another system, be aware that the backup folder location may be invalid on the new system. Double-check your backup location settings after restoring a backup.

5. Select the **Cleanup** option to keep either the last two or the last five backups.
6. Click **Save**.

Results

You can also go to **Admin** > **Troubleshooting** to create an on-demand backup.

What's included in the backup

Weekly and on-demand backups can be used for troubleshooting or migration.

The weekly or on-demand backup includes the following:

- Inventory data
- Performance data (if selected for inclusion in backup)
- Data sources and data source settings
- Integration packs

- Remote acquisition units
- ASUP/proxy settings
- Backup location settings
- Archive location settings
- Notification settings
- Users
- Performance policies
- Business entities and applications
- Device resolution rules and settings
- Dashboards and widgets
- Customized asset page dashboards and widgets
- Queries
- Annotations and annotation rules

The weekly backup does not include:

- Security tool settings / vault information (backed up via separate CLI process)
- Logs (can be saved to a .zip file on demand)
- Performance data (if not selected for inclusion in backup)
- Licenses

If you choose to include performance data in the backup, the most recent seven days of data is backed up. The remaining data will be in the archive if you have that feature enabled.

Performance data archiving

OnCommand Insight 7.3 introduces the ability to archive performance data on a daily basis. This supplements configuration and limited performance data backups.

OnCommand Insight retains up to 90 days of performance and violation data. However, when creating a backup of that data, only the most recent information is included in the backup. Archiving allows you to save the remainder of your performance data and load it as necessary.

Once the archive location is configured and archiving is activated, once a day Insight will archive the previous day's performance data for all objects into the archive location. Each day's archive is kept in the archive folder in a separate file. Archiving happens in the background and will continue as long as Insight is running.

The most recent 90 days of archives are retained; archive files older than 90 days are deleted as newer ones are created.

Enabling performance archive

To enable performance data archiving, follow these steps.

Steps

1. On the toolbar, click **Admin** > **Setup**.
2. Select the **Backup & Archive** tab.
3. In the Performance Archive section, ensure**Enable performance archive** is checked.
4. Specify a valid archive location.

   You cannot specify a folder under the Insight installation folder.

   Best Practice: Do not specify the same folder for archive as the Insight backup location.

5. Click **Save**.

   The archive process is handled in the background and does not interfere with other Insight activities.

Loading performance archive

To load the performance data archive, follow these steps.

Before you begin

Before loading the performance data archive, you must restore a valid weekly or manual backup.

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.

Configuring your email

You must configure OnCommand Insight to access your email system so that theOnCommand Insight Server can use your email to deliver reports, to which you subscribe, and transport support information for troubleshooting to NetApp technical support.

Email configuration prerequisites

Before you can configure OnCommand Insight to access your email system, you need to discover the host name or IP address to identify the (SMTP or Exchange) mail server and allocate an email account for OnCommand Insight reports.

Ask your email administrator to create an email account for OnCommand Insight. You will need the following information:

- The host name or IP address to identify the (SMTP or Exchange) mail server used by your organization. You can find this information through the application you use to read your email. In Microsoft Outlook, for example, you can find the name of the server by viewing your account configuration: Tools - E-mail accounts - View or change existing email account.
- Name of email account through which OnCommand Insight will send regular reports. The account must be a valid email address in your organization. (Most mail systems will not send messages unless they are sent from a valid user.) If the email server requires a user name and password in order to send mail, obtain this information from your system administrator.

Configuring your email for Insight

If your users want to receive Insight reports in their email accounts, you need to configure your email server to enable this feature.

Steps

1. On the Insight toolbar, click **Admin** and select **Notifications**.
2. Scroll down to the **Email** section of the page.
3. In the **Server** box, enter the name of your SMTP server in your organization, which is identified using either a hostname or an IP address (*nnn.nnn.nnn.nnn* format).

   If you specify a hostname, ensure that the name can be resolved through DNS.
4. In the **User name** box, enter your user name.
5. In the **Password** box, enter the password for accessing the email server, which is required only if your SMTP server is password-protected. This is the same password that you use to log into the application that lets you read your email. If a password is required, you must enter it a second time for verification.
6. In the **Sender email** box, enter the sender email account that will be identified as the sender on all OnCommand Insight reports.

   This account must be a valid email account within your organization.
7. In the **Email signature** box, enter the text that you want to be inserted in every email that is sent.
8. In the Recipients box, click ✚, enter an email address, and click **OK**.

   To edit an email address, select the address, and click ✎. To delete an email address, select the address, and click ✖.
9. To send a test email to specified recipients, click ✔.
10. Click **Save**.

Configuring SNMP notifications

OnCommand Insight supports SNMP notifications for configuration and Global Path policy changes as well as violations. For example, SNMP notifications are sent when data source thresholds are exceeded.

Before you begin

The following must have been completed:

- Identifying the IP address of the server that consolidates traps for each type of event.

  You might have to consult with your system administrator to obtain this information.

- Identifying the port number through which the designated machine obtains SNMP traps, for each type of event.

  The default port for SNMP traps is 162.

- Compiling the MIB at your site.

  The proprietary MIB comes with the installation software to support OnCommand Insight traps. The NetApp MIB is compatible with all standard SNMP management software and can be found on the Insight server in `<install dir>\SANscreen\MIBS\sanscreen.mib`.

Steps

1. Click **Admin** and select **Notifications**.
2. Scroll down to the **SNMP** section of the page.
3. Click **Actions** and select **Add trap source**.
4. In the **Add SNMP trap recipients** dialog box, enter these values:
   - **IP**

     The IP address to which OnCommand Insight sends SNMP trap messages.

   - **Port**

     The port number to which OnCommand Insight sends SNMP trap messages.

   - **Community String**

     Use “public” for SNMP trap messages.
5. Click **Save**.

Enabling the syslog facility

You can identify a location for the log of the OnCommand Insight violations and performance alerts as well as audit messages, and activate the logging process.

Before you begin

- You must have the IP address of the server on which to store the system log.
- You must know the facility level that corresponds to the type of program that is logging the message, such as LOCAL1 or USER.

About this task

The syslog includes the following types of information:

- Violation messages
- Performance alerts
- Optionally, Audit log messages

The following units are used in the syslog:

- Utilization metrics: percentage
- Traffic metrics: MB
- Traffic rate: MB/s

Steps

1. On the Insight toolbar, click **Admin** and select **Notifications**.
2. Scroll down to the **Syslog** section of the page.
3. Select the **Enable syslog** check box.
4. If desired, select the **Send audit** check box. New audit log messages will be sent to syslog in addition to being displayed on the Audit page. Note that already-existing audit log messages will not be sent to syslog; only newly-generated log messages will be sent.
5. In the **Server** field, enter the IP address of the log server.

   You can specify a custom port by appending it following a colon at the end of the server IP (e.g. server:port). If port is not specified, the default syslog port of 514 is used.

6. In the **Facility** field, select the facility level that corresponds to the type of program that is logging the message.
7. Click **Save**.

Insight syslog contents

You can enable a syslog on a server to collect Insight violation and performance alert messages that include utilization and traffic data.

Message types

The Insight syslog lists three types of messages:

- SAN path violations
- General violations
- Performance alerts

Data provided

Violation descriptions include the elements involved, time of the event, and relative severity or priority of the violation.

Performance alerts include these data:

- Utilization percentages
- Traffic types
- Traffic rate measured in MB

Configuring performance and assure violation notifications

OnCommand Insight supports notifications for performance and assure violations. By default, Insight does not send notifications for these violations; you must configure Insight to send email, to send syslog messages to the syslog server, or to send SNMP notifications when a violation occurs.

Before you begin

You must have configured email, syslog, and SNMP sending methods for violations.

Steps

1. Click **Admin** > **Notifications**.
2. Click **Events**.
3. In the **Performance Violations events** or **Assure Violations events** section, click the list for the notification method (**Email**, **Syslog**, or **SNMP**) you want, and select the severity level (**Warning and above** or **Critical**) for the violation.
4. Click **Save**.

Configuring system-level event notifications

OnCommand Insight supports notifications for system-level events such as acquisition unit failures or data source errors. To receive notifications you must configure Insight to send email when one or more of these events occur.

Before you begin

You must have configured email recipients for receiving notifications in **Admin** > **Notifications** > **Sending Methods**.

Steps

1. Click **Admin** > **Notifications**.
2. Click **Events**.
3. In the **System Alert Events** Email section, select the severity level (**Warning and above** or **Critical**) for the notification, or choose **Do not send** if you do not wish to receive notifications of system-level events.
4. Click **Save**.
5. Click **Admin** > **System Alerts** to configure the alerts themselves.
6. To Add a new alert, click **+Add** and give the alert a unique **Name**. You can also click the right-side icon to

Edit an existing alert.

7. Choose the **Event type** on which to alert, for example *Acquisition Unit Failure*.
8. Choose a **Snooze** interval to suppress notifications on duplicate events of the selected type for the selected time interval. If you select *Never*, you will receive repeat notifications once a minute until the event is no longer happening.
9. Choose a **Severity** (Warning or Critical) for the event notification.
10. Email notifications will be sent to the global email recipient list by default, or you can click the link provided to override the global list and send notifications to specific recipients.
11. Click Save to add the alert.

Configuring your ASUP processing

All NetApp products are equipped with automated capabilities to provide the best possible support for customers. The automated support (ASUP) periodically sends predefined and specific information to Customer Support. You can control the information to be forwarded to NetApp, and how often it is sent.

Before you begin

You must configure OnCommand Insight to forward data before any data is sent.

About this task

ASUP data is forwarded using the HTTPS protocol.

Steps

1. On the Insight toolbar, click **Admin**.
2. Click **Setup**.
3. Click the **ASUP & Proxy** tab.
4. In the **ASUP** section, select **Enable ASUP** to activate the ASUP facility.
5. If you want to change your corporate information, update the following fields:
   - **Company name**
   - **Site name**
   - **What to send**: Logs, configuration data, performance data
6. Click **Test Connection** to ensure that the connection that you specified works.
7. Click **Save**.
8. In the **Proxy** section, choose whether to **Enable Proxy**, and specify your proxy **host**, **port**, and **user** information.
9. Click **Test Connection** to ensure that the proxy that you specified works.
10. Click **Save**.

What's included in the Autosupport (ASUP) package

The Autosupport package contains the database backup as well as extended information.

The Autosupport package includes the following:

- Inventory data
- Performance data (if selected for inclusion in ASUP)
- Data sources and data source settings
- Integration packs
- Remote acquisition units
- ASUP/proxy settings
- Backup location settings
- Archive location settings
- Notification settings
- Users
- Performance policies
- Business entities and applications
- Device resolution rules and settings
- Dashboards and widgets
- Customized asset page dashboards and widgets
- Queries
- Annotations and annotation rules
- Logs
- Licenses
- Acquisition / data source status
- MySQL status
- System information

The Autosupport package does not include:

- Security tool settings / vault information (backed up via separate CLI process)
- Performance data (if not selected for inclusion in ASUP)

> If you choose to include performance data in the ASUP, the most recent seven days of data is included. The remaining data will be in the archive if you have that feature enabled. Archive data is not included in ASUP.

Defining applications

If you want to track data associated with specific applications running in your environment, you need to define those applications.

Before you begin

If you want to associate the application with a business entity, you must have already created the business entity.

About this task

You can associate applications with the following assets: hosts, virtual machines, volumes, internal volumes, qtrees, shares, and hypervisors.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Manage** and select **Applications**.

   After you define an application, the Applications page displays the application's name, its priority, and, if applicable, the business entity associated with the application.

3. Click **Add**.

   The Add Application dialog box displays.

4. Enter a unique name for the application in the **Name** box.
5. Click **Priority** and select the priority (critical, high, medium, or low) for the application in your environment.
6. If you plan to use this application with a business entity, click **Business Entity** and select the entity from the list.
7. **Optional**: If you do not use volume sharing, click to clear the **Validate volume sharing** box.

   This requires the Assure license. Set this when you want to ensure each host has access to the same volumes in a cluster. For example, hosts in high-availability clusters often need to be masked to the same volumes to allow for failover; however, hosts in unrelated applications usually have no need to access the same physical volumes. Additionally, regulatory policies might require you to explicitly disallow unrelated applications from accessing the same physical volumes for security reasons.

8. Click **Save**.

   The application appears in the Applications page. If you click the application's name, Insight displays the asset page for the application.

After you finish

After defining an application, you can go to an asset page for host, virtual machine, volume, internal volume, or hypervisor to assign an application to an asset.

Assigning applications to assets

After defining applications with or without business entities, you can associate the applications with assets.

Steps

1. Log in to the OnCommand Insight web UI.
2. Locate the asset (host, virtual machine, volume, or internal volume) to which you want to apply the application by doing either of the following:
   - Click **Dashboard**, select **Assets Dashboard**, and click the asset.
   - Click on the toolbar to display the **Search assets** box, type the name of the asset, and then select the asset from the list.
3. In the **User Data** section of the asset page, position your cursor over the name of the application currently assigned to the asset (if there is no application assigned, **None** displays instead) and then click (Edit application).

   The list of available applications for the selected asset display. The applications that are currently associated with the asset are preceded by a check mark.
4. You can type in the Search box to filter the application names, or you can scroll down the list.
5. Select the applications you want to associate with the asset.

   You can assign multiple applications to host, virtual machine, and internal volume; however, you can only assign one application to volume.
6. Click to assign the selected application or applications to the asset.

   The application names appear in the User Data section; if the application is associated with a business entity, the name of the business entity appears in this section also.

Editing applications

You might want to change an application's priority, the business entity associated with an application, or the status of volume sharing.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Manage** and select **Applications**.
3. Position your cursor over the application you want to edit and click .

   The Edit Application dialog box displays.
4. Do any of the following:
   - Click **Priority** and select a different priority.

     You cannot change the application's name.
   - Click **Business Entity** and select a different business entity to associate the application with or select **None** to remove the association of the application with the business entity.
   - Click to clear or select **Validate volume sharing**.

This option is only available if you have the Assure license.

5. Click **Save**.

Deleting applications

You might want to delete an application when it no longer fulfills a need in your environment.

Steps

1. Log in to the Insight web UI.
2. Click **Manage** and select **Applications**.
3. Position your cursor over the application you want to delete and click .

   A confirmation dialog box is displayed, asking if you want to delete the application.

4. Click **OK**.

Your business entities hierarchy

You can define business entities to track and report on your environment data at a more granular level.

In OnCommand Insight, the business entities hierarchy contains these levels:

- **Tenant** is primarily used by service providers to associate resources with a customer, for example, NetApp.
- **Line of Business (LOB)** is a line of business or product line within a company, for example, Data Storage.
- **Business Unit** represents a traditional business unit such as Legal or Marketing.
- **Project** is often used to identify a specific project within a business unit for which you want capacity chargeback. For example, "Patents" might be a project name for the Legal business unit and "Sales Events" might be a project name for the Marketing business unit. Note that level names may include spaces.

You are not required to use all of the levels in the design of your corporate hierarchy.

Designing your business entities hierarchy

You need to understand the elements of your corporate structure and what needs to be represented in the business entities because they become a fixed structure in your OnCommand Insight database. You can use the following information to set up your business entities. Remember you do not need to use all of the hierarchy levels to gather data in these categories.

Steps

1. Examine each level of the business entities hierarchy to determine if that level should be included in your business entity hierarchy for your company:

- **Tenant** level is needed if your company is an ISP and you want to track customer usage of resources.
- **Line of Business (LOB)** is needed in the hierarchy if the data for different product lines needs to be tracked.
- **Business Unit** is required if you need to track data for different departments. This level of the hierarchy is often valuable in separating a resource that one department uses that other departments do not.
- **Project** level can be used for specialized work within a department. This data might be useful to pinpoint, define, and monitor a separate project's technology needs compared to other projects in a company or department.

2. Create a chart showing each business entity with the names of all of the levels within the entity.
3. Check the names in the hierarchy to be certain they will be self-explanatory in OnCommand Insight views and reports.
4. Identify all applications that are associated with each business entity.

Creating business entities

After designing the business entities hierarchy for your company, you can set up applications and then associate the business entities with the applications. This process creates the business entities structure in your OnCommand Insight database.

About this task

Associating applications with business entities is optional; however, it is a best practice.

Steps

1. Log in to the Insight web UI.
2. Click **Manage** and select **Business entities**.

   The Business Entities page displays.

3. Click + Add to begin building a new entity.

   The **Add Business Entity** dialog box displays.

4. For each entity level (Tenant, Line of Business, Business Unit, and Project), you can do any of the following:
   - Click the entity level list and select a value.
   - Type a new value and press Enter.
   - Leave the entity level value as N/A if you do not want to use the entity level for the business entity.
5. Click **Save**.

Assigning business entities to assets

You can assign a business entity to an asset (host, port, storage, switch, virtual machine, qtree, share, volume, or internal volume) without having associated the business entity to an application; however, business entities are assigned automatically to an asset if that asset is associated with an application related to a business entity.

Before you begin

You must have already created a business entity.

About this task

While you can assign business entities directly to assets, it is recommended that you assign applications to assets and then assign business entities to assets.

Steps

1. Log in to the OnCommand Insight web UI.
2. Locate the asset to which you want to apply the business entity by doing either of the following:
   - Click on the asset in the Assets Dashboard.
   - Click on the toolbar to display the **Search assets** box, type the name of the asset, and then select the asset from the list.
3. In the **User Data** section of the asset page, position your cursor over **None** next to **Business Entities** and then click .

   The list of available business entities display.

4. Type in the **Search** box to filter the list for a specific entity or scroll down the list; select a business entity from the list.

   If the business entity you choose is associated with an application, the application name is displayed. In this case, the word “derived” appears next to the business entity name. If you want to maintain the entity for only the asset and not the associated application, you can manually override the assignment of the application.

5. To override an application derived from a business entity, place your cursor over the application name and click , select another business entity, and select another application from the list.

Assigning business entities to or removing business entities from multiple assets

You can assign business entities to or remove business entities from multiple assets by using a query instead of having to manually assign or remove them.

Before you begin

You must have already created the business entities you want to add to your desired assets.

Steps

1. Create a new query, or open an existing query.
2. If desired, filter for the assets to which you want to add business entities.
3. Select the desired assets in the list or click to select **All**.

   The **Actions** button displays.

4. To add a business entity to the selected assets, click Actions. If the selected asset type can have business entities assigned to it, you will see the menu choice to **Add Business Entity**. Select this.

5. Select the desired business entity from the list and click **Save**.

   Any new business entity you assign overrides any business entities that were already assigned to the asset. Assigning applications to assets will also override the business entities assigned in the same way. Assigning business entities to as asset may also override any applications assigned to that asset.

6. To remove a business entity assigned to the assets, click 

and select **Remove Business Entity**.
7. Select the desired business entity from the list and click **Delete**.

Defining annotations

When customizing OnCommand Insight to track data for your corporate requirements, you can define any specialized annotations needed to provide a complete picture of your data: for example, asset end of life, data center, building location, storage tier, or volume, and internal volume service level.

Steps

1. List any industry terminology to which environment data must be associated.
2. List corporate terminology to which environment data must be associated, which is not already being tracked using the business entities.
3. Identify any default annotation types that you might be able to use.
4. Identify which custom annotations you need to create.

Using annotations to monitor your environment

When customizing OnCommand Insight to track data for your corporate requirements, you can define specialized notes, called *annotations*, and assign them to your assets. For example, you can annotate assets with information such as asset end of life, data center, building location, storage tier, or volume service level.

Using annotations to help monitor your environment includes the following high-level tasks:

- Creating or edit definitions for all annotation types.
- Displaying asset pages and associating each asset with one or more annotations.

  For example, if an asset is being leased and the lease expires within two months, you might want to apply an end-of-life annotation to the asset. This helps prevent others from using that asset for an extended time.

- Creating rules to automatically apply annotations to multiple assets of the same type.
- Using the annotation import utility to import annotations.
- Filter assets by their annotations.
- Grouping data in reports based on annotations and generate those reports.

  See the *OnCommand Insight Reporting Guide* for more information about reports.

Managing annotation types

OnCommand Insight provides some default annotation types, such as asset life cycle (birthday or end of life), building or data center location, and tier, that you can customize to show in your reports. You can define values for default annotation types or create your own custom annotation types. You can later edit those values.

Default annotation types

OnCommandInsight provides some default annotation types. These annotations can be used to filter or group data and to filter data reporting.

You can associate assets with default annotation types such as the following:

- Asset life cycle, such as birthday, sunset, or end of life
- Location information about a device, such as data center, building, or floor
- Classification of assets, such as by quality (tiers), by connected devices (switch level), or by service level
- Status, such as hot (high utilization)

The following table lists the default annotation types. You can edit any of these annotation names to suit your needs.

Annotation types	Description	Type
Alias	User-friendly name for a resource.	Text
Birthday	Date when the device was or will be brought online.	Date
Building	Physical location of host, storage, switch, and tape resources.	List
City	Municipality location of host, storage, switch, and tape resources.	List
Compute Resource Group	Group assignment used by the Host and VM Filesystems data source.	List
Continent	Geographic location of host, storage, switch, and tape resources.	List
Country	National location of host, storage, switch, and tape resources.	List

Data Center	Physical location of the resource and is available for hosts, storage arrays, switches, and tapes.	List
Direct Attached	Indicates (Yes or No) if a storage resource is connected directly to hosts.	Boolean
End of Life	Date when a device will be taken offline, for example, if the lease expired or the hardware is being retired.	Date
Fabric Alias	User-friendly name for a fabric.	Text
Floor	Location of a device on a floor of a building. Can be set for hosts, storage arrays, switches, and tapes.	List
Hot	Devices already in heavy use on a regular basis or at the threshold of capacity.	Boolean
Note	Comments that you want associated with a resource.	Text
Rack	Rack in which the resource resides.	Text
Room	Room within a building or other location of host, storage, switch, and tape resources.	List
SAN	Logical partition of the network. Available on hosts, storage arrays, tapes, switches, and applications.	List
Service Level	A set of supported service levels that you can assign to resources. Provides an ordered options list for internal volumes, qtree, and volumes. Edit service levels to set performance policies for different levels.	List
State/Province	State or province in which the resource is located.	List

Sunset	Threshold set after which no new allocations can be made to that device. Useful for planned migrations and other pending network changes.	Date
Switch Level	Includes predefined options for setting up categories for switches. Typically, these designations remain for the life of the device, although you can edit them, if needed. Available only for switches.	List
Tier	Can be used to define different levels of service within your environment. Tiers can define the type of level, such as speed needed (for example, gold or silver). This feature is available only on internal volumes, qtrees, storage arrays, storage pools, and volumes.	List
Violation Severity	Rank (for example, major) of a violation (for example, missing host ports or missing redundancy), in a hierarchy of highest to lowest importance.	List

Alias, Data Center, Hot, Service Level, Sunset, Switch Level, Service Level, Tier, and Violation Severity are system-level annotations, which you cannot delete or rename; you can change only their assigned values.

How annotations are assigned

You can assign annotations manually or automatically using annotation rules. OnCommand Insight also automatically assigns some annotations on acquisition of assets and by inheritance. Any annotations that you assign to an asset appear in the User Data section of the asset page.

Annotations are assigned in the following ways:

- You can assign an annotation manually to an asset.

  If an annotation is assigned directly to an asset, the annotation appears as normal text on an asset page. Annotations that are assigned manually always take precedence over annotations that are inherited or assigned by annotation rules.

- You can create an annotation rule to automatically assign annotations to assets of the same type.

If the annotation is assigned by rule, Insight displays the rule name next to the annotation name on an asset page.

- Insight automatically associates a tier level with a storage tier model to expedite the assignment of storage annotations to your resources on acquisition of assets.

  Certain storage resources are automatically associated with a predefined tier (Tier 1 and Tier 2). For example, the Symmetrix storage tier is based on the Symmetrix and VMAX family and is associated with Tier 1. You can change the default values to match your tier requirements. If the annotation is assigned by Insight (for example, Tier), you see “System-defined” when you position your cursor over the annotation’s name on an asset page.

- A few resources (children of an asset) can derive the predefined Tier annotation from their asset (parent).

  For example, if you assign an annotation to a storage, the Tier annotation is derived by all the storage pools, internal volumes, volumes, qtrees, and shares belonging to the storage. If a different annotation is applied to an internal volume of the storage, the annotation is subsequently derived by all the volumes, qtrees, and shares. “Derived” appears next to the annotation name on an asset page.

Associating costs with annotations

Prior to running cost-related reports, you should associate costs with the Service Level, Switch Level, and Tier system-level annotations, which enables chargeback to the storage users based on their actual usage of production and replicated capacity. For example, for the Tier level, you might have gold and silver tier values and assign a higher cost to the gold tier than to the silver tier.

Steps

1. Log in to the Insightweb UI.
2. Click Manage and select **Annotations**.

   The Annotation page displays.

3. Position your cursor over the Service Level, Switch Level, or Tier annotation, and click .

   The Edit Annotation dialog box displays.

4. Enter the values for any existing levels in the **Cost** field.

   The Tier and Service Level annotations have Auto Tier and Object Storage values, respectively, which you cannot remove.

5. Click + Add to add additional levels.
6. Click **Save** when you finish.

Creating custom annotations

Using annotations, you can add custom business-specific data that matches your business needs to assets. While OnCommand Insight provides a set of default annotations, you might find that you want to view data in other ways. The data in custom

annotations supplements device data already collected, such as switch manufacturer, number of ports, and performance statistics. The data you add using annotations is not discovered by Insight.

Steps

1. Log in to the Insight web UI.
2. Click **Manage** and select **Annotations**.

   The Annotations page displays the list of annotations.

3. Click + Add.

   The **Add Annotation** dialog box displays.

4. Enter a name and a description in the **Name** and **Description** fields.

   You can enter up to 255 characters in these fields.

   Annotation names beginning or ending with a dot "." are not supported.

5. Click **Type** and then select one of the following options that represents the type of data allowed in this annotation:

   - Boolean

     This creates a drop-down list with the choices of yes and no. For example, the “Direct Attached” annotation is Boolean.

   - Date

     This creates a field that holds a date. For example, if the annotation will be a date, select this.

   - List

     This can create either of the following:

     - A drop-down fixed list

       When others are assigning this annotation type on a device, they cannot add more values to the list.

     - A drop-down flexible list

       If you select the **Add new values on the fly** option when you create this list, when others are assigning this annotation type on a device, they can add more values to the list.

   - Number

     This creates a field where the user assigning the annotation can enter a number. For example, if the annotation type is “Floor”, the user could select the Value Type of “number” and enter the floor number.

   - Text

This creates a field that allows free-form text. For example, you might enter “Language” as the annotation type, select “Text” as the value type, and enter a language as a value.

After you set the type and save your changes, you cannot change the type of the annotation. If you need to change the type, you have to delete the annotation and create a new one.

6. If you select **List**as the annotation type, do the following:
   a. Select **Add new values on the fly** if you want the ability to add more values to the annotation when on an asset page, which creates a flexible list.

      For example, suppose you are on an asset page and the asset has the City annotation with the values Detroit, Tampa, and Boston. If you selected the **Add new values on the fly** option, you can add additional values to City like San Francisco and Chicago directly on the asset page instead of having to go to the Annotations page to add them. If you do not choose this option, you cannot add new annotation values when applying the annotation; this creates a fixed list.

   b. Enter a value and a name in **Value** and **Description** fields.
   c. Click 

to add additional values.
   d. Click to remove a value.
7. Click **Save**.

Your annotations appear in the list on the Annotations page.

Related information

Importing and Exporting user data

Manually assigning annotations to assets

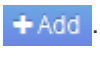
Assigning annotations to assets helps you sort, group, and report on assets in ways that are relevant to your business. Although you can assign annotations to assets of a particular type automatically, using annotation rules, you can assign annotations to an individual asset by using its asset page.

Before you begin

You must have created the annotation you want to assign.

Steps

1. Log in to the OnCommand Insight web UI.
2. Locate the asset to which you want to apply the annotation by doing either of the following:
   - Click the asset in the Assets Dashboard.
   - Click on the toolbar to display the **Search assets** box, type the type of or name of the asset, and then select the asset from the list that displays.

     The asset page displays.
3. In the **User Data** section of the asset page, click 

.

The Add Annotation dialog box displays.

4. Click **Annotation** and select an annotation from the list.
5. Click **Value** and do either of the following, depending on type of annotation you selected:
   - If the annotation type is list, date, or Boolean, select a value from the list.
   - If the annotation type is text, type a value.
6. Click **Save**.
7. If you want to change the value of the annotation after you assign it, click and select a different value.

   If the annotation is of list type for which the **Add values dynamically upon annotation assignment** option is selected, you can type to add a new value in addition to selecting an existing value.

Modifying annotations

You might want to change the name, description, or values for an annotation, or delete an annotation that you no longer want to use.

Steps

1. Log in to the OnCommand Insightweb UI.
2. Click **Manage** and select **Annotations**.

   The Annotations page displays.

3. Position your cursor over the annotation you want to edit and click .

   The **Edit Annotation** dialog box displays.

4. You can make the following modifications to an annotation:
   a. Change the name, description, or both.

      However, note that you can enter a maximum of 255 characters for both the name and description, and you cannot change the type of any annotation. Additionally, for system-level annotations, you cannot change the name or description; however, you can add or remove values if the annotation is a list type.

      If a custom annotation is published to the Data Warehouse and you rename it, you will lose historical data.

   b. To add another value to an annotation of list type, click + Add.
   c. To remove a value from an annotation of list type, click .

      You cannot delete an annotation value if that value is associated with an annotation contained in an annotation rule, query, or performance policy.

5. Click **Save** when you finish.

After you finish

If you are going to use annotations in the Data Warehouse, you need to force an update of annotations in the Data Warehouse. Refer to the *OnCommand Insight Data Warehouse Administration Guide*.

Deleting annotations

You might want to delete an annotation that you no longer want to use. You cannot delete a system-level annotation or an annotation that is used in an annotation rule, query, or performance policy.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Manage** and select **Annotations**.

   The Annotations page displays.

3. Position your cursor over the annotation you want to delete, and click .

   A confirmation dialog box displays.

4. Click **OK**.

Assigning annotations to assets using annotation rules

To automatically assign annotations to assets based on criteria that you define, you configure annotation rules. OnCommand Insight assigns the annotations to assets based on these rules. Insight also provides two default annotation rules, which you can modify to suit your needs or remove if you do not want to use them.

Default storage annotation rules

To expedite the assignment of storage annotations to your resources, OnCommand Insight includes 21 default annotation rules, which associate a tier level with a storage tier model. All of your storage resources are automatically associated with a tier upon acquisition of the assets in your environment.

The default annotation rules apply a tier annotations in the following way:

- Tier 1, storage quality tier

  The Tier 1 annotation is applied to the following vendors and their specified families: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 or FAS6200), and Violin (Memory).

- Tier 2, storage quality tier

  The Tier 2 annotation is applied to the following vendors and their specified families: HP (3PAR StoreServ or EVA), EMC (CLARiiON), HDS (AMS or D800), IBM (XIV), and NetApp (FAS3000, FAS3100, and FAS3200).

You can edit the default settings of these rules to match your tier requirements, or you can remove them if you do not need them.

Creating annotation rules

As an alternative to manually applying annotations to individual assets, you can automatically apply annotations to multiple assets using annotation rules. Annotations set manually on an individual asset pages take precedence over rule-based annotations when Insight evaluates the annotation rules.

Before you begin

You must have created a query for the annotation rule.

About this task

Although you can edit the annotation types while you are creating the rules, you should have defined the types ahead of time.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Manage** and select **Annotation rules**.

   The Annotation Rules page displays the list of existing annotation rules.
3. Click + Add.

   The Add Rule dialog box displays.
4. Do the following:
   a. In the **Name** box, enter a unique name that describes the rule.

      This name will appear in the Annotation Rules page.

   b. Click **Query** and select the query that OnCommand Insight should use to apply the annotation to assets.
   c. Click **Annotation** and select the annotation you want to apply.
   d. Click **Value** and select a value for the annotation.

      For example, if you choose Birthday as the annotation, you specify a date for the value.
5. Click **Save**.
6. Click **Run all rules** if you want to run all the rules immediately; otherwise, the rules are run at a regularly scheduled interval.

Setting annotation rule precedence

By default, OnCommand Insight evaluates annotation rules sequentially; however, you can configure the order in which OnCommand Insight evaluates annotation rules if you want Insight to evaluate rules in a specific order.

Steps

1. Log in to the Insightweb UI.
2. Click **Manage** and select **Annotation rules**.

   The Annotation Rules page displays the list of existing annotation rules.

3. Position your cursor over an annotation rule.

   The precedence arrows appear to the right of the rule.

4. To move a rule up or down in the list, click the up arrow or the down arrow.

   By default, new rules are added sequentially to the list of rules. Annotations set manually on an individual asset pages take precedence over rule-based annotations when Insight evaluates the annotation rules.

Modifying annotation rules

You can modify an annotation rule to change the rule's name, its annotation, the annotation's value, or the query associated with the rule.

Steps

1. Log in to the OnCommand Insightweb UI.
2. Click **Manage** and select **Annotation rules**.

   The Annotation Rules page displays the list of existing annotation rules.

3. Locate the rule that you want to modify:
   - On the Annotation Rules page, you can filter the annotation rules by entering a value in the filter box.
   - Click a page number to browse through the annotation rules by page if there are more rules than fit on a page.
4. Perform one of the following to display the **Edit Rule** dialog box:
   - If you are on theAnnotation Rules page, position your cursor over the annotation rule and click  .
   - If you are on an asset page, position your cursor over the annotation associated with the rule, position your cursor over the rule name when it displays, and then click the rule name.
5. Make the required changes and click **Save**.

Deleting annotation rules

You can delete an annotation rule when the rule is no longer required to monitor the objects in your network.

Steps

1. Log in to the OnCommand Insightweb UI.
2. Click **Manage**, and select **Annotation rules**.

   The Annotation Rules page displays the list of existing annotation rules.

3. Locate the rule that you want to delete:
   - On the Annotation Rules page, you can filter the annotation rules by entering a value in the filter box.
   - Click a page number to browse through the annotation rules by page if there are more rules than fit on a single page.
4. Point the cursor over the rule that you want to delete, and then click .

   A confirmation message is displayed, prompting whether you want to delete the rule.
5. Click **OK**.

Importing annotation values

If you maintain annotations on SAN objects (such as storage, hosts, and virtual machines) in a CSV file, you can import that information into OnCommand Insight. You can import applications, business entities, or annotations such as tier and building.

About this task

The following rules apply:

- If an annotation value is empty, that annotation is removed from the object.
- When annotating volumes or internal volumes, the object name is a combination of storage name and volume name using the dash and arrow (->) separator:

  ```
  <storage_name>-><volume_name>
  ```

- When storage, switches, or ports are annotated, the Application column is ignored.
- The columns of Tenant, Line_of_Business, Business_Unit, and Project make up a business entity.

  Any of the values can be left empty. If an application is already related with a business entity different from the input values, the application is assigned to the new business entity.

The following object types and keys are supported in the import utility:

Type	Key
Host	`id-><id>` or `<Name>` or `<IP>`
VM	`id-><id>` or `<Name>`
Storage pool	`id-><id>` or `<Storage_name>-><Storage_Pool_name>`
Internal volume	`id-><id>` or `<Storage_name>-><Internal_volume_name>`

Volume	`id-><id>` or `<Storage_name>-><Volume_name>`
Storage	`id-><id>` or `<Name>` or `<IP>`
Switch	`id-><id>` or `<Name>` or `<IP>`
Port	`id-><id>` or `<WWN>`
Share	`id-><id>` or `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree>` is optional if there is a default qtree.
Qtree	`id-><id>` or `<Storage Name>-><Internal Volume Name>-><Qtree Name>`

The CSV file should use the following format:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

Steps

1. Log in to the Insight web UI.
2. Click **Admin** and select **Troubleshooting**.

   The Troubleshooting page displays.
3. In the **Other tasks section** of the page, click the **OnCommand Insight Portal** link.
4. Click **Insight Connect API**.
5. Log in to the portal.
6. Click **Annotation Import Utility**.
7. Save the `.zip` file, unzip it, and read the `readme.txt` file for additional information and samples.

8. Place the CSV file in same folder as the `.zip` file.
9. In the command line window, enter the following:

```
java -jar rest-import-utility.jar [-uusername] [-ppassword]
[-aserver name or IP address] [-bbatch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

The -l option, which enables extra logging, and the -c option, which enables case sensitivity, are set to false by default. Therefore, you must specify them only when you want to use the features.

There are no spaces between the options and their values.

The following keywords are reserved and prevent users from specifying them as annotation names: - Application - Application_Priority - Tenant - Line_Of_Business - Business_Unit - Project Errors are generated if you attempt to import an annotation type using one of the reserved keywords. If you have created annotation names using these keywords, you must modify them so that the import utility tool can work correctly.

The Annotation Import utility requires Java 8 or Java 11. Ensure that one of those is installed prior to running the import utility. It is recommended to use the latest OpenJDK 11.

Assigning annotations to multiple assets using a query

Assigning an annotation to a group of assets helps you more easily identify or use those related assets in queries or dashboards.

Before you begin

Annotations that you wish to assign to assets must have previously been created.

About this task

You can simplify the task of assigning an annotation to multiple assets by using a query. For example, if you want to assign a custom address annotation to all of your arrays at a specific data center location.

Steps

1. Create a new query to identify the assets on which you wish to assign an annotation. Click **Queries** > **+New Query**.
2. In the **Search for…** drop-down, choose **Storage**. You can set filters to further narrow down the list of storages displayed.
3. In the list of storages displayed, select one or more by clicking on the check box beside the storage name. You may also select all the displayed storages by clicking on the main check box at the top of the list.
4. When you have selected all of the desired storages, click **Actions** > **Edit Annotation**.

   The system displays the Add Annotation dialog.

5. Select the **Annotation** and **Value** you want to assign to the storages and click **Save**.

   If you are displaying the column for that annotation, it will appear on all the selected storages.

6. You can now use the annotation to filter for storages in a widget or query. In a widget, you can do the following:

   a. Create a dashboard or open an existing one. Add a **Variable** and choose the annotation you set on the storages above. The variable is added to the dashboard.

   b. In the variable field you just added, click on **Any** and enter the appropriate Value to filter on. Click on the check mark to save the variable value.

   c. Add a widget. In the widget's Query, click on the**Filter by+**button and select the appropriate annotation from the list.

   d. Click on **Any** and select the annotation variable you added above. Variables you have created start with "$" and are displayed in the drop-down.

   e. Set any other filters or fields you desire, then click **Save** when the widget is customized to your liking.

   The widget on the dashboard displays the data for only the storages to which you assigned the annotation.

Querying assets

Queries enable you to monitor and troubleshoot your network by searching the assets in your environment at a granular level based on user-selected criteria (annotations and performance metrics). Additionally, annotation rules, which automatically assign annotations to assets, require a query.

Assets used in queries and dashboards

Insight queries and dashboard widgets can be used with a wide range of asset types

The following asset types can be used in queries, dashboard widgets, and custom asset pages. The fields and counters available for filters, expressions, and display will vary among asset types. Not all assets can be used in all widget types.

- Application
- Datastore
- Disk
- Fabric
- Generic Device
- Host
- Internal Volume
- iSCSI Session
- iSCSI Network Portal
- Path
- Port

- Qtree
- Quota
- Share
- Storage
- Storage Node
- Storage Pool
- Switch
- Tape
- VMDK
- Virtual Machine
- Volume
- Zone
- Zone Member

Creating a query

You can create a query to enable you to search the assets in your environment at a granular level. Queries enable you to slice data by adding filters and then sorting the results to view inventory and performance data in one view.

About this task

For example, you can create a query for volumes, add a filter to find particular storages associated with the selected volume, add a filter to find a particular annotation, such as Tier 1, on the selected storages, and finally add another filter to find all storages with IOPS - Read (IO/s) greater than 25. When the results are displayed, you can then sort the columns of information associated with the query in ascending or descending order.

When a new data source is added which acquires assets or any annotation or application assignments are made, you can query for those assets, annotations, or applications after the queries are indexed, which occurs at a regularly scheduled interval.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Queries** and select **+ New Query**.
3. Click **Select Resource Type** and select a type of asset.

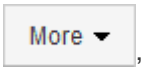
   When a resource is selected for a query, a number of default columns are automatically displayed; you can remove these columns or add new ones at any time.

4. In the **Name** text box, type the name of the asset or type a portion of text to filter through the asset names.

   You can use any of the following alone or combined to refine your search in any text box on the New Query page:

   - An asterisk enables you to search for everything. For example, `vol*rhel` displays all resources that start with “vol” and end with “rhel”.

- The question mark enables you to search for a specific number of characters. For example, `BOS-PRD??-S12` displays BOS-PRD12-S12, BOS-PRD13-S12, and so on.
- The OR operator enables you to specify multiple entities. For example, `FAS2240 OR CX600 OR FAS3270` finds multiple storage models.
- The NOT operator allows you to exclude text from the search results. For example, `NOT EMC*` finds everything that does not start with “EMC”. You can use `NOT *` to display fields that contain no value.

5. Click  to display the assets.
6. To add a criteria, click 

, and do either of the following:
   - Type to search for a specific criteria and then select it.
   - Scroll down the list and select a criteria.
   - Enter a range of values if you choose a performance metric like IOPS - Read (IO/s). Default annotations provided by Insight are indicated by ; it is possible to have annotations with duplicate names.

   A column is added to the Query results list for the criteria and the results of the query in the list updates.
7. Optionally, you can click to remove an annotation or performance metric from the query results.

   For example, if your query shows maximum latency and maximum throughput for datastores and you want to show only maximum latency in the query results list, click this button, and clear the **Throughput - Max** check box. The Throughput - Max (MB/s) column is removed from the Query results list.

   Depending on the number of columns displayed in the query results table, you may not be able to view additional added columns. You can remove one or more columns until your desired columns become visible.
8. Click **Save**, enter a name for the query, and click **Save** again.

   If you have an account with an administrator role, you can create custom dashboards. A custom dashboard can comprise any of the widgets from Widget Library, several of which, let you represent query results in a custom dashboard. For more information about custom dashboards, see the *OnCommand Insight Getting Started Guide*.

Related information

Importing and Exporting user data

Viewing queries

You can view your queries to monitor your assets and change how your queries display the data related to your assets.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Queries** and select **Show all queries**.

3. You can change how queries display by doing any of the following:
   - You can enter text in the **filter** box to search to display specific queries.
   - You can change the sort order of the columns in the table of queries to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.
   - To resize a column, hover the mouse over the column header until a blue bar appears. Place the mouse over the bar and drag it right or left.
   - To move a column, click on the column header and drag it right or left.
   - When scrolling through the query results, be aware that the results may change as Insight automatically polls your data sources. This may result in some items being missing, or some items appearing out of order depending on how they are sorted.

Exporting query results to a .CSV file

You might want to export the results of a query into a .CSV file to import the data into another application.

Steps

1. Log in to the OnCommand Insight web UI.
2. Click **Queries** and select **Show all queries**.

   The Queries page is displayed.
3. Click a query.
4. Click to export query results to a `.CSV` file.
5. Do one of the following:
   - Click **Open with** and then **OK** to open the file with Microsoft Excel and save the file to a specific location.
   - Click **Save file** and then **OK** to save the file to your Downloads folder. Only the attributes for the displayed columns will be exported. Some displayed columns, particularly those that are part of complex nested relationships, are not exported.

   When a comma appears in an asset name, the export encloses the name in quotes, preserving the asset name and the proper .csv format.

   + When exporting query results, be aware that **all** rows in the results table will be exported, not just those selected or displayed on the screen, up to a maximum of 10,000 rows.

   +

When opening an exported .CSV file with Excel, if you have an object name or other field that is in the format NN:NN (two digits followed by a colon followed by two more digits), Excel will sometimes interpret that name as a Time format, instead of Text format. This can result in Excel displaying incorrect values in those columns. For example, an object named "81:45" would show in Excel as "81:45:00". To work around this, import the .CSV into Excel using the following steps:

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the
column data format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

Modifying queries

You can change the criteria that are associated with a query when you want to change the search criteria for the assets that you are querying.

Steps

1. Log in to the Insightweb UI.
2. Click **Queries** and select **Show all queries**.

   The Queries page is displayed.

3. Click the query name.
4. To remove a criterion from the query, click .
5. To add a criteria to the query, click More, and select a criteria from the list.
6. Do one of the following:
   - Click **Save** to save the query with the name that was used initially.
   - Click **Save as** to save the query with another name.
   - Click **Rename** to change the query name that you had used initially.
   - Click **Revert** to change the query name back to the one that you had used initially.

Deleting queries

You can delete queries when they no longer gather useful information about your assets. You cannot delete a query if it is used in an annotation rule.

Steps

1. Log in to the Insightweb UI.
2. Click **Queries** and select **Show all queries**.

   The Queries page displays.

3. Position your cursor over the query you want to delete and click .

   A confirmation message displays, asking if you want to delete the query.

4. Click **OK**.

Assigning multiple applications to or removing multiple applications from assets

You can assign multiple applications to or remove multiple application from assets by using a query instead of having to manually assign or remove them.

Before you begin

You must have already created a query that finds all the assets that you to edit.

Steps

1. Click **Queries** and select **Show all queries**.

   The Queries page displays.

2. Click the name of the query that finds the assets.

   The list of assets associated with the query displays.

3. Select the desired assets in the list or click to select **All**.

   The **Actions** button displays.

4. To add an application to the selected assets, click Actions, and select **Edit Application**.
   a. Click **Application** and select one or more applications.

      You can select multiple applications for hosts, internal volumes, and virtual machines; however, you can select only one application for a volume.

   b. Click **Save**.
5. To remove an application assigned to the assets, click Actions and select **Remove Application**.
   a. Select the application or applications you want to remove.

b. Click **Delete**.

Any new applications you assign override any applications on the asset that were derived from another asset. For example, volumes inherit applications from hosts, and when new applications are assigned to a volume, the new application takes precedence over the derived application.

Editing or removing multiple annotations from assets

You can edit multiple annotations for assets or remove multiple annotations from assets by using a query instead of having to manually edit or remove them.

Before you begin

You must have already created a query that finds all the assets that you want to edit.

Steps

1. Click **Queries** and select **Show all queries**.

   The Queries page displays.

2. Click the name of the query that find the assets.

   The list of assets associated with the query displays.

3. Select the desired assets in the list or click ☐ ▾ to select **All**.

   The **Actions** button displays.

4. To add an annotation to the assets or edit the value of an annotation assigned to the assets, click Actions ▾, and select **Edit Annotation**.
   a. Click **Annotation** and select an annotation you want to change the value for, or select a new annotation to assign it to all the assets.
   b. Click **Value** and select a value for the annotation.
   c. Click **Save**.

5. To remove an annotation assigned to the assets, click Actions ▾, and select **Remove Annotation**.
   a. Click **Annotation** and select the annotation you want to remove from the assets.
   b. Click **Delete**.

Copying table values

You can copy values in tables for use in search boxes or other applications.

About this task

There are two methods you can use to copy values from tables or query results.

Steps

1. Method 1: Highlight the desired text with the mouse, copy it, and paste it into search fields or other applications.
2. Method 2: For single-value fields whose length exceeds the width of the table column, indicated by ellipses (…), hover over the field and click the clipboard icon. The value is copied to the clipboard for use in search fields or other applications.

   Note that only values that are links to assets can be copied. Note also that only fields that include single values (i.e. non-lists) have the copy icon.

Managing performance policies

OnCommand Insight enables you to create performance policies to monitor your network for various thresholds and to raise alerts when those thresholds are crossed. Using performance policies, you can detect a violation of a threshold immediately, identify the implication, and analyze the impact and root cause of the problem in a manner that enables rapid and effective correction.

A performance policy enables you to set thresholds on any objects (datastore, disk, hypervisor, internal volume, port, storage, storage node, storage pool, VMDK, virtual machine, and volume) with reported performance counters (for example, total IOPS). When a violation of a threshold occurs, Insight detects and reports it in the associated asset page, by displaying a red solid circle; by email alert, if configured; and in the Violations Dashboard or any custom dashboard that reports violations.

Insight provides some default performance policies, which you can modify or delete if they are not applicable to your environment, for the following objects:

- Hypervisor

  There are ESX swapping and ESX utilization policies.

- Internal volume and volume

  There are two latency policies for each resource, one annotated for Tier 1 and the other annotated for Tier 2.

- Port

  There is a policy for BB credit zero.

- Storage node

  There is a policy for node utilization.

- Virtual machine

  There are VM swapping and ESX CPU and memory policies.

- Volume

  There are latency by tier and misaligned volume policies.

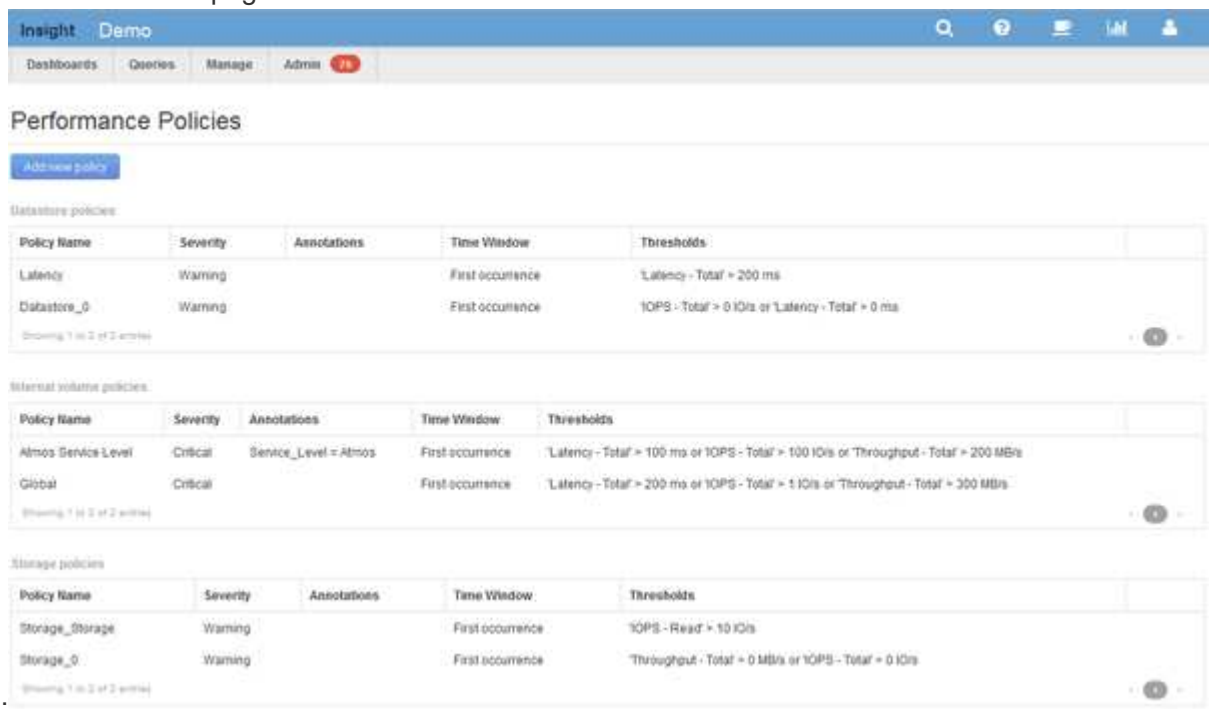
Creating performance policies

You create performance policies to set thresholds that trigger alerts to notify you about issues related to the resources in your network. For example, you can create a performance policy to alert you when the total utilization for storage pools is greater than 60%.

Steps

1. Open OnCommand Insight in your browser.
2. Select **Manage** > **Performance Policies**.

   The Performance Policies page is displayed.



   Policies are organized by object, and are evaluated in the order in which they appear in the list for that object.

3. Click **Add new policy**.

   The Add Policy dialog box is displayed.

4. In the **Policy name** field, enter a name for the policy.

   You must use a name that is different from all the other policy names for the object. For example, you cannot have two policies named “Latency” for an internal volume; however, you can have a “Latency” policy for an internal volume and another “Latency” policy for a different volume. The best practice is to always use a unique name for any policy, regardless of the object type.

5. From the **Apply to objects of type** list, select the type of object to which the policy applies.
6. From the **With annotation** list, select an annotation type, if applicable, and enter a value for the annotation in the **Value** box to apply the policy only to objects that have this particular annotation set.
7. If you selected **Port** as the object type, from the **Connected to** list, select what the port is connected to.

8. From the **Apply after a window of** list, select when an alert is raised to indicate a threshold violation.

   The First occurrence option triggers an alert when a threshold is exceeded on the first sample of data. All other options trigger an alert when the threshold is crossed once and is continuously crossed for at least the specified amount of time.

9. From the **With severity** list, select the severity for the violation.
10. By default, email alerts on policy violations will be sent to the recipients in the global email list. You can override these settings so that alerts for a particular policy are sent to specific recipients.
    - Click the link to open the recipients list, then click the **+** button to add recipients. Violation alerts for that policy will be sent to all recipients in the list.
11. Click the **any** link in the **Create alert if any of the following are true** section to control how alerts are triggered:
    - **any**

      This is the default setting, which creates alerts when any of the thresholds related to a policy are crossed.

    - **all**

      This setting creates an alert when all of the thresholds for a policy are crossed. When you select **all**, the first threshold that you create for a performance policy is referred to as the primary rule. You must ensure that the primary rule threshold is the violation that you are most concerned about for the performance policy.

12. In the **Create alert if** section, select a performance counter and an operator, and then enter a value to create a threshold.
13. Click **Add threshold** to add more thresholds.
14. To remove a threshold, click the trash can icon.
15. Select the **Stop processing further policies if alert is generated** check box if you want the policy to stop processing when an alert occurs.

    For example, if you have four policies for datastores, and the second policy is configured to stop processing when an alert occurs, the third and fourth policies are not processed while a violation of the second policy is active.

16. Click **Save**.

    The Performance Policies page displays, and the performance policy appears in the list of policies for the object type.

Performance policy evaluation precedence

The Performance Policies page groups policies by object type and Insight evaluates the policies in the order in which they appear in the object's performance policy list. You can change the order in which Insight evaluates policies in order to show the information that is most important to you in your network.

Insight evaluates all policies that are applicable to an object sequentially when performance data samples are taken into the system for that object; however, depending on annotations, not all policies apply to one group of

objects. For example, suppose that internal volume has the following policies:

- Policy 1 (the Insight-supplied default policy)
- Policy 2 (with an annotation of “Service Level = Silver” with the **Stop processing further policies if alert is generated** option
- Policy 3 (with an annotation of"`Service Level = Gold`")
- Policy 4

For an internal volume tier with a Gold annotation, Insight evaluates Policy 1, ignores Policy 2, and then evaluates Policy 3 and Policy 4. For an unannotated tier, Insight evaluates by the order of the policies; thus, Insight evaluates only Policy 1 and Policy 4. For an internal volume tier with a Silver annotation, Insight evaluates Policy 1 and Policy 2; however, if an alert is triggered when the policy’s threshold is crossed once and is continuously crossed for the window of time specified in the policy, then Insight no longer evaluates the other policies in the list while it evaluates the current counters for the object. When Insight captures the next set of performance samples for the object, it again begins to evaluate the performance policies for the object by filter and then order.

Changing the precedence of a performance policy

By default, Insight evaluates an object’s policies sequentially. You can configure the order in which Insight evaluates performance policies. For example, if you have a policy configured to stop processing when a violation occurs for Gold Tier storage, you can place that policy first in the list and avoid seeing more generic violations for the same storage asset.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

   The Performance Policies page displays.

3. Hover your cursor over a policy name in an object type’s performance policy list.

   The precedence arrows appear to the right of the policy.

4. To move a policy up in the list, click the up arrow; to move a policy down in the list, click the down arrow.

   By default, new policies are added sequentially to an object’s list of policies.

Editing performance policies

You can edit existing and default performance policies to change how Insight monitors the conditions of interest to you in your network. For example, you might want to change a policy’s threshold.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

The Performance Policies page displays.

3. Hover your cursor over a policy name in an object's performance policy list.
4. Click .

   The Edit Policy dialog box displays.

5. Make the required changes.

   If you change any option other than the policy name, Insight deletes all existing violations for that policy.

6. Click **Save.**

Deleting performance policies

You can delete a performance policy if you feel that it is no longer applicable to monitoring the objects in your network.

Steps

1. Open Insight in your browser.
2. From the **Manage** menu, select **Performance Policies**.

   The Performance Policies page displays.

3. Hover your cursor over the name of a policy in an object's performance policy list.
4. Click .

   A message appears, asking if you want to delete the policy.

5. Click **OK**.

Importing and Exporting user data

The import and export functions allow you to export annotations, annotation rules, queries, performance policies, and custom dashboards to one file. This file can then be imported into different OnCommand Insight servers.

The export and import functions are supported only between servers that are running the same version of OnCommand Insight.

To Export or Import user data, Click on **Admin** and select **Setup**, then choose the **Import/Export user data** tab.

During the import operation, data is added, merged, or replaced, depending on the objects and object types that are being imported.

- Annotation Types
  - Adds an annotation if no annotation with the same name exists in the target system.
  - Merges an annotation if the annotation type is a list, and an annotation with the same name exists in

the target system.

- Replaces an annotation if the annotation type is anything other than a list, and an annotation with the same name exists in the target system.

> If an annotation with the same name but with a different type exists in the target system, the import fails. If objects depend on the failed annotation, those objects may show incorrect or unwanted information. You must check all annotation dependencies after the import operation is complete.

- Annotation Rules
  - Adds an annotation rule if no annotation rule with the same name exists in the target system.
  - Replaces an annotation rule if an annotation rule with the same name exists in the target system.

> Annotation rules are dependent on both queries and annotations. You must check all the annotation rules for accuracy after the import operation is complete.

- Policies
  - Adds a policy if no policy with the same name exists in the target system.
  - Replaces a policy if a policy with the same name exists in the target system.

> Policies may be out of order after the import operation is complete. You must check the policy order after the import. Policies that are dependent on annotations may fail if the annotations are incorrect. You must check all the annotation dependencies after the import.
>
> +

- Queries
  - Adds a query if no query with the same name exists in the target system.
  - Replaces a query if a query with the same name exists in the target system, even if the resource type of the query is different.

> If the resource type of a query is different, after the import, any dashboard widgets that use that query may display unwanted or incorrect results. You must check all query-based widgets for accuracy after the import. Queries that are dependent on annotations may fail if the annotations are incorrect. You must check all the annotation dependencies after the import.
>
> +

- Dashboards
  - Adds a dashboard if no dashboard with the same name exists in the target system.
  - Replaces a dashboard if a dashboard with the same name exists in the target system, even if the resource type of the query is different.

You must check all query-based widgets in dashboards for accuracy after the import. If the source server has multiple dashboards with the same name, they are all exported. However, only the first one will be imported to the target server. To avoid errors during import, you should ensure that your dashboards have unique names before exporting them.

+

Copyright information

Trademark information