# Contents

**OnCommand Insight overview** ................................................................. 8  
Insight architecture ............................................................................. 8  
How Insight is used by administrators, managers, and planners .......... 9  
**Setting up Insight** ............................................................................... 11  
Accessing the web UI ........................................................................ 11  
Installing your Insight licenses ......................................................... 12  
OnCommand Insight licenses .............................................................. 13  
Setting up and managing user accounts ............................................ 16  
Insight user roles ............................................................................. 16  
Configuring Insight for LDAP(s) ....................................................... 17  
Changing user passwords ................................................................. 21  
Editing a user definition .................................................................. 21  
Deleting a user account .................................................................. 22  
Insight Security .................................................................................. 22  
Managing keys in a complex service provider environment .......... 23  
Managing security on the Insight server ........................................ 24  
Managing security on the local acquisition unit .............................. 25  
Managing security on an RAU or EMU .......................................... 26  
Managing security on the Data Warehouse .................................... 28  
Changing OnCommand Insight internal user passwords .............. 29  
Smart Card and certificate login support ........................................ 33  
Configuring hosts for Smart Card and certificate login ................. 33  
Configuring a client to support Smart Card and certificate login .... 35  
Enabling CAC on a Linux server ..................................................... 36  
Configuring Data Warehouse for Smart Card and certificate login .. 36  
Configuring Cognos for Smart Card and certificate login (OnCommand  
Insight 7.3.2 and earlier) ................................................................. 37  
Configuring Cognos for Smart Card and certificate login (OnCommand  
Insight 7.3.3 and later) ................................................................... 39  
Importing CA-signed SSL certificates for Cognos and DWH (Insight  
7.3.2 and earlier) ........................................................................... 39  
Importing CA-signed SSL certificates for Cognos and DWH (Insight  
7.3.3, 7.3.4) .................................................................................. 43  
Importing CA-signed SSL certificates for Cognos and DWH (Insight  
7.3.5 and later) .............................................................................. 45  
Importing SSL certificates ............................................................... 46  
Setting up weekly backups for your Insight database ................... 49  
What's included in the backup ........................................................... 49  
Performance data archiving ............................................................... 50  
Enabling performance archive .......................................................... 51  
Loading performance archive ........................................................... 51
Configuring your email ................................................................. 51
  Email configuration prerequisites .................................................. 51
  Configuring your email for Insight ................................................. 52
Configuring SNMP notifications ..................................................... 52
  Enabling the syslog facility .......................................................... 53
  Insight syslog contents ................................................................. 54
Configuring performance and assure violation notifications ............... 54
Configuring your ASUP processing ............................................... 55
  What's included in the Autosupport (ASUP) package ..................... 56
Defining applications ....................................................................... 57
  Assigning applications to assets .................................................. 58
  Editing applications ..................................................................... 58
  Deleting applications .................................................................. 59
How OnCommand Insight Ethernet monitoring works ......................... 59
  Ethernet monitoring unit network configuration .......................... 60
  Viewing Ethernet monitored data in the web UI ......................... 61
How OnCommand Insight anomaly detection works ............................ 61
  Configuring applications for anomaly detection .......................... 62
  Using the Anomalies section ....................................................... 63
  Anomaly detection monitoring status ......................................... 64
  Creating an application performance policy ................................. 64
Your business entities hierarchy ...................................................... 66
  Designing your business entities hierarchy ................................. 66
  Creating business entities ............................................................ 67
  Assigning business entities to assets ............................................. 67
  Assigning business entities to or removing business entities from
    multiple assets ......................................................................... 68
Defining annotations ....................................................................... 69
  Using annotations to monitor your environment ............................ 69
Querying assets ............................................................................. 81
  Assets used in queries and dashboards ........................................ 81
  Creating a query ......................................................................... 82
  Viewing queries ......................................................................... 83
  Exporting query results to a .CSV file ....................................... 84
  Modifying queries ...................................................................... 85
  Deleting queries ........................................................................ 85
  Assigning multiple applications to or removing multiple applications
    from assets ............................................................................. 85
  Editing or removing multiple annotations from assets ................. 86
  Copying table values .................................................................. 87
Managing performance policies ...................................................... 87
  Creating performance policies .................................................... 88
  Performance policy evaluation precedence ................................. 89
  Editing performance policies ...................................................... 90
  Deleting performance policies .................................................... 91
# Importing and Exporting user data

Importing and Exporting user data ................................................................. 91

## Insight data source management

**Insight data source management** ................................................................. 93

Setting up your data sources in Insight .......................................................... 93

Data source support information ................................................................. 93

Adding data sources .................................................................................. 94

Cloning a data source ............................................................................... 96

Testing the data source configuration ...................................................... 97

Vendor-specific data source reference ......................................................... 97

### 3PAR InServ data source

3PAR InServ data source ........................................................................ 97

### Amazon AWS EC2 data source

Amazon AWS EC2 data source .................................................................. 98

### Brocade Enterprise Fabric Connectivity Manager data source

Brocade Enterprise Fabric Connectivity Manager data source ................. 99

### Brocade FC Switch data source

Brocade FC Switch data source ................................................................ 100

### Brocade Sphereon/Intrepid Switch data source

Brocade Sphereon/Intrepid Switch data source ......................................... 102

### Cisco FC Switch Firmware (SNMP) data source

Cisco FC Switch Firmware (SNMP) data source ...................................... 103

### Dell Compellent Storage Center data source

Dell Compellent Storage Center data source ............................................ 105

### EMC Celerra data source

EMC Celerra data source .......................................................................... 106

### EMC CLARiiON (NaviCLI) data source

EMC CLARiiON (NaviCLI) data source ................................................... 107

### EMC Data Domain data source

EMC Data Domain data source .................................................................. 109

### EMC ECC StorageScope data source

EMC ECC StorageScope data source .......................................................... 110

### EMC Isilon data source

EMC Isilon data source ............................................................................ 110

### EMC RecoverPoint data source

EMC RecoverPoint data source ................................................................ 111

### EMC Solutions Enabler with SMI-S Performance data source

EMC Solutions Enabler with SMI-S Performance data source .................. 112

### EMC VNX data source

EMC VNX data source ............................................................................... 115

### EMC VNXe data source

EMC VNXe data source ............................................................................ 115

### EMC VPLEX data source

EMC VPLEX data source .......................................................................... 117

### EMC XtremIO data source

EMC XtremIO data source .......................................................................... 118

### Fujitsu Eternus data source

Fujitsu Eternus data source ........................................................................ 119

### HDS HiCommand Device Manager data source

HDS HiCommand Device Manager data source .......................................... 120

### HDS NAS (HNAS) data source

HDS NAS (HNAS) data source .................................................................. 123

### HP CommandView AE data source

HP CommandView AE data source ............................................................. 124

### HP EVA Storage data source

HP EVA Storage data source ...................................................................... 126

### Huawei OceanStor data source

Huawei OceanStor data source .................................................................. 128

### IBM DS data source

IBM DS data source .................................................................................. 129

### IBM PowerVM data source

IBM PowerVM data source ........................................................................ 130

### IBM SVC data source

IBM SVC data source ................................................................................ 131

### IBM Tivoli Monitoring data source

IBM Tivoli Monitoring data source ............................................................ 133

### IBM TotalStorage DS4000 data source

IBM TotalStorage DS4000 data source ...................................................... 134

### IBM XIV data source

IBM XIV data source ................................................................................ 134

### Infinidat InfiniBox data source

Infinidat InfiniBox data source .................................................................. 135

### Microsoft Azure compute data source

Microsoft Azure compute data source ........................................................ 136

### Microsoft Hyper-V data source

Microsoft Hyper-V data source .................................................................. 137

### NetApp Clustered Data ONTAP data source

NetApp Clustered Data ONTAP data source ............................................. 138

### NetApp Clustered Data ONTAP for Unified Manager data source

NetApp Clustered Data ONTAP for Unified Manager data source ............ 139

### NetApp Data ONTAP operating in 7-Mode data source

NetApp Data ONTAP operating in 7-Mode data source ............................. 139

### NetApp E-Series data source

NetApp E-Series data source ...................................................................... 141
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition unit status</td>
<td>186</td>
</tr>
<tr>
<td>Restoring the Insight database</td>
<td>187</td>
</tr>
<tr>
<td>Updating expired licenses</td>
<td>187</td>
</tr>
<tr>
<td>Licenses no longer compliant</td>
<td>188</td>
</tr>
<tr>
<td>Replacing licenses for older Insight versions</td>
<td>188</td>
</tr>
<tr>
<td>Applying a service pack</td>
<td>188</td>
</tr>
<tr>
<td>Preparing a special troubleshooting report</td>
<td>189</td>
</tr>
<tr>
<td>Manually backing up the OnCommand Insight database</td>
<td>189</td>
</tr>
<tr>
<td>Bundling logs for Support</td>
<td>189</td>
</tr>
<tr>
<td>Sending information to NetApp Support</td>
<td>189</td>
</tr>
<tr>
<td>Scrubbing data for transfer to support</td>
<td>190</td>
</tr>
<tr>
<td>Advanced troubleshooting</td>
<td>191</td>
</tr>
<tr>
<td>Configuring the number of hours to ignore dynamic data</td>
<td>191</td>
</tr>
<tr>
<td>Generating logs for Customer Support</td>
<td>193</td>
</tr>
<tr>
<td>Displaying system information</td>
<td>193</td>
</tr>
<tr>
<td>Listing installed OnCommand Insight components</td>
<td>193</td>
</tr>
<tr>
<td>Calculating the number of database objects</td>
<td>194</td>
</tr>
<tr>
<td>Restarting the OnCommand Insight Server</td>
<td>194</td>
</tr>
<tr>
<td>Moving MySQL data using the migrate option</td>
<td>194</td>
</tr>
<tr>
<td>Forcing annotation updates</td>
<td>195</td>
</tr>
<tr>
<td>Configuring Client settings</td>
<td>196</td>
</tr>
<tr>
<td>Checking the status of server resources</td>
<td>196</td>
</tr>
<tr>
<td>Finding ghost data sources</td>
<td>197</td>
</tr>
<tr>
<td>Adding a missing disk model</td>
<td>197</td>
</tr>
<tr>
<td><strong>Monitoring your environment</strong></td>
<td>200</td>
</tr>
<tr>
<td>Asset page data</td>
<td>200</td>
</tr>
<tr>
<td>Types of asset pages</td>
<td>200</td>
</tr>
<tr>
<td>Searching your environment for specific assets</td>
<td>201</td>
</tr>
<tr>
<td>Determining data source acquisition status</td>
<td>205</td>
</tr>
<tr>
<td>Asset page sections</td>
<td>206</td>
</tr>
<tr>
<td>Balancing network resources</td>
<td>220</td>
</tr>
<tr>
<td>Examining network performance</td>
<td>221</td>
</tr>
<tr>
<td>Analyzing slow PC performance</td>
<td>221</td>
</tr>
<tr>
<td>Analyzing correlated resources</td>
<td>222</td>
</tr>
<tr>
<td>Fibre Channel environment monitoring</td>
<td>223</td>
</tr>
<tr>
<td>Time-to-live (TTL) and downsampled data</td>
<td>223</td>
</tr>
<tr>
<td>Pruning of inventory history</td>
<td>225</td>
</tr>
<tr>
<td>NAS path for VMs</td>
<td>226</td>
</tr>
<tr>
<td>Capacity as Time Series</td>
<td>226</td>
</tr>
<tr>
<td><strong>Copyright</strong></td>
<td>227</td>
</tr>
<tr>
<td><strong>Trademark</strong></td>
<td>228</td>
</tr>
<tr>
<td><strong>How to send comments about documentation and receive update</strong></td>
<td>229</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>230</td>
</tr>
</tbody>
</table>
OnCommand Insight overview

OnCommand Insight enables you to simplify operational management of complex private and hybrid cloud and virtual IT environments. Insight is a single solution to enable cross-domain, multi-vendor resource management and analysis across networks, storage, and servers in physical and virtual environments.

Insight can help you optimize your current infrastructure, allowing you to right-size operations to meet business demands. It simplifies the process of determining what and when to buy. It also reduces risk during complex technology migrations, such as moving to a hybrid cloud, by identifying which workloads are candidates for cloud migration. With Insight, you can manage the IT infrastructure as an end-to-end service by integrating the resources into the company’s entire IT service delivery chain.

Insight architecture

A typical installation of OnCommand Insight includes data acquisition and data warehousing with reports, all easily accessible from a web-based UI. For more secure environments, acquisition can be done through a remote acquisition unit.

The major components of the Insight architecture are shown in the following diagram:

OnCommand Insight Server

The OnCommand Insight Server contains the main data repository and analysis components. The server is continuously building an end-to-end topology of the environment, analyzing the environment, and generating alerts when an incident or violation is detected.

Acquisition

The Insight collection engine is built on one or more acquisition units. Each Insight server contains a local acquisition unit and can support remote acquisition units. Each unit is a service running on the network that accesses (through modules called data sources) and
collects data from devices in the data center. Information collected by the acquisition units is then sent to the server for analysis.

The collection engine is designed to be highly modular and easily patched.

**Integration API**

An API allows the collection of data from external agents. Integration data can be viewed in the web UI using queries and widgets. Dashboards can contain 'native' Insight data and integration data. You can apply filtering, roll-ups, and grouping to the data in these dashboards.

**Ethernet monitor**

Insight uses an Ethernet monitoring unit (EMU) to inspect Ethernet NAS traffic flow between the storage, network switches, and clients. This enables administrators to easily identify the heaviest NFSv3 workloads contributing to Internal Volume activities.

**Web UI**

The HTML5 web-based user interface for Insight enables you to set up data sources and your monitoring environment, including policies, thresholds and alerts. You then use the web UI Asset Dashboard and asset pages to identify and research potential problems. You can create custom dashboards with a variety of widgets, each of which provides extensive flexibility in displaying, analyzing, and charting your data.

**Anomaly Detection**

Anomalies are performance change events in application infrastructure that do not conform to previously observed and expected patterns. Anomaly detection targets the infrastructure servicing an application, identifying changes in processing patterns and behaviors. These cyclical processing patterns include historical "ebbs and flows" in a workloads performance during hours of business operation and non-business operation.

**Data Warehouse**

The OnCommand Insight Data Warehouse is a centralized repository that stores data from multiple Insight servers and transforms data into a common, multidimensional data model for querying and analysis.

The OnCommand Insight Data Warehouse enables access to an open database consisting of several data marts that let you generate custom capacity and performance reports such as chargeback reports, trending reports with historical data, consumption analyses, and forecasting reports.

The Data Warehouse consolidates and prepares data for reporting for one or multiple installations of Insight. The data includes history, trending, inventory, chargeback, show back and data presentations to support long-term planning of the data center's infrastructure.

**Cognos**

Cognos is the reporting engine for Insight, an IBM business intelligence tool that enables you to view pre-defined reports or create custom reports. Insight reporting generates reports from the Data Warehouse data.

**How Insight is used by administrators, managers, and planners**

OnCommand Insight supplies information that is vital for storage administrators, managers, and storage architects to perform troubleshooting and analysis.

Experienced storage administrators use OnCommand Insight along with their network storage knowledge to accomplish these typical tasks:
• Manage the SAN and NAS environment.
• Work with SAN engineers on network concerns.
• Evaluate, test, and integrate new storage technologies into the environment.
• Troubleshoot performance issues, alerts, policy breaches, violations, and vulnerabilities.

Managers and network planners use OnCommand Insight to perform these business tasks:
• Capacity planning
• Develop project budgets and timelines.
• Evaluate and revise project plans to meet changing project demands.
• Manage project planning and expenses.
• Purchase hardware and software.
• Provide business reports for capacity management, charge back billing, right sizing, and service level agreements.
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.

   **Note:** An Insight browser session that is inactive for 30 minutes is timed out and you are logged out of the system.

---

**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.

<table>
<thead>
<tr>
<th>Feature (admin)</th>
<th>With Perform license</th>
<th>Without Perform license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Yes</td>
<td>No performance data or charts; no anomaly detection-related widgets</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Host</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Datastore</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>VMDK</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Internal volume</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Volume</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Storage pool</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Disk</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Storage</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Storage node</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Fabric</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Switch port</td>
<td>Yes</td>
<td>No performance data or charts; “Port Errors” shows “N/A”</td>
</tr>
<tr>
<td>Storage port</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NPV port</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Switch</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>NPV switch</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Qtrees</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Quota</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Path</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Zone</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Zone member</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Generic device</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Tape</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Masking</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>ISCSI sessions</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Feature (admin)</td>
<td>With Perform license</td>
<td>Without Perform license</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>ICSI network portals</td>
<td>Yes</td>
<td>No performance data or charts</td>
</tr>
<tr>
<td>Search</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Admin</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Widgets</td>
<td>Yes</td>
<td>Partially available (only asset, query, and admin widgets are available)</td>
</tr>
<tr>
<td>Violations dashboard</td>
<td>Yes</td>
<td>Hidden</td>
</tr>
<tr>
<td>Assets dashboard</td>
<td>Yes</td>
<td>Partially available (storage IOPS and VM IOPS widgets are hidden)</td>
</tr>
<tr>
<td>Manage performance policies</td>
<td>Yes</td>
<td>Hidden</td>
</tr>
<tr>
<td>Manage annotations</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage annotation rules</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Queries</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage business entities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

Note: 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.

Result

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. This account type does not allow you to perform actions such as identifying generic devices and defining the policies in the Java UI.
• 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.

Note: 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.
  Note: 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.
Tip: 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.

Tip: 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.

<table>
<thead>
<tr>
<th>Role attribute</th>
<th>memberOf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail attribute</td>
<td>mail</td>
</tr>
<tr>
<td>Distinguished Name attribute</td>
<td>distinguishedName</td>
</tr>
<tr>
<td>Referral</td>
<td>follow</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Insight Group</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insight server administrator group</td>
<td>insight.server.admins</td>
</tr>
<tr>
<td>Insight administrators group</td>
<td>insight.admins</td>
</tr>
<tr>
<td>Insight users group</td>
<td>insight.users</td>
</tr>
<tr>
<td>Insight guests group</td>
<td>insight.guests</td>
</tr>
<tr>
<td>Reporting administrator group</td>
<td>insight.report.admins</td>
</tr>
<tr>
<td>Reporting pro authors group</td>
<td>insight.report.prauthors</td>
</tr>
<tr>
<td>Reporting authors group</td>
<td>insight.report.business.authors</td>
</tr>
<tr>
<td>Reporting consumers group</td>
<td>insight.report.business.consumers</td>
</tr>
<tr>
<td>Reporting recipients group</td>
<td>insight.report.recipients</td>
</tr>
</tbody>
</table>
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.

**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 bottom of the page to display the LDAP setup, 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.

     **Note**: 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.

**Note**: 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.

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:
   
   `securityadmin -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.

   **Note**: 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.

**Important**: 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

**Important:** 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, DWH, and EMU 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.

5. 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 (-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.

Note: 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.

Important: 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.

Important: 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, DWH, and EMU 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 or EMU

The securityadmin tool allows you to manage security options on RAUs and EMUs. 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 and EMU is to update the 'acquisition' user password when the password for that user has been changed on the server. All of the RAUs, EMUs and the LAU use the same password as that of the server 'acquisition' user to communicate with the server.
Note:
The 'acquisition' user only exists on the Insight server. The RAU, LAU, and EMU login as that user when they connect to the server.

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

Steps
1. Perform a remote login to the server running the RAU or EMU
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/EMU

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.

   Note: 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 or EMU encryption keys used to encrypt or decrypt device passwords.

   Important: 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.

   Important: 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, DWH, and EMU 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.

   **Note:** 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

**Note:** When you change the dwhuser, hosts, inventory, or root passwords, you have the option to use SHA-256 password hashing. This option 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**

**Warning:** 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.

<table>
<thead>
<tr>
<th><strong>Insight Server Passwords</strong></th>
<th><strong>Required changes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>_internal</td>
<td></td>
</tr>
<tr>
<td>acquisition</td>
<td>LAU, RAU, EMU</td>
</tr>
<tr>
<td>dwh_internal</td>
<td>Data Warehouse</td>
</tr>
<tr>
<td>hosts</td>
<td></td>
</tr>
<tr>
<td>inventory</td>
<td>Data Warehouse</td>
</tr>
<tr>
<td>root</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th><strong>Data Warehouse Passwords</strong></th>
<th><strong>Required changes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>cognos_admin</td>
<td></td>
</tr>
<tr>
<td>dwh</td>
<td></td>
</tr>
<tr>
<td>dwh_internal (Changed using the Server Connector configuration UI)</td>
<td>Insight server</td>
</tr>
<tr>
<td>dwhuser</td>
<td></td>
</tr>
</tbody>
</table>
Data Warehouse Passwords | Required changes
---|---
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, EMU |

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.

![Edit Connector Advanced screen](image)

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 the Java client, a custom dialog appears with all personal certificates, regardless of issuer.

**Note:** 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.

**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.
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=localityName,I,S=stateName,C=countryName"

6. Generate a certificate signing request:
   
   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, import the certificate and 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 certificate with 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 -importkeystore -destkeystore "C:\Program Files\SANscreen\java64\bin\keytool.exe" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"

12. Import the root certificate:
13. Import the intermediate email certificate:

C:\Program Files\SANscreen\java64\bin\keytool.exe -importkeystore -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"

Repeat this step for all intermediate email certificates.

14. Import the intermediate certificate:

C:\Program Files\SANscreen\java64\bin\keytool.exe -importkeystore -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.truststore" -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.

16. 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. Run the appropriate command:

<table>
<thead>
<tr>
<th>OS</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td><code>&lt;install dir&gt;\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat</code></td>
</tr>
<tr>
<td>Linux</td>
<td><code>/opt/netapp/oci/wildfly/bin\enableCACforRemoteEJB.sh</code></td>
</tr>
</tbody>
</table>

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

17. 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.

**About this task**

The following are the common client configuration requirements:

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

Additional configuration steps include the following:

**Steps**

1. Disable unnecessary dialog pop-ups when launching the Java client:
   
   a. Open the “Java” control panel.
b. Select the “Advanced” tab.

c. Select “Advanced Security Settings”.

d. Clear the “Use certificates and keys in browser keystore” option.

2. Import soft certificates into a user's personal certificates using the Chrome browser:

   a. Navigate to “Advanced Settings”.

   b. Select “Manage Certificates”

   c. Select the “Personal” certificates tab”.

   d. Select “Import…”.

   e. Choose the .p12 file.

   f. Complete the wizard, making sure to fill in the password field with the password that was used to create the certificate.

   Similar steps are required to configure the Internet Explorer and Firefox browsers.

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/scripts/wildfly.server

2. Edit "wildfly.server" and change the value of clientAuth 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.

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 trust store:
   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.truststore -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.truststore -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:

<table>
<thead>
<tr>
<th>OS</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>&lt;install dir&gt;\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat</td>
</tr>
<tr>
<td>Linux</td>
<td>/opt/netapp/oci/wildfly/bin\enableCACforRemoteEJB.sh</td>
</tr>
</tbody>
</table>

   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 7.3.2 and earlier)**

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 7.3.2 and earlier.

**Steps**

1. Add certificate authorities (CAs) to the Cognos trust store:
   a. In a command window, go to ..\SANscreen\cognos\c10_64\configuration\certs\n   b. Use the keytool utility to list the trusted CAs:

   ```
   C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore CognosTruststore.jks -storepass changeit
   ```

   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. Optional: To include customer's CAs with OnCommand Insight trusted CAs, go to .. \SANscreen\cognos\c10_64\configuration\certs\.
e. Use the `keytool` utility to import the `.pem` file

   ```
   C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore CognosTruststore.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 `changeit`, the default password.

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

2. Modify the reporting portal registry:

   a. Use `regedit` to modify `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Prefs\com\netapp\sanscreen\reporting`.

   b. Change the `portal_url` value to `https:\DWHServer.name:8080/ibmcognos`.

3. Redirect the reporting portal:

   a. Open the `..\SANscreen\wildfly\standalone\deployments\dwh-redirect.war\redirect.html` file in edit mode.

   b. Change the URL value from `https:\DWHServer.name:9300/p2pd/servlet/dispatch` to `https:\DWHServer.name:8080/ibmcognos`.

4. Enable CAC mode:

   a. Open the `..\SANscreen\cognos\c10_6\configuration\SANscreenAP.properties` file in edit mode.

   b. Change `authentication.mode=form` to `authentication.mode=cac`.

   c. Save the file.

   d. Restart the Cognos service: From the Windows Start menu, select `All Programs > IBM Cognos > IBM Cognos configuration`

5. Start the ServletGateway:

   a. Go to `..\SANscreen\cognos\c10_64\wlp\bin`.

   b. Set the Java Home path:

   ```
   set java_home=..\SANscreen\cognos\c10_64\bin64\jre\7.0
   ```

   c. Start the ServletGateway: `server start servletgateway`

6. Changing the ServletGateway port from the default port (8080) to a custom port requires repeating the following steps:

   a. Update the reporting portal in registry entry.

   b. Update the reporting portal redirect.

   c. Restart the ServletGateway port.

After you finish

- After enabling CAC, logging in to Cognos might fail with a TLS version issue. Enabling TLS1.0, 1.1, and 1.2 on IE corrects this problem. You might experience the same errors other browsers. You should be able to correct them by enabling TLS versions.
• The ServletGateway must be stopped and started manually every time the server is rebooted or a command prompt session is closed because no ServletGateway service is available.

• ETL must be built to reflect the new reporting portal URL in the OnCommand Insight server.

• All of the manual steps might need to be performed after a Data Warehouse Cognos upgrade.

Configuring Cognos for Smart Card and certificate login (OnCommand Insight 7.3.3 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 7.3.3 and later.

Steps
1. Add certificate authorities (CAs) to the Cognos trust store.
   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. Optional: 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

Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.2 and earlier)

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 7.3.2 and earlier.
You must have admin privileges to perform this procedure.

**Steps**

1. Access the Data Warehouse using a remote desktop
2. Back up the ..\SANscreen\cognos\c10_64\configuration\cogstartup.xml file.
3. Back up the certs and csk folders in ..\SANscreen\cognos\c10_64\configuration
4. List the contents of the Cognos CAMKeystore to see if both signing and encryption certificates are signed by the same CA:
   
   "D:\Program Files\SANscreen\java\bin\keytool.exe" -keystore "D:\Program Files\SANscreen\cognos\c10_64\configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoPassWordSet -list -v
   
   If the issuer (CA) SHA1 is not the same for both the signing and encryption certificate, perform the following steps:
   a. Stop the Cognos services.
   b. Close the IBM Cognos Configuration.
   c. Delete the CAMKeystore and CAMKeystore.lock files from the ..\SANscreen\cognos \c10_64\configuration\certs folder.
   d. Launch the IBM Cognos Configuration tool as administrator.
      
      SANscreen\cognos\c10_64\bin\cogconfig.sh
      
   e. Save the configuration.
      
   This will generate a new CAMKeystore keystore.
5. Generate a Certificate Signing Request from Cognos. In the Admin CMD prompt window, enter the following:

   D: cd "Program Files\SANscreen\cognos\c10_64\bin"

   ThirdPartyCertificateTool.bat -java:local -c -e -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptrequest.csr

   If this command results in a “NoClassFound” error perform the following steps and then repeat the command.
   a. Modify ..\SANscreen\cognos\c10_64\bin\ThirdPartyCertificateTool.bat.
   b. Under “uselocal section (line 49)” Change J_HOME to ..\bin64\jre\7.0.
   c. Save the file.
   d. Generate a Certificate Signing Request from Cognos again.
6. Open the c:\temp\encryptrequest.csr file and copy the generated content.
7. Input encryptRequest.csr content and generate certificates using the CA signing portal.
8. Download the chain certificates, including the root certificate using PKCS7 format. This will download fqdn.p7b.
9. Obtain a certificate in .p7b format from your CA. Use a name that identifies it as the certificate for the Cognos Web server. For example, name it CGWEB001.Cognos.
10. Upload the file to D: on the DWH server.
11. Perform the following steps using the Admin UI:
a. Open the .p7b certificate in "Crypto Shell Extensions".
b. Click Certificates in the left pane.
c. Right click on your certificate.
d. Click All Tasks > Export.
e. Click Base-64 encoded X.509 (.CER).
f. Specify the name of the file you want to export (D:\root cert.cer).

Repeat these steps to export all of the certificates separately into .cer files. Name them intermediate.cer and cognos.cer.

12. Merge the root.cer and the intermediate.cer into one file.
   a. Open the intermediate.cer with NotePad and copy all of the content.
   b. Open the root.cer with NotePad and add the content of the intermediate.cer file.
   c. Save the file as CA.cer.

13. Import the certificates into Cognos. In the Admin command prompt, enter the following command:
    D: cd "Program Files\sanscreen\cognos\c10-64\bin
    ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp.cognos.cer -t c:\temp\CA.cer


15. Open the IBM Cognos Configuration as an Administrator.
   a. Select Local > Security > Cryptography> Cognos.
   b. Change "Use third party CA?" to True.
   c. Save the configuration.
   d. Restart Cognos.

16. Export the latest Cognos certificate from the Cognos trust store to the following file: c:\tmp cognosssl.crt.
    "D:\Program Files\SANscreen\java\bin\keytool.exe" -keystore "D:\Program Files\SANscreen\cognos\c10_64\configuration\certs\CAMKeystore" -storetype PKCS12 -storepass NoPasswordSet -exportcert -file "c:\temp cognosssl.crt" -alias encryption

17. Import the latest Cognos certificate (c:\temp\cognosssl1.crt) into the DWH truststore to establish SSL communication between the DWH and Cognos servers.
    "D:\Program Files\SANscreen\java\bin\keytool.exe" -importcert -file "c: \temp\cognosssl1.crt" -keystore "D:\Program Files\SANscreen\wildfly \standalone\configuration\server.truststore" -alias cognosssl

18. Clear the existing Java path variable as it might cause problems during this procedure:
    SET PATH=.

19. Navigate to ..\SANscreen\cognos\c10_64\bin

20. Enter the following command:
    ThirdPartyCertificateTool.bat -java:local -i -e -r OCIDWH.cer -t chain.p7b
Where OCIDWH.cer is the OCI DWH certificate, and the chain.p7b is the chain of certificates including the root certificate.

21. Use the following command to make Cognos trust the Root certificate:

```
ThirdPartyCertificateTool.bat -java:local -i -T -r ca.cer
```

In the example, ca.cer is your organization's root certificate. This step is required even though the previous certificate import steps seemed to log messages about trusting certificate authorities.

22. Open the IBM Cognos configuration UI and enable third party certificates: Certificate Authority setting > Use a 3rd party CA? > True

23. Save the changes

24. Restart the Cognos services

25. Enter the following command in the Admin command prompt window to export the latest Cognos certificate to a file: c:\temp\cognosssl.crt.

```
"D:\Program Files\SANscreen\java\bin\keytool.exe" -keystore "D:\Program Files\SANscreen\cognos\c10_64\configuration\certs\CAMKeystore" -
storetype PKCS12 -storepass NoPassWordSet -exportcert -file "c:\temp\cognosssl.crt" -alias encryption

26. Enter the following command in the Admin command prompt window to import the latest Cognos certificate (c:\temp\cognosssl.crt)

"D:\Program Files\SANscreen\java\bin\keytool.exe" -importcert -file "c:\temp\cognosssl.crt" -keystore "D:\Program Files\SANscreen\wildfly\standalone\configuration\server.truststore" -alias cognosssl

   a. Backup \SANscreen\wildfly\standalone\configuration\server.truststore
   b. Import the new certs into the trust store:

   C:\Program Files\SANscreen\java64\bin>keytool -importcert -file C:\ocidwhcert.cer -keystore D:\Program Files\SANscreen\wildfly\standalone\configuration\server.truststore"

   c:\ocidwhcert.cer is the public certificate of your OCI DWH

27. Restart the Insight server.

28. Log in to the Data Warehouse server and perform a backup.
   The backup should complete successfully, including backing up the Cognos content store.

**Importing CA-signed SSL certificates for Cognos and DWH (Insight 7.3.3, 7.3.4)**

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 7.3.3 and 7.3.4.

**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 -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. Input encryptRequest.csr content and generate a certificate using the CA signing portal and add the additional attribute "SAN:dns=FQDN (For example, win2k12r2image.na.ead.netapp.com)".

   If you want to add SubjectAltName, google chrome complains if SubjectAltName is missing from the certificate for version 58 onwards.

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. 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 -e -r c:\temp\cognos.cer -t c:\temp\CA.cer
       This will set CA.cer as root Certificate Authority.

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. Take the backup of DWH server truststore at ..\SANscreen\wildfly\standalone\configuration\server.trustore

13. Import the “c:\temp\cognos.crt” into dwh truststore 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 7.3.5 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 7.3.5 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\sansscreen\cognos\analytics\bin”
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 truststore 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 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

**Note:** 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:

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

   **Example**

   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}"/>
   ```

9. 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 trust stores, 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 Insight Java client or 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 trust store 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 local Insight server or on a remote server that is accessible from the Insight server.
   
   **Note**: 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.

**Result**

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
• Ethernet monitoring units
• ASUP/proxy settings
• Backup location settings
• Archive location settings
• Notification settings
• Anomaly detection scores and devices
• Anomaly detection application 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

Note: 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**.
   - **Note:** 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 the OnCommand 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 and activate the logging process.

Before you begin
• You must have the IP address of the server 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 changes
• Performance alerts
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 **Syslog Enabled** check box.
4. In the **Server** field, enter the IP address of the log server.
5. In the **Facility** field, select the facility level that corresponds to the type of program that is logging the message.
6. 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 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

By default, ASUP data is forwarded using the HTTPS protocol. Although ASUP supports FTP and email for the delivery of ASUP data, you should use HTTPS because it provides the best security, and supports the latest ASUP features.

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
6. Select your preferences for the following options:
   - What to send: Logs, inventory data, performance data
   - How to send: HTTP, HTTPS, FTP, email
7. Enter the size and split file limits:
   - Size limit: For email ASUP data transmission, enter the maximum data size to be sent.
   - Split files if bigger than: For email ASUP data transmission, indicate the cutoff point for file size.
     The default split file limit is 1 MB.
8. Click Test Connection to ensure that the connection that you specified works.
9. Click Save.
10. In the Proxy section, if you have selected the HTTP or HTTPS protocol for ASUP data transmission to connect to the Internet, enable the proxy, and define it.
11. Click Test Connection to ensure that the proxy that you specified works.
12. 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
- Ethernet monitoring units
- ASUP/proxy settings
- Backup location settings
- Archive location settings
- Notification settings
- Anomaly detection scores and devices
- Anomaly detection application 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)

**Note:** 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.
   **Note:** If the anomaly detection engine is installed, the Applications Dashboard page also shows an Anomaly Score for the application. For more information about installing and configuring the anomaly detection engine, see the OnCommand Insight Configuration and Administration Guide.
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.
     
     Note: 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.
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**.

### How OnCommand Insight Ethernet monitoring works

OnCommand Insight uses an Ethernet monitoring unit (EMU) to inspect Ethernet packet headers on a switch adjacent to storage, and determines the type of NFSv3 operation being performed, the destination IP address of the operation, and the volumes or shares being addressed.

The EMU continually monitors the mirrored traffic and builds top-k list of the "k" most heavily loaded volumes IDs and share names, sorted by total observed operation count. For each volume and share, the EMU generates a top-n list of the top "N" client IP addresses contributing to the load on that specific volume or share, sorted by total observed operation count. Top-k and top-n lists are maintained independently for each protocol. Monitored traffic is only examined to update internal counters relevant to per-volume and per-client operation accounting. The monitored traffic is not persistently stored.

Ethernet traffic monitoring is supported on hardware platforms running the following software:

- ONTAP 9.0
- Clustered Data ONTAP
- Data ONTAP 7-Mode

Collected data is sent to the corresponding Insight server associated with the EMU. Since the Insight server is also acquiring the relevant storage details, for the same volumes and shares and potentially the host details, the server can merge the EMU data into the standard Insight data model, correlating Volume IDs and share names to discovered Internal Volumes and client IPs to resolved physical hosts or discovered Virtual Machines.

The information is available in OnCommand Insight, providing the following:

- Volumes or shares with the highest number of NFS v3 protocol operations
- Clients driving the NFS v3 protocol operations on specific volumes
- Details of the NFS v3 protocol traffic for each volume and share for clients over a user defined time period

The information allows customers to pro-actively monitor NAS traffic and easily identify top contributing clients that are putting the heaviest loads on specific volumes or shares.
Ethernet monitoring unit network configuration

The Ethernet monitoring unit (EMU) is a separate server connected to the network switches using mirror ports or Switch Port Analyzer 'SPAN' ports. These ports are configured to mirror packets flowing to the ports connected to the storage links. The EMU is designed to parse every packet it receives to determine information about operations and endpoint IP addresses. This information includes:

- Client IP address
- Target (storage) IP address
- Target Volume ID or share name
- Operation type

The OnCommand Insight server and the EMU server do not require access to the production VLAN traffic. The OnCommand Insight server needs connectivity to the storage array via the management VLAN. The EMU needs connectivity to the Insight server, potentially over the management VLAN. The connectivity between the EMU and the switch connected to the storage array is by way of the mirror ports only. For this configuration, no VLAN connectivity or IP addresses are required for the EMU.

The switches can be 1GbE or 10GbE capable. The amount of traffic on the switch can exceed the capability of the mirror port. Enterprise grade switches expect this to happen and will drop packets in a first-come, first-served basis, without causing network utilization issues. The recommendation is that the mirror port is 10GbE, however 1GbE ports will work, but with a higher probability of packets being dropped. When packets are dropped, the EMU receives a representative portion of all the traffic. Under these overloaded network circumstances, the server creating the load and the degraded resources continue to be visible in the correct proportions but with lower fidelity.

The illustration below is a simple representation of an Ethernet topology containing an EMU. Clients (any number of physical Hosts or Virtual Machines) are accessing NAS shares accessible through a set of Ethernet switches to a number of storage systems. Ethernet NAS traffic is flowing between the storage systems and the clients.

Supported platforms

The following hardware platforms are supported for this release of Ethernet monitoring:
• ONTAP 9.0
• Clustered Data ONTAP
• Data ONTAP 7-Mode

Restrictions
The following restrictions apply to this release of the EMU:

• Only Ethernet/-IPv4/NFSv3 traffic is monitored. Packets with other protocols are not inspected.
• If the traffic to the storage array is encrypted, the EMU does not parse the packets.
• The storage arrays must be monitored by the same OnCommand Insight server that the EMU is connected to.
• If client servers are not discovered by the OnCommand Insight server, only the IP address of the initiator is displayed.

Ethernet Monitoring Unit monitoring and management
Ethernet Monitoring Units (EMUs) are similar to Acquisition Units (AU). The OnCommand Insight web UI includes an Ethernet Monitoring Units administration screen which allows you to perform the following operations:

• View status messages for the EMU
• Restart the EMU
• Delete an EMU (provided it is not in "Active" status)
• Access the EMU landing page

The EMU landing page is similar to a Data source status page. It presents the overall status of the single EMU Data source. The EMU detail shows the polling status for the last 3 weeks, provides the ability to generate an error report, and the ability to install a Patch.

Viewing Ethernet monitored data in the web UI
Data collected by the EMU is presented on the Internal volume landing pages and on the Host or Virtual Machine landing pages.

On the Internal Volume landing pages, the Active NAS contributors table presents the top clients that have been sending NAS traffic to a specific volume, sorted by total observed operations and NFSv3 operations. Use the pencil icon to display a graph of the observed total IOPS or observed NFSv3 IOPS.

On the Host or Virtual Machine landing pages the NAS activity tables list the storage system and the Internal Volumes that a Host or VM has sent traffic to. Traffic is sorted by total operations and NFSv3 operations.

How OnCommand Insight anomaly detection works
OnCommand Insight contains machine-learning anomaly detection analytics which provide visibility into an application's infrastructure and identifies performance anomalies before they become service disruptions.

Anomaly analysis helps you identify the normal operating workload range for an application and informs when changes in performance are outside of expected levels. The application anomaly
detection engine ingests performance metrics collected by Insight and identifies anomalies in the application infrastructure.

You can use anomaly detection to perform these tasks:

- Identify significant changes in the application infrastructure behavior
- Track an application through the entire stack and across multiple counters
- Diagnose the cause of periodically recurring events in an application workload
- Provide a more comprehensive set of information compared to data from performance counters using static threshold values
- Monitor in an improved reactive mode, with an end-to-end view of the topology and the ability to focus on the most anomalous behaviors.

The anomaly detection engine uses Insight data for application analysis. When monitoring is first started, up to 14 days of historical performance data can be ingested by the analysis engine. Data is collected for weeks or even months, providing more accurate data about a given resource. The data includes totals for the following counters:

<table>
<thead>
<tr>
<th>Objects</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM</td>
<td>Latency, IOPS</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>CPU utilization, IOPS</td>
</tr>
<tr>
<td>Edge port</td>
<td>BB credit zero</td>
</tr>
<tr>
<td>Storage Node</td>
<td>Latency, utilization, IOPS</td>
</tr>
<tr>
<td>Volume</td>
<td>Latency, IOPS</td>
</tr>
<tr>
<td>Internal volume</td>
<td>Latency, IOPS</td>
</tr>
<tr>
<td>Storage pool</td>
<td>IOPS, utilization</td>
</tr>
</tbody>
</table>

Data collected by the anomaly detection engine is archived when Performance Data Archiving is enabled on the Insight server. See the System Health page to determine if archiving is enabled.

The anomaly detection engine is runs on a separate server than the Insight server. It can be configured on a physical machine or a VM. See the OnCommand Insight Installation Guide for Windows or Linux for more information.

**Configuring applications for anomaly detection**

You must turn on anomaly detection in order to monitor an application's infrastructure for abnormal behavior. Anomaly detection monitoring is turned on or off for applications only.

**Before you begin**

- You must have installed and configured the anomaly detection engine.
- You must have assigned an application to the compute resource (virtual machine or host) for any assets for which you want anomaly detection information. Insight discovers the rest of the resources automatically.

**Steps**

1. Log in to the OnCommand Insight web UI.
2. Click Manage and select Applications.
3. Locate the application assigned to the compute resource.

4. In the Anomalies section, ensure that the Monitor control box in the upper right of the section shows ON rather than OFF; if not, click anywhere in the Monitor control box to switch the control to ON.

You are able to concurrently monitor up to 48 applications for anomalies.

The status in the section displays “Learning” for at least an hour; the anomaly detection engine preloads up to 14 days of any existing performance data so the engine can learn the behavior of your environment. After the Insight server performs the first poll of your environment's assets, the anomaly detection engine calculates and returns a score for the application within that time.

Related tasks

Assigning applications to assets on page 58

Using the Anomalies section

The Anomalies section, which displays only on an application asset page, provides insight into the application infrastructure and enables you to identify abnormal behaviors that could result in service disruptions.

Steps

1. Turn anomaly monitoring on for the desired application and allow it to collect data.

2. While the anomaly detection engine is running, you can view the following information in the Anomalies section of the application asset page:
   - The anomaly detection score is shown by a blue bar, representing a score between 0 and 100. Scoring is performed resource-by-resource and counter-by-counter resulting in an overall significance score for the entire application infrastructure.

   - Application assets view
   Located below the anomaly detection score, this shows how all the assets contribute to the current anomaly score. If an asset is not contributing significantly to the anomaly score, it is represented by 图片。If the asset is contributing to the significance of the anomaly score, either 1, 2, or three blue bars appear, for example, 图片。The values represented by the number of bars indicate the significance of that asset's contribution to the anomaly score as follows: 1 bar = 1-33; 2 bars = 34-67; 3 bars = 68-100. Assets that are assigned to an application (hosts, virtual machines, volumes, internal volumes, and hypervisors) and also assets in the infrastructure that are somehow connected to the assigned assets (for example, nodes, ports, and so on) contribute to the anomaly detection score. Both assets that contribute and those that do not contribute to the specific anomaly are displayed, because the data from the assigned application resources may flow through them. If there are more than 60 assets of one type, the More button displays, which you can click to display the remaining assets. That status of those remaining assets, for example, 图片，appears next to the More button. This example indicates that of a total of 129 assets not shown, 124 of those assets did not contribute to the anomaly score; however, five of those assets did contribute some level of significance to the anomaly score.

   - Anomaly graph
   The anomaly graph displays the highest anomaly score, indicated by the orange circle, for the time range (3 hours, 24 hours, 3 days, 7 days, 30 days, or a custom time range) selected for the application asset page. You can drag your pointer over the chart to see the anomaly scores, indicated by a blue circle, for other points during the time range and then click the blue circle, which will update the application assets view to display the assets that contributed to the score at that point in time.
3. To aid you in troubleshooting asset performance, you can add an asset from the application assets view to the expert view chart in the application asset page by doing the following:
   a. Click an asset icon in the applications assets view.
      The following displays: The name of the asset, which is a hyperlink to its asset page, the metric that contributed to the anomaly, the significance of the asset's contribution, and a button that enables you to add the asset to the expert view chart.
   b. Click .
      The asset is added to the expert view chart.

**Anomaly detection monitoring status**

Anomaly detection monitoring status is available in application queries, widgets and asset pages.

**Anomaly detection monitoring status**

For each application, you will see one of the following:

- **OK**
  No problems are detected.

- **Learning**
  The anomaly detection server is fetching up to 14 days of performance data, and loading it into the anomaly detection engine.

- **Exceeds maximum assets**
  The maximum number of assets being monitored for an application has been exceeded. No more than 4000 assets can be monitored for an application. Monitoring is paused until the number of assets is less than or equal to 4000. Reduce the number of assets being monitored to continue monitoring.

- **Failed**
  The connection to the anomaly detection server has failed.

- **Not monitored**
  Monitoring is turned off for the application. In queries and widgets, this field is left blank.

**Creating an application performance policy**

You can create an application performance policy based on the anomaly score for the application. Crossing thresholds triggers alerts that notify you about issues related to the resources in your application.

**Before you begin**

The anomaly detection engine must be running on your Insight server in order to monitor the thresholds set in an application performance policy.

**About this task**

You can create policies that provide alerts on different types of anomaly scores you might want to monitor:

- To identify any anomaly spikes, create a policy that alerts on first occurrence with a threshold set to a high anomaly score (>90).
• To identify a change in behavior over time, create a policy that alerts after 1 hour on a medium-high anomaly score. This policy provides an alert based on 3 consecutive anomaly detection scores.

**Steps**

1. Open OnCommand Insight in your browser.
2. Click Manage > Performance Policies
   The Performance Policies page is displayed.
3. Click +Add.
   The Add Policy dialog box is displayed.
4. Enter a unique policy name in the **Policy Name** field.
   You must use a name that is different from all the other policy names for the object.
5. From the **Apply to objects of type** list, select Application.
6. Select the application priority from the **Application Priority** list.
7. 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 crossed on the first score. All other options trigger an alert when the threshold is crossed once and is continuously crossed for at least the specified amount of time.
   The anomaly score is provided in 30 minute intervals (at 5 minutes past the hour and 35 minutes past the hour), therefore only time periods divisible by 30 should be selected.

<table>
<thead>
<tr>
<th>Apply after window of</th>
<th>Number of buckets required to throw violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>First occurrence</td>
<td>1</td>
</tr>
<tr>
<td>5 minutes</td>
<td>2</td>
</tr>
<tr>
<td>10 minutes</td>
<td>2</td>
</tr>
<tr>
<td>15 minutes</td>
<td>2</td>
</tr>
<tr>
<td>30 minutes</td>
<td>2</td>
</tr>
<tr>
<td>45 minutes</td>
<td>3</td>
</tr>
<tr>
<td>1 hour</td>
<td>3</td>
</tr>
<tr>
<td>2 hour</td>
<td>4</td>
</tr>
</tbody>
</table>

8. From the **Warning** list, select Critical or Warning
9. Configure Email if you want to change the default Email notification method.
10. In the **Create alert if** section, select an operator, and then enter a value to create a threshold. The anomaly score is the only performance counter used for application performance policies.
   You can create a set of alerts using ranges similar to the following:
   • 0-20 Warning alert
   • 21-50 Warning alert
   • 51-80 Warning alert
• >80 Critical alert

11. Select the **Stop processing further policies if alert is generated** check box if you want the policy to stop processing when an alert occurs.

**Result**

Notifications are not the only means of viewing violations. Violations are displayed on the application landing page and the violations dashboard, where you can filter them. You can also create a dashboard, add a violation table widget, and filter on your performance policy name to identify application violations.

**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 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 . 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

OnCommand Insight 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.

<table>
<thead>
<tr>
<th>Annotation types</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>User-friendly name for a resource.</td>
<td>Text</td>
</tr>
<tr>
<td>Birthday</td>
<td>Date when the device was or will be brought online.</td>
<td>Date</td>
</tr>
<tr>
<td>Building</td>
<td>Physical location of host, storage, switch, and tape resources.</td>
<td>List</td>
</tr>
<tr>
<td>City</td>
<td>Municipality location of host, storage, switch, and tape resources.</td>
<td>List</td>
</tr>
<tr>
<td>Compute Resource Group</td>
<td>Group assignment used by the Host and VM Filesystems data source.</td>
<td>List</td>
</tr>
<tr>
<td>Continent</td>
<td>Geographic location of host, storage, switch, and tape resources.</td>
<td>List</td>
</tr>
<tr>
<td>Country</td>
<td>National location of host, storage, switch, and tape resources.</td>
<td>List</td>
</tr>
<tr>
<td>Data Center</td>
<td>Physical location of the resource and is available for hosts, storage arrays, switches, and tapes.</td>
<td>List</td>
</tr>
<tr>
<td>Direct Attached</td>
<td>Indicates (Yes or No) if a storage resource is connected directly to hosts.</td>
<td>Boolean</td>
</tr>
<tr>
<td>End of Life</td>
<td>Date when a device will be taken offline, for example, if the lease expired or the hardware is being retired.</td>
<td>Date</td>
</tr>
<tr>
<td>Fabric Alias</td>
<td>User-friendly name for a fabric.</td>
<td>Text</td>
</tr>
<tr>
<td>Floor</td>
<td>Location of a device on a floor of a building. Can be set for hosts, storage arrays, switches, and tapes.</td>
<td>List</td>
</tr>
<tr>
<td>Hot</td>
<td>Devices already in heavy use on a regular basis or at the threshold of capacity.</td>
<td>Boolean</td>
</tr>
<tr>
<td>Note</td>
<td>Comments that you want associated with a resource.</td>
<td>Text</td>
</tr>
<tr>
<td>Rack</td>
<td>Rack in which the resource resides.</td>
<td>Text</td>
</tr>
<tr>
<td>Room</td>
<td>Room within a building or other location of host, storage, switch, and tape resources.</td>
<td>List</td>
</tr>
<tr>
<td>SAN</td>
<td>Logical partition of the network. Available on hosts, storage arrays, tapes, switches, and applications.</td>
<td>List</td>
</tr>
<tr>
<td>Annotation types</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Service Level</td>
<td>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.</td>
<td>List</td>
</tr>
<tr>
<td>State/Province</td>
<td>State or province in which the resource is located.</td>
<td>List</td>
</tr>
<tr>
<td>Sunset</td>
<td>Threshold set after which no new allocations can be made to that device. Useful for planned migrations and other pending network changes.</td>
<td>Date</td>
</tr>
<tr>
<td>Switch Level</td>
<td>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.</td>
<td>List</td>
</tr>
<tr>
<td>Tier</td>
<td>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.</td>
<td>List</td>
</tr>
<tr>
<td>Violation Severity</td>
<td>Rank (for example, major) of a violation (for example, missing host ports or missing redundancy), in a hierarchy of highest to lowest importance.</td>
<td>List</td>
</tr>
</tbody>
</table>

*Note:* Annotation types that cannot be deleted or renamed include 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 Insight web 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.

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.

**Note:** 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.

      a. Click **Add** to add additional values.

      b. Click **Delete** to remove a value.

7. Click **Save**.

Your annotations appear in the list on the Annotations page.
After you finish

In the web UI, the annotation is available immediately for use. To use the annotation in the Java client, you must restart any running Java client before you can apply the annotation. If you are adding or changing annotation values, or deleting an annotation type, you do not need to restart the Java client.

Related references

Importing and Exporting user data on page 91

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 Insight web 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.
      **Note:** 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 ➕. 
   
   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 Insight web 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 Insight web 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 the Annotation 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 Insight web 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 (\(\rightarrow\)) 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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>id-&gt;&lt;id&gt; or &lt;Name&gt; or &lt;IP&gt;</td>
</tr>
<tr>
<td>VM</td>
<td>id-&gt;&lt;id&gt; or &lt;Name&gt;</td>
</tr>
<tr>
<td>Storage pool</td>
<td>id-&gt;&lt;id&gt; or &lt;Storage_name&gt;-&lt;Storage_Pool_name&gt;</td>
</tr>
<tr>
<td>Internal volume</td>
<td>id-&gt;&lt;id&gt; or &lt;Storage_name&gt;-&lt;Internal_volume_name&gt;</td>
</tr>
<tr>
<td>Volume</td>
<td>id-&gt;&lt;id&gt; or &lt;Storage_name&gt;-&lt;Volume_name&gt;</td>
</tr>
</tbody>
</table>
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
   java -jar rest-import-utility.jar [-username] [-password]
   [-aserver name or IP address] [-batch size] [-ccase sensitive:true/false]
   [-lexta 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.

   **Note:** There are no spaces between the options and their values.
**Note:** 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.

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

5. Click ✅ to display the assets.

6. To add a criteria, click ⬇️ More, 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.

   Note: 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 references

Importing and Exporting user data on page 91

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.

**Note:** 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.

**Note:** 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 Insight web 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 , 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 Insight web 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 , 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 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 , 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.

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.

    **Example**
    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.

  Note: 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.

  Note: 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.

  **Note:** 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.

  **Note:** 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.

  **Note:** 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.
**Insight data source management**

Data sources are the most critical component used to maintain an OnCommand Insight environment. Because they are the primary source of information for Insight, it is imperative that you maintain data sources in a running state.

You can monitor the data sources in your network by selecting a data source to check the events related to its status and noting any changes that might have caused problems.

In addition to examining an individual data source, you can perform these operations:

- Clone a data source to create many similar data sources in Insight
- Edit data source information
- Change credentials
- Control polling
- Delete the data source
- Install data source patches
- Install a new data source from a patch
- Prepare an error report for NetApp Customer Support

**Setting up your data sources in Insight**

Data sources are the most critical component when trying to maintain a Insight environment. Data sources discover network information that is used for analysis and validation. You need to configure your data sources within Insight so that they can be monitored within your network.

For each data source, the specific requirements to define that data source depend on the vendor and model of the corresponding devices. Before adding the data sources, you need network addresses, account information, and passwords for all devices and possibly these additional details:

- Switches
- Device management stations
- Storage systems that have IP connectivity
- Storage management stations
- Host servers running management software for storage devices that do not have IP connectivity

For more information about your data source definitions, see the "Vendor-specific data source reference" information in this section.

**Data source support information**

As part of your configuration planning, you should ensure that the devices in your environment can be monitored by Insight. To do so, you can check the Data source support matrix for details about
operating systems, specific devices, and protocols. Some data sources might not be available on all operating systems.

**Location of the most up-to-date version of the Data Source Support Matrix**

The OnCommand Insight Data Source Support Matrix is updated with each service pack release. The latest version of the document can be found at the NetApp Support Site: mysupport.netapp.com/NOW/products/interoperability/.

**Adding data sources**

You can add data sources quickly, using the Add data source dialog box.

**Steps**

1. Open OnCommand Insight in your browser and log in as a user with administrative permissions.
2. Select **Admin** and choose **Data sources**.
3. Click the **+Add** button.
   The Add data source wizard opens.
4. In the **Settings** section, enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique network name for this data source. NOTE: only letters, numbers and the underscore (_) character are allowed in the data source name.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Choose the vendor of the data source from the drop-down.</td>
</tr>
<tr>
<td>Model</td>
<td>Choose the model of the data source from the drop-down.</td>
</tr>
<tr>
<td>Where to run</td>
<td>Choose Local, or you may choose a remote acquisition unit if RAU's are configured in your environment.</td>
</tr>
<tr>
<td>What to collect</td>
<td>For most data sources, these options will be Inventory and Performance. Inventory is always selected by default and cannot be un-selected. Note that some data sources may have different options. The collection options you select change the available fields in the Configuration and Advanced configuration sections.</td>
</tr>
</tbody>
</table>
5. Click the **Configuration** link and enter the basic setup information required for the data source with your selected data collection type.
6. If this type of data source usually requires more detailed information to set it up in your network, click the **Advanced configuration** link to enter additional information.
7. For details about configuration or advanced configuration information required or available for your specific data source, see the Vendor-specific data source reference on page 97.
8. Click the **Test** link to be certain that the data source is properly configured.
9. Click **Save**.
Importing data sources from a spreadsheet

You can import multiple data sources into OnCommand Insight from a spreadsheet. This might be helpful if you already maintain your discovery devices in a spreadsheet. This process adds new data sources, but cannot be used to update existing data sources.

**About this task**

OnCommand Insight includes a spreadsheet to help you create data sources. This spreadsheet has the following attributes:

- The spreadsheet can be used with Microsoft Excel 2003 or later.
- Each tab holds one data source type, for example, Brocade SSH/CLI.
- Each row represents an instance of a new data source to be created.

The spreadsheet includes a macro that creates a new data source in OnCommand Insight.

**Steps**

1. Locate the spreadsheet in the `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
2. In the spreadsheet, enter data source information in the cells with color.
3. Delete empty rows.
4. From the spreadsheet, run the CreateDataSources macro to create the data sources.
5. When prompted for credentials, enter the OnCommand Insight Server administration user name and password.
   
   The results are logged in the acquisition log.
6. A prompt asks if the machine currently running the macro has OnCommand Insight installed.
   
   Select one of the following:
   - No: Select "No" if a batch file will be created that must be run on the OnCommand Insight machine. Run this batch file from the install directory.
   - Yes: Select "Yes" if OnCommand Insight is already installed and no additional steps are required to generate the data source information.
7. To verify the addition of the data sources, open Insight in your browser.
8. On the Insight toolbar, click **Admin**.
9. Check the Data sources list for the data sources you imported.

Adding a new data source by patch

New data sources are released as patch files that can be loaded onto the system using the patch process. This process enables new data sources to be available between scheduled releases of OnCommand Insight.

**Before you begin**

You must have uploaded the patch file that you want to install.
Steps
1. On the Insight toolbar, click Admin.
2. Select Patches.
3. Select Actions > Install service pack or patch.
4. In the Install Service Pack or Patch dialog box, click Browse to locate and select the patch file that you uploaded.
5. Click Next in the Patch Summary dialog box.
6. Review the Read Me information, and click Next to continue.
7. In the Install dialog box, click Finish.

Cloning a data source

Using the clone facility, you can quickly add a data source that has the same credentials and attributes as another data source. Cloning allows you to easily configure multiple instances of the same device type.

Steps
1. On the Insight toolbar, click Admin.
   The Data sources list opens.
2. Highlight the data source that has the setup information you want to use for your new data source.
3. To the right of the highlighted data source, click the Clone icon.
   The Clone this data source dialog box lists the information you must supply for the selected data source, as shown in this example for a NetApp data source:

   ![Clone this data source dialog box](image)

   - **Data source name**
   - **Address of Filer**
   - **Address of HA Partner Filer in Cluster**

   4. Enter the required information in the fields; those details cannot be copied from the existing data source.
   5. Click Clone.
Result
The clone operation copies all other attributes and settings to create the new data source.

Testing the data source configuration
When you are adding a data source, you can verify the correctness of configuration to communicate with the device before saving or updating that data source.

When you click the Test button in the data source wizard, communication with the specified device is checked. The test produces one of these results:

• PASSED: the data source is configured correctly.

• WARNING: the testing was incomplete, probably due to timing out during processing or acquisition not running.

• FAILED: the data source, as configured, cannot communicate with the specified device. Check your configuration settings and re-test.

Vendor-specific data source reference
The configuration details vary depending on the vendor and model of the data source being added.

If a vendor's data source requires advanced Insight configuration instructions, such as special requirements and specific commands, that information is included in this section.

3PAR InServ data source
OnCommand Insight uses the 3PAR InServ (Firmware 2.2.2+, SSH) data source to discover inventory for HP 3PAR StoreServ storage arrays.

Terminology
OnCommand Insight acquires the following inventory information from the 3PAR InServ data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage System</td>
<td>Storage</td>
</tr>
<tr>
<td>Controller Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Common Provisioning Group</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Virtual Volume</td>
<td>Volume</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements
• IP address or FQDN of the InServ cluster
• For inventory, read-only user name and password to the InServ Server.
• For performance, read-write user name and password to the InServ Server.
• Port requirements: 22 (inventory collection), 5988 or 5989 (performance collection) [Note: 3PAR Performance is supported for InServ OS 3.x+]

• For performance collection confirm that SMI-S is enabled by logging into the 3PAR array via SSH.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster IP</td>
<td>IP address or fully-qualified domain name of the InServ cluster</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the InServ Server</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the InServ Server</td>
</tr>
<tr>
<td>SMI-S Host IP</td>
<td>IP address of the SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S User Name</td>
<td>User name for the SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S Password</td>
<td>Password used for the SMI-S Provider Host</td>
</tr>
</tbody>
</table>

**Advanced Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Exclude Devices</td>
<td>Comma-separated list of device IPs to exclude</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Number of SSH Retries</td>
<td>Number of SSH retry attempts</td>
</tr>
<tr>
<td>SSH Banner Wait Timeout (sec)</td>
<td>SSH banner wait timeout (default 20 seconds)</td>
</tr>
<tr>
<td>SMI-S Port</td>
<td>Port used by SMI-S Provider Host</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used to connect to the SMI-S provider</td>
</tr>
<tr>
<td>SMI-S namespace</td>
<td>SMI-S namespace</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>Number of SMI-S Connection Retries</td>
<td>Number of SMI-S connection retry attempts</td>
</tr>
</tbody>
</table>

**Amazon AWS EC2 data source**

OnCommand Insight uses this data source to discover inventory and performance for Amazon AWS EC2.

**Pre-requisites:**

• The IAM Access Key ID and Secret Access Key for your Amazon AWS EC2 cloud account
How to configure this data source

To configure the Amazon AWS EC2 data source, you will need the AWS IAM Access Key ID and Secret Access Key for your AWS account.

Fill in the data source fields according to the tables below:

**Configuration:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Region</td>
<td>Choose AWS region</td>
</tr>
<tr>
<td>AWS IAM Access Key ID</td>
<td>Enter AWS IAM Access Key ID</td>
</tr>
<tr>
<td>AWS IAM Secret Access Key</td>
<td>Enter AWS IAM Secret Access Key</td>
</tr>
<tr>
<td>I understand AWS will</td>
<td>Check this to verify your understanding that AWS</td>
</tr>
<tr>
<td>bill me for API requests</td>
<td>bills you for API requests made by Insight polling</td>
</tr>
</tbody>
</table>

**Advanced Configuration:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>HTTP connection and socket timeout (sec)</td>
<td>HTTP connection timeout (default 300 seconds)</td>
</tr>
<tr>
<td>Include AWS tags</td>
<td>Check this to enable support for AWS tags in Insight annotations</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 1800 seconds)</td>
</tr>
</tbody>
</table>

**Mapping AWS tags to Insight annotations**

The AWS EC2 data source includes an option that allows you to populate Insight annotations with tags configured on AWS. The annotations must be named exactly as the AWS tags. Insight will always populate same-named text-type annotations, and will make a "best attempt" to populate annotations of other types (number, boolean, etc). If your annotation is of a different type and the data source fails to populate it, it may be necessary to remove the annotation and re-create it as a text type.

Note that AWS is case-sensitive, while Insight is case-insensitive. So if you create an annotation named “OWNER” in Insight, and tags named “OWNER”, “Owner”, and “owner” in AWS, all of the AWS variations of “owner” will map to Insight's “OWNER” annotation.

**Brocade Enterprise Fabric Connectivity Manager data source**

OnCommand Insight uses the Brocade Enterprise Fabric Connectivity Manager (EFCM) data source to discover inventory for Brocade EFCM switches. Insight supports EFCM versions 9.5, 9.6, and 9.7.

**Requirements**

- Network address or fully-qualified domain name for the EFCM server
- EFCM version must be 9.5, 9.6, or 9.7
• IP address of the EFCM server
• Read-only username and password for the EFCM server
• Validated access to the Connectrix switch by Telnet from the Insight server, using the read-only username and password over port 51512

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFC server</td>
<td>IP address or fully-qualified domain name of the EFC Server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the switch</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the switch</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 15 minutes)</td>
</tr>
<tr>
<td>Fabric Name</td>
<td>Fabric name to be reported by the EFCM data source. Leave blank to report the fabric name as WWN.</td>
</tr>
<tr>
<td>Communication Port</td>
<td>Port used for communication with the switch</td>
</tr>
<tr>
<td>Enable Trapping</td>
<td>Select to enable acquisition upon receiving an SNMP trap from the device. If you select enable trapping, you must also activate SNMP.</td>
</tr>
<tr>
<td>Minimum Time Between Traps (sec)</td>
<td>Minimum time between acquisition attempts triggered by traps (default 15 seconds)</td>
</tr>
<tr>
<td>Inactive Zonesets</td>
<td>Comma-separated list of inactive Zonesets on which to perform acquisition, in addition to performing acquisition on the active zone sets</td>
</tr>
<tr>
<td>NIC to Use</td>
<td>Specify which network interface should be used on the RAU when reporting on SAN devices</td>
</tr>
<tr>
<td>Exclude Devices</td>
<td>Comma-separated list of unit names to include or exclude from polling</td>
</tr>
<tr>
<td>Use the EFCM switch nickname as the Insight switch name</td>
<td>Select to use the EFCM switch nickname as the Insight switch name</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**Brocade FC Switch data source**

OnCommand Insight uses the Brocade FC Switch (SSH) data source to discover inventory for Brocade or rebranded switch devices running Factored Operating System (FOS) firmware 4.2 and later. Devices in both FC switch and Access Gateway modes are supported.

**Terminology**

OnCommand Insight acquires the following inventory information from the Brocade FC Switch data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:
<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>Switch</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>Virtual Fabric, Physical Fabric</td>
<td>Fabric</td>
</tr>
<tr>
<td>Zone</td>
<td>Zone</td>
</tr>
<tr>
<td>Logical Switch</td>
<td>Logical Switch</td>
</tr>
<tr>
<td>LSAN Zone</td>
<td>IVR Zone</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- There must be IP connectivity to all switches in the fabric. If you select the Discover all switches in the fabric check box, OCI identifies all the switches in the fabric; however, it needs IP connectivity to these additional switches to discover them.

- The same account is needed globally across all switches in the fabric. You can use PuTTY (open source terminal emulator) to confirm access.

- If the Perform license is installed, ports 161 and 162 must be open to all switches in the fabric for SNMP performance polling.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch IP</td>
<td>IP address or fully-qualified domain name of the switch</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the switch</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the switch</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMP version</td>
</tr>
<tr>
<td>SNMP Community String</td>
<td>SNMP read-only community string used to access the switch</td>
</tr>
<tr>
<td>SNMP User Name</td>
<td>SNMP version protocol user name (applies only to SNMP v3)</td>
</tr>
<tr>
<td>SNMP Password</td>
<td>SNMP version protocol password (applies only to SNMP v3)</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Name</td>
<td>Fabric name to be reported by the data source. Leave blank to report the fabric name as WWN.</td>
</tr>
<tr>
<td>Exclude Devices</td>
<td>Comma-separated list of device IDs to exclude from polling</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 15 minutes)</td>
</tr>
<tr>
<td>Timeout (sec)</td>
<td>Connection timeout (default 30 seconds)</td>
</tr>
<tr>
<td>Banner Wait Timeout (sec)</td>
<td>SSH banner wait timeout (default 5 seconds)</td>
</tr>
<tr>
<td>Admin Domains Active</td>
<td>Select if using Admin Domains</td>
</tr>
</tbody>
</table>
### Brocade Sphereon/Intrepid Switch data source

OnCommand Insight uses the Brocade Sphereon/Intrepid Switch (SNMP) data source to discover inventory for Brocade Sphereon or Intrepid switches.

#### Requirements

- There must be IP connectivity to all switches in the fabric. If you select the Discover all switches in the fabric check box, OCI identifies all the switches in the fabric; however, it needs IP connectivity to these additional switches to discover them.
- Read-only community string if using SNMP V1 or SNMP V2.
- HTTP access to the switch to obtain zoning information.
- Access validation by running the `snmpwalk` utility to the switch (see `<install_path>\bin\`).

#### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sphereon Switch</td>
<td>IP address or fully-qualified domain name of the switch</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMP version</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>SNMP read-only community string used to access the switch</td>
</tr>
<tr>
<td>User Name</td>
<td>SMI-S user name for the switch (SNMP v3 only)</td>
</tr>
<tr>
<td>Password</td>
<td>SMI-S password for the switch (SNMP v3 only)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve MPR Data</td>
<td>Select to acquire routing data from your multiprotocol router (MPR)</td>
</tr>
<tr>
<td>Enable Trapping</td>
<td>Select to enable acquisition upon receiving an SNMP trap from the device. If you select enable trapping, you must also activate SNMP.</td>
</tr>
<tr>
<td>Minimum Time Between Traps (sec)</td>
<td>Minimum time between acquisition attempts triggered by traps (default 10 seconds)</td>
</tr>
<tr>
<td>Discover all switches in the fabric</td>
<td>Select to discover all switches in the fabric</td>
</tr>
<tr>
<td>Choose Favoring HBA vs. Zone Aliases</td>
<td>Choose whether to favor HBA or zone aliases</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>SNMP Auth Protocol</td>
<td>SNMP authentication protocol (SNMP v3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Protocol</td>
<td>SNMP privacy protocol (SNMP v3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Password</td>
<td>SNMP privacy password (SNMP v3 only)</td>
</tr>
<tr>
<td>SNMP Retries</td>
<td>Number of SNMP retry attempts</td>
</tr>
<tr>
<td>SNMP Timeout (ms)</td>
<td>SNMP timeout (default 5000 ms)</td>
</tr>
</tbody>
</table>
Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 15 minutes)</td>
</tr>
<tr>
<td>SNMP Auth Protocol</td>
<td>SNMP authentication protocol (SNMPv3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Protocol</td>
<td>SNMP privacy protocol (SNMPv3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Password</td>
<td>SNMP privacy password</td>
</tr>
<tr>
<td>SNMP Number of Retries</td>
<td>Number of SNMP retry attempts</td>
</tr>
<tr>
<td>SNMP Timeout (ms)</td>
<td>SNMP timeout (default 5000 ms)</td>
</tr>
<tr>
<td>Fabric Name</td>
<td>Fabric name to be reported by the data source. Leave blank to report the fabric name as WWN.</td>
</tr>
<tr>
<td>Enable Trapping</td>
<td>Select to enable acquisition upon receiving an SNMP trap from the device. If you select enable trapping, you must also activate SNMP.</td>
</tr>
<tr>
<td>Minimum Time Between Traps (seconds)</td>
<td>Minimum time between acquisition attempts triggered by traps (default 10 seconds)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

Cisco FC Switch Firmware (SNMP) data source

OnCommand Insight uses the Cisco FC Switch Firmware 2.0+ (SNMP) data source to discover inventory for Cisco MDS Fibre Channel switches as well as a variety of Cisco Nexus FCoE switches on which the FC service is enabled. Additionally, you can discover many models of Cisco devices running in NPV mode with this data source.

Terminology

OnCommand Insight acquires the following inventory information from the Cisco FC Switch data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>Switch</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>VSAN</td>
<td>Fabric</td>
</tr>
<tr>
<td>Zone</td>
<td>Zone</td>
</tr>
<tr>
<td>Logical Switch</td>
<td>Logical Switch</td>
</tr>
<tr>
<td>Name Server Entry</td>
<td>Name Server Entry</td>
</tr>
<tr>
<td>Inter-VSAN Routing (IVR) Zone</td>
<td>IVR Zone</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- An IP address of one switch in the fabric or individual switches
• Chassis discovery, to enable fabric discovery
• If using SNMP V2, read-only community string
• Access validation using the `snmpwalk` utility to the switch (see `<install_path>\bin\`)

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Switch IP</td>
<td>IP address or fully-qualified domain name of the switch</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>SNMP version v2 or later is required for performance acquisition</td>
</tr>
<tr>
<td>SNMP Community String</td>
<td>SNMP read-only community string used to access the switch (not applicable for SNMP v3)</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the switch (SNMP v3 only)</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the switch (SNMPv3 only)</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>SNMP Auth Protocol</td>
<td>SNMP authentication protocol (SNMPv3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Protocol</td>
<td>SNMP privacy protocol (SNMPv3 only)</td>
</tr>
<tr>
<td>SNMP Privacy Password</td>
<td>SNPMP privacy password</td>
</tr>
<tr>
<td>SNMP Retries</td>
<td>Number of SNMP retry attempts</td>
</tr>
<tr>
<td>SNMP Timeout (ms)</td>
<td>SNMP timeout (default 5000 ms)</td>
</tr>
<tr>
<td>Enable Trapping</td>
<td>Select to enable trapping. If you enable trapping, you must also activate SNMP notifications.</td>
</tr>
<tr>
<td>Minimum Time Between Traps (sec)</td>
<td>Minimum time between acquisition attempts triggered by traps (default 10 seconds)</td>
</tr>
<tr>
<td>Discover All Fabric Switches</td>
<td>Select to discover all switches in the fabric</td>
</tr>
<tr>
<td>Exclude Devices</td>
<td>Comma-separated list of device IPs to exclude from polling</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include Devices</td>
<td>Comma-separated list of device IPs to include in polling</td>
</tr>
<tr>
<td>Check Device Type</td>
<td>Select to accept only those devices that explicitly advertise themselves as Cisco devices</td>
</tr>
<tr>
<td>Primary Alias Type</td>
<td>Provide a first preference for resolution of the alias. Choose from the following:</td>
</tr>
<tr>
<td></td>
<td><strong>Device Alias</strong></td>
</tr>
<tr>
<td></td>
<td>This is a user-friendly name for a port WWN (pWWN) that can be used in all configuration commands, as required. All switches in the Cisco MDS 9000 Family support Distributed Device Alias Services (device aliases).</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong></td>
</tr>
<tr>
<td></td>
<td>Do not report any alias</td>
</tr>
<tr>
<td></td>
<td><strong>Port Description</strong></td>
</tr>
<tr>
<td></td>
<td>A description to help identify the port in a list of ports</td>
</tr>
<tr>
<td></td>
<td><strong>Zone Alias (all)</strong></td>
</tr>
<tr>
<td></td>
<td>A user-friendly name for a port that can be used only for zoning configuration</td>
</tr>
<tr>
<td></td>
<td><strong>Zone Alias (only active)</strong></td>
</tr>
<tr>
<td></td>
<td>A user-friendly name for a port that can be used only for the active configuration. This is the default.</td>
</tr>
<tr>
<td>Secondary Alias Type</td>
<td>Provide a second preference for resolution of the alias</td>
</tr>
<tr>
<td>Tertiary Alias Type</td>
<td>Provide a third preference for resolution of the alias</td>
</tr>
<tr>
<td>Enable SANTap Proxy Mode Support</td>
<td>Select if your Cisco switch is using SANTap in proxy mode. If you are using EMC RecoverPoint, then you are probably using SANTap.</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**Dell Compellent Storage Center data source**

The Dell Compellent Storage Center data source collects network information for analysis and validation from Dell Compellent Storage Center storage arrays using the Dell Compellent Enterprise Manager. This data source uses the Dell Java API.

**Terminology**

OnCommand Insight acquires the following inventory information from the Dell Compellent data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Disk Folder</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Vendor/Model Term</td>
<td>Insight Term</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Storage Center</td>
<td>Storage</td>
</tr>
<tr>
<td>Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>Fiber Channel I/O Port</td>
<td>Port</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- Administrator credentials for the Dell Compellent Enterprise Manager server.
- IP address of the Compellent Enterprise Manager server
- Port 3033 for access to the device

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address of Enterprise Manager</td>
<td>IP address of the Compellent Enterprise Manager server</td>
</tr>
<tr>
<td>Port</td>
<td>Port used for communication with of the Compellent Enterprise Manager server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the Compellent Enterprise Manager server</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the Compellent Enterprise Manager server</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (up to 3600 seconds)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**EMC Celerra data source**

The Celerra (SSH) data source collects inventory information from Celerra storage. For configuration, this data source requires the IP address of the storage processors and a read-only user name and password.

**Terminology**

OnCommand Insight acquires the following inventory information from the EMC Celerra data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Celerra Network Server</td>
<td>Storage</td>
</tr>
</tbody>
</table>
Vendor/Model Term | Insight Term
--- | ---
Celerra Meta Volume / Celerra Storage Pool | Storage Pool
File System | Internal Volume
Data Mover | Controller
File System mounted on a data Mover | File Share
CIFS and NFS Exports | Share
Disk Volume | Backend LUN

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**
- The IP address of the storage processor
- Read-only user name and password
- SSH access

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address of Celerra</td>
<td>IP address or fully-qualified domain name of the Celerra device</td>
</tr>
<tr>
<td>User Name</td>
<td>Name used to log in to the Celerra device</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to log in to the Celerra device</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (minutes)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 600 seconds)</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of inventory retry attempts</td>
</tr>
<tr>
<td>SSH Banner Wait Timeout (sec)</td>
<td>SSH banner wait timeout (default 20 seconds)</td>
</tr>
</tbody>
</table>

**EMC CLARiiON (NaviCLI) data source**

Before configuring this data source, make sure that the EMC Navisphere CLI is installed on the target device and on the Insight server. The Navisphere CLI version must match the firmware version on the controller. For performance data collection, statistics logging must be turned on.

**NaviSphere Command Line Interface syntax**

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope <scope,use 0 for global scope> -port <use 443 by default> command
```
Terminology

OnCommand Insight acquires the following inventory information from the EMC CLARiiON data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Storage Processor</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Thin Pool, RAID Group</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>LUN</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

Requirements

- An IP address of each CLARiiON storage processor
- Read-only Navisphere username and password to the CLARiiON arrays
- NaviCLI must be installed on the Insight server/RAU
- Access validation: Run NaviCLI from the Insight server to each array using the above username and password.
- NaviCLI version should correspond with the newest FLARE code on your array
- For performance, statistics logging must be turned on.

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLARiiON storage</td>
<td>IP address or fully-qualified domain name of the CLARiiON Storage</td>
</tr>
<tr>
<td>User Name</td>
<td>Name used to log into the CLARiiON storage device.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to log into the CLARiiON storage device.</td>
</tr>
<tr>
<td>CLI Path to navicli.exe or naviseccli.exe path</td>
<td>Full path to the navicli.exe OR naviseccli.exe executable</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Use Secure Client (naviseccli)</td>
<td>Select to use secure client (naviseccli)</td>
</tr>
<tr>
<td>Scope</td>
<td>The secure client scope. The default is Global.</td>
</tr>
<tr>
<td>CLARiiON CLI Port</td>
<td>Port used for CLARiiON CLI</td>
</tr>
</tbody>
</table>
EMC Data Domain data source

This data source collects storage and configuration information from EMC Data Domain deduplication storage systems. To add the data source, you must use specific configuration instructions and commands and be aware of data source requirements and usage recommendations.

Terminology

OnCommand Insight acquires the following inventory information from the EMC Data Domain data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>Filesys</td>
<td>Internal Volume</td>
</tr>
<tr>
<td>Mtree</td>
<td>QTree</td>
</tr>
<tr>
<td>Quota</td>
<td>Quota</td>
</tr>
<tr>
<td>NFS and CIFS share</td>
<td>FileShare</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- IP address of the Data Domain device
- Read-only user name and password to the Data Domain storage
- SSH port 22

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address or fully-qualified domain name of the Data Domain storage array</td>
</tr>
<tr>
<td>User name</td>
<td>The user name for the Data Domain storage array</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the Data Domain storage array</td>
</tr>
</tbody>
</table>
**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 180 seconds)</td>
</tr>
<tr>
<td>SSH Port</td>
<td>SSH service port</td>
</tr>
</tbody>
</table>

**EMC ECC StorageScope data source**

The EMC ECC StorageScope device has three types of data sources: 5.x, 6.0, and 6.1.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC server</td>
<td>IP address or fully-qualified domain name of the ECC Server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the ECC server</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the ECC server</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC Port</td>
<td>Port used for the ECC server</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 30 minutes)</td>
</tr>
<tr>
<td>Protocol to Connect to Database</td>
<td>Protocol Used to Connect to the Database</td>
</tr>
<tr>
<td>Query File System Information</td>
<td>Select to retrieve details for WWN Aliases and File Systems.</td>
</tr>
</tbody>
</table>

**EMC Isilon data source**

The Isilon SSH data source collects inventory and performance from EMC Isilon scale-out NAS storage.

**Terminology**

OnCommand Insight acquires the following inventory information from the EMC Isilon data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive</td>
<td>Disk</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>File System</td>
<td>Internal Volume</td>
</tr>
</tbody>
</table>
Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- Administrator permissions to the Isilon storage
- Validated access by using `telnet` to port 22

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address or fully-qualified domain name of the Isilon cluster</td>
</tr>
<tr>
<td>User name</td>
<td>The user name for the Isilon cluster</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the Isilon cluster</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>SSH Process Wait Timeout</td>
<td>SSH process timeout (default 60 seconds)</td>
</tr>
<tr>
<td>SSH Port</td>
<td>SSH service port</td>
</tr>
</tbody>
</table>

EMC RecoverPoint data source

The EMC RecoverPoint data source collects inventory information from EMC recoverPoint storage. For configuration, the data source requires the IP address of the storage processors and a read-only user name and password.

The EMC RecoverPoint data source gathers the volume-to-volume replication relationships that RecoverPoint coordinates across other storage arrays. OnCommand Insight shows a storage array for each RecoverPoint cluster, and collects inventory data for nodes and storage ports on that cluster. No storage pool or volume data is collected.

Requirements

- IP address or fully-qualified domain name of storage processor
- Read-only user name and password
- SSH access via PuTTY
Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address of RecoverPoint</td>
<td>IP address or fully-qualified domain name of RecoverPoint cluster</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the RecoverPoint cluster</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the RecoverPoint cluster</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>TCP Port used to connect to Recoverpoint cluster</td>
</tr>
<tr>
<td>Inventory Poll Interval (minutes)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Excluded Clusters</td>
<td>Comma-separated list of cluster IDs or names to exclude when polling</td>
</tr>
</tbody>
</table>

EMC Solutions Enabler with SMI-S Performance data source

OnCommand Insight discovers Symmetrix storage arrays by using Solutions Enabler `symcli` commands in conjunction with an existing Solutions Enabler server in your environment. The existing Solutions Enabler server has connectivity to the Symmetrix storage array through access to gatekeeper volumes. Administrator permissions are required to access this device.

Terminology

OnCommand Insight acquires the following inventory information from the EMC Solutions Enabler data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Disk Group</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Storage Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Director</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Device Pool, Storage Resource Pool (SRP)</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Device, TDev</td>
<td>Volume</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

Before configuring this data source, you should ensure that the OnCommand Insight server has TCP connectivity to port 2707 on the existing Solutions Enabler server. OnCommand Insight discovers all the Symmetrix arrays that are “Local” to this server, as seen in “symcfg list” output from that server.

- The EMC Solutions Enabler (CLI) with SMI-S provider application must be installed and the version must match or be earlier than the version running on the Solutions Enabler Server.
• A properly configured \{installdir\}\EMC\SYMAPI\config\netcnfg file is required. This file defines service names for Solutions Enabler servers, as well as the access method (SECURE / NOSECURE / ANY).

• If you require read/write latency at the storage node level, the SMI-S Provider must communicate with a running instance of the UNISPHERE for VMAX application.

• Administrator permissions on the Solutions Enabler (SE) Server

• Read-only user name and password to the SE software

• Solutions Enabler Server 6.5X requirements:
  ◦ SMI-S provider 3.3.1 for SMIS-S V1.2 installed
  ◦ After install, run \Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd

• The UNISPHERE for VMAX application must be running and collecting statistics for the Symmetrix VMAX storage arrays that are managed by the SMI-S Provider installation

• Access validation: Verify that the SMI-S provider is running: `telnet <se_server> 5988`

  **Note:** If SMI-S user authentication is not enabled, the default values in the OnCommand Insight data source are ignored.

Having symauth enabled on Symmetrix arrays might inhibit the ability of OnCommand Insight to discover them. OnCommand Insight Acquisition runs as the SYSTEM user on the OnCommand Insight / Remote Acquisition Unit server that is communicating with the Solutions Enabler server. If hostname\SYSTEM does not have symauth privileges, OnCommand Insight fails to discover the array.

**Configuration**

The EMC Solutions Enabler Symmetrix CLI data source includes support for device configuration for thin provisioning and Symmetrix Remote Data Facility (SRDF).

Definitions are supplied for Fibre Channel and Switch Performance packages.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Service name as specified in netcnfg file</td>
</tr>
<tr>
<td>Full path to CLI</td>
<td>Full path to the Symmetrix CLI</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Choose 'Exclude' or 'Include' to</td>
<td>Specify whether to include or exclude the array list below when collecting</td>
</tr>
<tr>
<td>specify a list</td>
<td>data</td>
</tr>
<tr>
<td>Inventory Exclude Devices</td>
<td>Comma-separated list of device IDs to include or exclude</td>
</tr>
</tbody>
</table>
### Field Description

**Connection Caching**

Choose connection caching method:

- **LOCAL** means that the OnCommand Insight Acquisition service is running on the Solutions Enabler server, which has Fibre Channel connectivity to the Symmetrix arrays you seek to discover, and has access to gatekeeper volumes. This might be seen in some Remote Acquisition Unit (RAU) configurations.

- **REMOTE_CACHED** is the default and should be used in most cases. This uses the NETCNFG file settings to connect using IP to the Solutions Enabler server, which must have Fibre Channel connectivity to the Symmetrix arrays you seek to discover, and has access to Gatekeeper volumes.

- In the event that **REMOTE_CACHED** options make CLI commands fail, use the **REMOTE** option. Keep in mind that it will slow down the acquisition process (possibly to hours or even days in extreme cases). The NETCNFG file settings are still used for an IP connection to the Solutions Enabler server that has Fibre Channel connectivity to the Symmetrix arrays being discovered.

**Note:** This setting does not change OnCommand Insight behavior with respect to the arrays listed as **REMOTE** by the "symcfg list" output. OnCommand Insight gathers data only on devices shown as **LOCAL** by this command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI Timeout (sec)</td>
<td>CLI process timeout (default 7200 seconds)</td>
</tr>
<tr>
<td>SMI-S Host IP</td>
<td>IP address of the SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S Port</td>
<td>Port used by SMI-S Provider Host</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used to connect to the SMI-S provider</td>
</tr>
<tr>
<td>SMI-S Namespace</td>
<td>Interoperability namespace that the SMI-S provider is configured to use</td>
</tr>
<tr>
<td>SMI-S User Name</td>
<td>User name for the SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S Password</td>
<td>User name for the SMI-S Provider Host</td>
</tr>
<tr>
<td>Performance Polling Interval (sec)</td>
<td>Interval between performance polls (default 1000 seconds)</td>
</tr>
<tr>
<td>Performance Filter Type</td>
<td>Specify whether to include or exclude the array list below when collecting performance data</td>
</tr>
<tr>
<td>Performance Filter Device List</td>
<td>Comma-separated list of device IDs to include or exclude</td>
</tr>
<tr>
<td>RPO Polling Interval (sec)</td>
<td>Interval between RPO polls (default 300 seconds)</td>
</tr>
</tbody>
</table>
EMC VNX data source

For configuration, the EMC VNX (SSH) data source requires the IP address of the Control Station and a read-only username and password.

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNX IP</td>
<td>IP address or fully-qualified domain name of the VNX Control Station</td>
</tr>
<tr>
<td>VNX User Name</td>
<td>User name for the VNX Control Station</td>
</tr>
<tr>
<td>VNX Password</td>
<td>Password for the VNX Control Station</td>
</tr>
</tbody>
</table>

### Requirements

- An IP address of the Control Station
- Read-only username and password.
- Access validation: Verify SSH access via PuTTY.

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>VNX SSH Process Wait Timeout (sec)</td>
<td>VNX SSH process timeout (default 600 seconds)</td>
</tr>
<tr>
<td>Celerra Command Retry Attempts</td>
<td>Number of Celerra command retry attempts</td>
</tr>
<tr>
<td>CLARiiON External Process Timeout for Inventory (sec)</td>
<td>CLARiiON external process timeout for inventory (default 1800 seconds)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>CLARiiON External Process Timeout for Performance (sec)</td>
<td>CLARiiON external process timeout for performance (default 1800 seconds)</td>
</tr>
</tbody>
</table>

### EMC VNXe data source

The EMC VNXe data source provides inventory support for EMC VNXe unified storage arrays. Insight currently supports iSCSI and NAS protocols.

The EMC VNXe data source provides inventory support for EMC VNXe and Unity unified storage arrays.

This data source is CLI-based and requires that you install the Unisphere for VNXe CLI, (uemcli.exe) on the acquisition unit that the VNXe data source resides on. uemcli.exe uses HTTPS as the transport protocol, so the acquisition unit must be able to initiate HTTPS connections to the VNXe/Unity arrays. You must have at least a read-only user for use by the data source.

### Terminology

OnCommand Insight acquires the following inventory information from the EMC VNXe data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:
<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Processor</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>General iSCSI Block info, VMware VMFS</td>
<td>Volume</td>
</tr>
<tr>
<td>Shared Folder</td>
<td>Internal Volume</td>
</tr>
<tr>
<td>CIFS Share, NFS Share, Share from VMware NFS datastore</td>
<td>Share</td>
</tr>
<tr>
<td>Replication Remote System</td>
<td>Synchronization</td>
</tr>
<tr>
<td>iSCSI Node</td>
<td>iSCSI Target Node</td>
</tr>
<tr>
<td>iSCSI Initiator</td>
<td>iSCSI Target Initiator</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

The following are requirements to configure and use this data source:

- The VNXe data collector is CLI based; you must install the Unisphere for VNXe CLI, (uemcli.exe) onto the acquisition unit where your VNXe data collector resides.
- uemcli.exe uses HTTPS as the transport protocol, so the acquisition unit will need to be able to initiate HTTPS connections to the VNXe.
- You must have at least a read-only user for use by the data source.
- IP address of the managing Solutions enabler server.
- HTTPS on Port 443 is required
- The EMC VNXe data collector provides NAS and iSCSI support for inventory; fibre channel volumes will be discovered, but Insight does not report on FC mapping, masking, or storage ports.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNXe Storage</td>
<td>IP address or fully-qualified domain name of the VNXe device</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the VNXe device</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the VNXe device</td>
</tr>
<tr>
<td>Full path to the uemcli executable</td>
<td>Full path to the uemcli.exe executable</td>
</tr>
</tbody>
</table>
Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>VNXe CLI Port</td>
<td>Port used for the VNXe CLI</td>
</tr>
<tr>
<td>Inventory External Process Timeout (sec)</td>
<td>External process timeout (default 1800 seconds)</td>
</tr>
</tbody>
</table>

EMC VPLEX data source

For configuration, this data source requires an IP address of the VPLEX server and an administrative level domain account.

Terminology

OnCommand Insight acquires the following inventory information from the EMC VPLEX data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Engine</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Device, System</td>
<td>Backend Storage Pool</td>
</tr>
<tr>
<td>Extend</td>
<td></td>
</tr>
<tr>
<td>Virtual Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>Front-End Port, Backend Port</td>
<td>Port</td>
</tr>
<tr>
<td>Distributed Device</td>
<td>Storage Synchronization</td>
</tr>
<tr>
<td>Storage View</td>
<td>Volume Map, Volume Mask</td>
</tr>
<tr>
<td>Storage Volume</td>
<td>Backend LUN</td>
</tr>
<tr>
<td>ITLs</td>
<td>Backend Path</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- An IP address of the VPLEX server
- Administrative level domain account for the VPLEX server
- Validate access: Verify by using `telnet` to port 443. For a port other than the default port, with any browser use `HTTPS://<ip>:<port>`

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of VPLEX Management Console</td>
<td>IP address or fully-qualified domain name of the VPLEX Management Console</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for VPLEX CLI</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Password used for VPLEX CLI</td>
</tr>
<tr>
<td>Performance Remote IP Address of VPLEX Management Console</td>
<td>Performance Remote IP address of the VPLEX Management Console</td>
</tr>
<tr>
<td>Performance Remote User Name</td>
<td>Performance Remote user name of VPLEX Management Console</td>
</tr>
<tr>
<td>Performance Remote Password</td>
<td>Performance Remote Password of VPLEX Management Console</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Port</td>
<td>Port used for VPLEX CLI</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of inventory retry attempts</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 600 seconds)</td>
</tr>
<tr>
<td>Performance SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 600 seconds)</td>
</tr>
<tr>
<td>SSH Banner Wait Timeout (sec)</td>
<td>SSH banner wait timeout (default 20 seconds)</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of performance retry attempts</td>
</tr>
</tbody>
</table>

### EMC XtremIO data source

To configure the EMC XtremIO (HTTP) data source, you must have the XtremIO Management Server (XMS) Host address and an account with administrator privileges.

### Terminology

OnCommand Insight acquires the following inventory information from the EMC XtremIO data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk (SSD)</td>
<td>Disk</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>LUN Map</td>
<td>Volume Map</td>
</tr>
<tr>
<td>Initiator, Target</td>
<td>Volume Mask</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.
Requirements

- An IP address of each XtremIO Management Server
- An account with Administrator privileges
- Access to port 443 (HTTPS)

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMS Host</td>
<td>IP address or fully-qualified domain name of the XtremIO Management Server</td>
</tr>
<tr>
<td>User name</td>
<td>User name for the XtremIO Management Server</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the XtremIO Management Server</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP port</td>
<td>TCP Port used to connect to XTremIO Management Server (default 443 )</td>
</tr>
<tr>
<td>Inventory poll interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Connection timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Performance poll interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

Fujitsu Eternus data source

The Fujitsu Eternus data source requires the IP address of the storage. It cannot be comma delimited.

Terminology

OnCommand Insight acquires the following inventory information from the Fujitsu Eternus data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Thin Pool, Flexible Tier Pool, Raid Group</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Standard Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV)</td>
<td>Volume</td>
</tr>
</tbody>
</table>
Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- An IP address of the Eternus storage, which cannot be comma delimited
- Administration-level user name and password
- Access validation by using SSH to the configured IP and logging in
- Ensure that the page scroll is disabled.

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address of Eternus Storage</td>
<td>IP address of the Eternus storage</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for Eternus storage</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the sternus</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 600 seconds)</td>
</tr>
</tbody>
</table>

HDS HiCommand Device Manager data source

The HDS HiCommand and HiCommand Lite data sources support the HiCommand Device Manager server. OnCommand Insight communicates with the HiCommand Device Manager server using the standard HiCommand API.

Terminology

OnCommand Insight acquires the following inventory information from the HDS HiCommand and HiCommand Lite data sources. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDEV</td>
<td>Disk</td>
</tr>
<tr>
<td>Journal Pool</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Storage Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Port Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Array Group, DP Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Logical Unit, LDEV</td>
<td>Volume</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.
Inventory Requirements

- IP address of the HiCommand Device Manager server
- Read-only user name and password for the HiCommand Device Manager software and peer privileges
- Validate access:
  - Log in to the HiCommand Device Manager software using peer user name and password.
  - Verify access to the HiCommand Device Manager API: `telnet <HiCommand Device_Manager_server_ip> 2001`

Performance Requirements

- HDS USP, USP V, and VSP performance
  - Performance Monitor must be licensed.
  - Monitoring switch must be enabled.
  - The Export Tool (Export.exe) must be copied to the OnCommand Insight Server.
  - The Export Tool version must match the microcode version of the target array.
- HDS AMS performance
  - Performance Monitor needs to be licensed.
  - The Storage Navigator Modular 2 (SNM2) CLI utility needs to be installed on the OnCommand Insight Server.
  - You must register all AMS, WMS, SMS storage arrays whose performance needs to be acquired by OnCommand Insight by using the following command:
    `auunitaddauto.exe -ip <IP address of Controller0> IP address of Controller1>`
  - You must ensure that all the arrays that you registered are listed in the output of this command: `auunitref.exe`.

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiCommand Server</td>
<td>IP address or fully-qualified domain name of the HiCommand Device Manager server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the HiCommand Device Manager server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the HiCommand Device Manager server.</td>
</tr>
</tbody>
</table>
### Devices - VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices - VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages</td>
<td>Device list for VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages. Each storage requires:</td>
</tr>
<tr>
<td></td>
<td>• Array's IP: IP address of the storage</td>
</tr>
<tr>
<td></td>
<td>• User Name: User name for the storage</td>
</tr>
<tr>
<td></td>
<td>• Password: Password for the storage</td>
</tr>
<tr>
<td></td>
<td>• Folder Containing Export Utility JAR Files: The folder containing the Export utility .jar files</td>
</tr>
</tbody>
</table>

### SNM2Devices - WMS/SMS/AMS Storages

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNM2Devices - WMS/SMS/AMS Storages</td>
<td>Device list for WMS/SMS/AMS storages. Each storage requires:</td>
</tr>
<tr>
<td></td>
<td>• Array's IP: IP address of the storage</td>
</tr>
<tr>
<td></td>
<td>• Storage Navigator CLI Path: SNM2 CLI path</td>
</tr>
<tr>
<td></td>
<td>• Account Authentication Valid: Select to choose valid account authentication</td>
</tr>
<tr>
<td></td>
<td>• User Name: User name for the storage</td>
</tr>
<tr>
<td></td>
<td>• Password: Password for the storage</td>
</tr>
</tbody>
</table>

### Choose Tuning Manager for Performance

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Tuning Manager for Performance</td>
<td>Choose Tuning Manager for performance and override other performance options</td>
</tr>
<tr>
<td>Tuning Manager Host</td>
<td>IP address or fully-qualified domain name of tuning manager</td>
</tr>
<tr>
<td>Tuning Manager Port</td>
<td>Port used for Tuning Manager</td>
</tr>
<tr>
<td>Tuning Manager Username</td>
<td>User name for Tuning Manager</td>
</tr>
<tr>
<td>Tuning Manager Password</td>
<td>Password for Tuning Manager</td>
</tr>
</tbody>
</table>

**Note:** In HDS USP, USP V, and VSP, any disk can belong to more than one array group.

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiCommand Server Port</td>
<td>Port used for the HiCommand Device Manager</td>
</tr>
<tr>
<td>HTTPs Enabled</td>
<td>Select to enable HTTPs</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Choose 'Exclude' or 'Include' to specify a list</td>
<td>Specify whether to include or exclude the array list below when collecting data</td>
</tr>
<tr>
<td>Exclude or Include Devices</td>
<td>Comma-separated list of device ID's or array names to include or exclude</td>
</tr>
<tr>
<td>Query Host Manager</td>
<td>Select to query host manager</td>
</tr>
<tr>
<td>HTTP Timeout (sec)</td>
<td>HTTP connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Performance Polling Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>
### HDS NAS (HNAS) data source

The HDS NAS (HNAS) data source is an inventory and configuration data source to support discovery of HDS NAS clusters. Insight supports discovering NFS and CIFS shares, file systems (Insight Internal Volumes), and spans (Insight Storage Pools).

This data source is SSH based, so the acquisition unit that will host it needs to be able to initiate SSH sessions to TCP 22 on the HNAS itself, or the Systems Management Unit (SMU) that the cluster is connected to.

### Terminology

OnCommand Insight acquires the following inventory information from the HNAS data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Span</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>File System</td>
<td>Internal Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

### Requirements

The following are requirements to configure and use this data source:

- Device IP address
- Port 22, SSH protocol
- Username and password - privilege level: Supervisor

**Note:** This data collector is SSH based, so the AU that hosts it must be able to initiate SSH sessions to TCP 22 on the HNAS itself, or the Systems Management Unit (SMU) that the cluster is connected to.

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HNAS Host</td>
<td>IP address or fully-qualified domain name of HNAS Management Host</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for HNAS CLI</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for HNAS CLI</td>
</tr>
</tbody>
</table>
### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 30 minutes)</td>
</tr>
<tr>
<td>SSH Banner Wait Timeout (sec)</td>
<td>SSH banner wait timeout (default 15 seconds)</td>
</tr>
<tr>
<td>SSH Command Timeout (sec)</td>
<td>SSH command timeout (default 30 seconds)</td>
</tr>
</tbody>
</table>

### HP CommandView AE data source

The HP CommandView Advanced Edition (AE) and CommandView AE CLI/SMI (AE Lite) data sources support inventory and performance from a CommandView (also referred to as HiCommand) Device Manager server.

### Terminology

OnCommand Insight acquires the following inventory information from the HP CommandView AE and AE Lite data sources. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDEV</td>
<td>Disk</td>
</tr>
<tr>
<td>Journal Pool</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Storage Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Port Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Array Group, DP Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Logical Unit, LDEV</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

### Inventory Requirements

- IP address of the HiCommand Device Manager server
- Read-only user name and password for the CommandView AE software and peer privileges
- The CommandView AE Lite version of the device manager has only the CLI licensed
- Validate access:
  - Log in to the HiCommand Device Manager software using peer user name and password.
  - Verify access to the HiCommand Device Manager API: `telnet <HiCommand Device_Manager_server_ip> 2001`

### Performance Requirements

- HDS USP, USP V, and VSP performance
  - Performance Monitor must be licensed.
  - Monitoring switch must be enabled.
  - The Export Tool (`Export.exe`) must be copied to the OnCommand Insight Server.
The Export Tool version must match the microcode version of the target array.

- HDS AMS performance
  - Performance Monitor needs to be licensed.
  - The Storage Navigator Modular 2 (SNM2) CLI utility needs to be installed on the OnCommand Insight Server.
  - You must register all AMS, WMS, SMS storage arrays whose performance needs to be acquired by OnCommand Insight by using the following command:
    `auunitaddauto.exe -ip <IP address of Controller0> IP address of Controller1>`
  - You must ensure that all the arrays that you registered are listed in the output of this command: `auunitref.exe`.

## Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiCommand Server</td>
<td>IP address or fully-qualified domain name of the HiCommand Device Manager server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the HiCommand Device Manager server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the HiCommand Device Manager server.</td>
</tr>
<tr>
<td>Devices - USP, USP V, VSP/R600 Storages</td>
<td>Device list for VSP G1000 (R800), VSP (R700), HUS VM (HM700) and USP storages. Each storage requires:</td>
</tr>
<tr>
<td>• Array's IP: IP address of the storage</td>
<td></td>
</tr>
<tr>
<td>• User Name: User name for the storage</td>
<td></td>
</tr>
<tr>
<td>• Password: Password for the storage</td>
<td></td>
</tr>
<tr>
<td>• Folder Containing Export Utility JAR Files: The folder containing the Export utility .jar files</td>
<td></td>
</tr>
<tr>
<td>SNM2Devices - WMS/SMS/AMS Storages</td>
<td>Device list for WMS/SMS/AMS storages. Each storage requires:</td>
</tr>
<tr>
<td>• Array's IP: IP address of the storage</td>
<td></td>
</tr>
<tr>
<td>• Storage Navigator CLI Path: SNM2 CLI path</td>
<td></td>
</tr>
<tr>
<td>• Account Authentication Valid: Select to choose valid account authentication</td>
<td></td>
</tr>
<tr>
<td>• User Name: User name for the storage</td>
<td></td>
</tr>
<tr>
<td>• Password: Password for the storage</td>
<td></td>
</tr>
<tr>
<td>Choose Tuning Manager for Performance</td>
<td>Choose Tuning Manager for performance and override other performance options</td>
</tr>
<tr>
<td>Tuning Manager Host</td>
<td>IP address or fully-qualified domain name of tuning manager</td>
</tr>
<tr>
<td>Tuning Manager Port</td>
<td>Port used for Tuning Manager</td>
</tr>
<tr>
<td>Tuning Manager Username</td>
<td>User name for Tuning Manager</td>
</tr>
</tbody>
</table>
**Tuning Manager Password**  
Password for Tuning Manager

**Note:** In HDS USP, USP V, and VSP, any disk can belong to more than one array group.

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HiCommand Server Port</td>
<td>Port used for the HiCommand Device Manager</td>
</tr>
<tr>
<td>HTTPs Enabled</td>
<td>Select to enable HTTPs</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Choose 'Exclude' or 'Include' to</td>
<td>Specify whether to include or exclude the array list below when collecting</td>
</tr>
<tr>
<td>specify a list</td>
<td>data</td>
</tr>
<tr>
<td>Exclude or Include Devices</td>
<td>Comma-separated list of device ID's or array names to include or exclude</td>
</tr>
<tr>
<td>Query Host Manager</td>
<td>Select to query host manager</td>
</tr>
<tr>
<td>HTTP Timeout (sec)</td>
<td>HTTP connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Performance Polling Interval</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>(sec)</td>
<td></td>
</tr>
<tr>
<td>Export timeout in seconds</td>
<td>Export utility timeout (default 300 seconds)</td>
</tr>
</tbody>
</table>

### HP EVA Storage data source

For configuration, the EVA Storage (SSSU) data source requires the IP address of the Command View (CV) server and a *read-only* username and password to the CV software. The user must be defined in the CV software.

### Terminology

OnCommand Insight acquires the following inventory information from the HP EVA data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Disk Group</td>
<td>Disk Group (not modeled)</td>
</tr>
<tr>
<td>Storage Cell</td>
<td>Storage</td>
</tr>
<tr>
<td>Virtual Disk</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Virtual Disk</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

### Inventory Requirements

- IP address of the CV server
• Read-only username and password to the CV software. The user must be defined in the CV software.

• Third-party software installed on the OnCommand Insight Server/RAU: sssu.exe. The sssu.exe version should correspond to the CV version.

• Access validation: Run sssu.exe commands using username and password.

Performance Requirements

The HP StorageWorks Command View EVA software suite must be installed on the OnCommand Insight Server. Alternatively, you can install a Remote Acquisition Unit (RAU) on the EVA server:

1. Install HP StorageWorks Command View EVA Software Suite on the OnCommand Insight Server, or install a Remote Acquisition Unit on the Command View EVA server.

2. Locate the evaperf.exe command. For example, c:\Program Files\Hewlett-Packard \EVA Performance Monitor\

3. Using the IP of the Command View server, perform these steps:

   a. Run this command where 860 is the default port

   Evaperf.exe server <Command View Server IP> 860 <username>

   b. Enter the Command View server password at the password prompt. This should return a command line prompt and nothing else.

4. Verify the setup by running evaperf.exe ls. You should see a list of arrays or controllers managed by the Command View server. Each line shows a controller on an EVA array.

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CommandView Server</td>
<td>IP address or fully-qualified domain name of the EVA Storage Manager</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the Command View manager. The name must be defined in Command View.</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the Command View manager.</td>
</tr>
<tr>
<td>Performance User Name</td>
<td>For performance, the user name for the Command View manager. The name must be defined in Command View.</td>
</tr>
<tr>
<td>Performance Password</td>
<td>For performance, the password used for the Command View manager.</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>CLI Home</td>
<td>Full pathname to the CLI home directory where sssu.exe is located</td>
</tr>
<tr>
<td>Inventory Exclude Devices</td>
<td>Comma-separated list of device names to include</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Performance CLI Home | For Array Performance, full pathname to the CLI home directory where sssu.exe is located. To validate access, run sssu.exe
Command Timeout (sec) | evaperf command wait timeout (default 600 seconds)
Performance Exclude Devices | Comma-separated list of device names to exclude from collecting performance data

**Huawei OceanStor data source**

OnCommand Insight uses the Huawei OceanStor (REST/HTTPS) data source to discover inventory for Huawei OceanStor storage.

**Terminology**

OnCommand Insight acquires the following inventory and performance information from the Huawei OceanStor. For each asset type acquired by OnCommand Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>OnCommand Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>File System</td>
<td>Internal Volume</td>
</tr>
<tr>
<td>Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>FC Port (Mapped)</td>
<td>Volume Map</td>
</tr>
<tr>
<td>Host FC Initiator (Mapped)</td>
<td>Volume Mask</td>
</tr>
<tr>
<td>NFS/CIFS Share</td>
<td>Share</td>
</tr>
<tr>
<td>Share</td>
<td>iSCSI Target Node</td>
</tr>
<tr>
<td>iSCSI Link Initiator</td>
<td>iSCSI Initiator Node</td>
</tr>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>LUN</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Requirements**

The following are requirements to configure and use this data collector:

- Device IP
- Credentials to access OceanStor device manager
- Port 8088 must be available

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OceanStor Host IP Address</td>
<td>IP address or fully-qualified domain name of the OceanStor Device Manager</td>
</tr>
<tr>
<td>User Name</td>
<td>Name used to log into the OceanStor Device Manager</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to log into the OceanStor Device Manager</td>
</tr>
</tbody>
</table>
Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>TCP Port used to connect to OceanStor Device Manager (default 8088)</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Connection Timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
</tbody>
</table>

IBM DS data source

The IBM DS (CLI) data source supports DS6xxx and DS8xxx devices only. DS3xxx, DS4xxx, and DS5xxx devices are supported by the NetApp E-Series data source. You should refer to the Insight data source support matrix for supported models and firmware versions.

Terminology

OnCommand Insight acquires the following inventory information from the IBM DS data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Drive Module</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage Image</td>
<td>Storage</td>
</tr>
<tr>
<td>Extent Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Fixed Block Volume</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

Requirements

- IP address of each DS array
- Storage Display Name is optional and cosmetic only
- Read-only username and password on each DS array
- Third-party software installed on the Insight server: IBM dscli
- Access validation: Run `dscli` commands using the username and password

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS storage</td>
<td>IP address or fully-qualified domain name of the DS Storage Host</td>
</tr>
<tr>
<td>User Name</td>
<td>Name used for the DS CLI</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the DS CLI</td>
</tr>
<tr>
<td>Executable dscli.exe Path</td>
<td>Full path to the <code>dscli.exe</code> utility.</td>
</tr>
</tbody>
</table>
Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>Storage Display Name</td>
<td>Name of the IBM DS storage array</td>
</tr>
<tr>
<td>Inventory Exclude Devices</td>
<td>Comma-separated list of device serial numbers to exclude from inventory collection</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>Performance Filter Type</td>
<td>Include: Data collected only from devices on list. Exclude: No data from these devices is collected</td>
</tr>
<tr>
<td>Performance Filter Device List</td>
<td>Comma-separated list of device IDs to include or exclude from performance collection</td>
</tr>
</tbody>
</table>

IBM PowerVM data source

The IBM PowerVM (SSH) data source collects information about virtual partitions running on IBM POWER hardware instances managed by a hardware management console (HMC). For configuration, this data source requires the user name to log in to the HMC through SSH, and the view-level permission on HMC configurations.

Terminology

OnCommand Insight acquires the following inventory information from the IBM PowerVM data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>hdisk</td>
<td>Virtual Disk</td>
</tr>
<tr>
<td>Managed System</td>
<td>Host</td>
</tr>
<tr>
<td>LPAR, VIO Server</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Volume Group</td>
<td>Data Store</td>
</tr>
<tr>
<td>Physical Volume</td>
<td>LUN</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

- User name and password that provide access to HMC through SSH
- View permission on all management systems and logical partition security domains

The user must also have View permission on HMC configurations and the ability to collect VPD information for the HMC console security grouping. The user must also be allowed Virtual IO Server Command access under the Logical Partition security grouping. It is a best practice to start from a role of an operator and then remove all roles. Read-only users on the HMC do not have privileges to run proxied commands on AIX hosts.
### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Management Console (HMC) Address</td>
<td>IP address or fully-qualified domain name of the PowerVM Hardware Management Console</td>
</tr>
<tr>
<td>HMC User</td>
<td>User name for the Hardware Management Console</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the Hardware Management Console</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Port used for SSH to the PowerVM</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 600 seconds)</td>
</tr>
<tr>
<td>Number of Retries</td>
<td>Number of inventory retry attempts</td>
</tr>
<tr>
<td>Exclude Devices</td>
<td>Comma-separated list of device IDs or display names to exclude</td>
</tr>
</tbody>
</table>

### IBM SVC data source

The IBM SVC data source collects inventory and performance data using SSH, supporting a variety of devices that run the SVC operating system. The list of supported devices includes models such as the SVC, the v7000, the v5000, and the v3700. Refer to the Insight data source support matrix for supported models and firmware versions.

### Terminology

OnCommand Insight acquires the following inventory information from the IBM SVC data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive</td>
<td>Disk</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Mdisk Group</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Vdisk</td>
<td>Volume</td>
</tr>
<tr>
<td>Mdisk</td>
<td>Backend LUN</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

### Inventory Requirements

- IP address of each SVC cluster
- Port 22 available
- Public and private key pair that you either generate with Insight or reuse a keypair already in use on your SVC
If you are reusing an existing keypair, you must convert them from Putty format to OpenSSH format.

- Public key installed on the SVC cluster
- Private key needs to be identified in the data source
- Access validation: Open ssh session to the SVC cluster using the private key

**Note:** No third-party software needs to be installed.

### Performance Requirements

- SVC Console, which is mandatory for any SVC cluster and required for the SVC discovery foundation package.
- Administrative access level required only for copying performance data files from cluster nodes to the config node.

  **Note:** Because this access level is not required for the SVC foundation discovery package, the SVC foundation user might not work successfully.

- Port 22 required
- A private and public SSH key must be generated for this user, and the private key stored so that it is accessible from the Acquisition Unit. If the SVC foundation user has the proper permissions, then the same user and key works. The same SSH key can be used for inventory and performance data.
- Enable data collection by connecting to the SVC cluster by SSH and running: `svctask startstats -interval 1`

  **Note:** Alternatively, enable data collection using the SVC management user interface.

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster/s IP</td>
<td>IP address of fully-qualified domain name for the SVC storage</td>
</tr>
<tr>
<td>Choose 'Password' or 'OpenSSH Key File' to specify credential type</td>
<td>The credential type used to connect to the device via SSH</td>
</tr>
<tr>
<td>Inventory User Name</td>
<td>User name for the SVC CLI</td>
</tr>
<tr>
<td>Inventory Password</td>
<td>Password for the SVC CLI</td>
</tr>
<tr>
<td>Full Path to Inventory Private Key</td>
<td>Full path to the Inventory private key file</td>
</tr>
<tr>
<td>Performance User Name</td>
<td>User name for the SVC CLI for performance collection</td>
</tr>
<tr>
<td>Performance Password</td>
<td>Password for the SVC CLI for performance collection</td>
</tr>
<tr>
<td>Full Path to Performance Private Key</td>
<td>Full path to the Performance private key file</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
</tbody>
</table>
IBM Tivoli Monitoring data source

This data source is used solely for File System Utilization. It communicates directly with the Tivoli Monitoring Database, also known as the Tivoli Monitoring Data Warehouse. Oracle and DB2 databases are supported.

Oracle error message

If the specified SID results in the error message containing "ORA-12154" on attempting to connect, double-check your Oracle DB network service configuration. If the access configuration specifies a fully qualified hostname (for example, "NAMES.DEFAULT_DOMAIN"), try inserting the fully qualified service name in the SID field. A simple example would be that the connection to SID testdb is failing and your Oracle configuration specifies a domain of company.com. The following string can be used instead of the base SID to try to connect: testdb.company.com.

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Monitoring Database IP</td>
<td>IP address or fully-qualified domain name of the Tivoli Monitoring server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the Tivoli Monitoring server</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Tivoli Monitoring server</td>
</tr>
</tbody>
</table>

Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Monitoring Database Port</td>
<td>Port used for Tivoli monitoring database</td>
</tr>
<tr>
<td>Oracle SID or DB2 Database Name</td>
<td>Oracle listener service ID or DB2 database name</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Database Driver to Use</td>
<td>Choose Database Driver to use</td>
</tr>
<tr>
<td>Protocol Used to Connect to the Database</td>
<td>Protocol Used to Connect to the Database</td>
</tr>
<tr>
<td>Database Schema</td>
<td>Enter Database Schema</td>
</tr>
</tbody>
</table>
IBM TotalStorage DS4000 data source

This data source collects inventory and performance information. There are two possible configurations (firmware 6.x and 7.x+), and they both have the same values. The API collects the volume data statistics.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comma Separated List of Array SANtricity Controller IPs</td>
<td>IP addresses or fully-qualified domain names of controllers, separated by commas</td>
</tr>
</tbody>
</table>

**Requirements**

- IP address of each DS5 or FAStT array
- Access validation: Ping the IP address of both controllers on each array.

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 30 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (up to 3600 seconds)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

IBM XIV data source

IBM XIV (CLI) data source inventory is performed by using the XIV command-line interface. XIV performance is accomplished by making SMI-S calls to the XIV array, which runs a SMI-S provider on port 5989.

**Terminology**

OnCommand Insight acquires the following inventory information from the IBM XIV data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Storage System</td>
<td>Storage</td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- Port requirement: TCP port 5989
- IP address of the XIV management interface
- Read-only user name and password
- The XIV CLI must be installed on the Insight server or RAU
- Access validation: Log in to the XIV user interface from the Insight server using the user name and password.

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address or fully-qualified domain name for the XIV storage</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the XIV storage</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the XIV storage</td>
</tr>
<tr>
<td>Full path to XIV CLI directory</td>
<td>Full path to the XIV CLI directory</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 40 minutes)</td>
</tr>
<tr>
<td>CLI Process Wait Timeout (ms)</td>
<td>CLI process timeout (default 7200000 ms)</td>
</tr>
<tr>
<td>SMI-S Host IP</td>
<td>IP address of the SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S Port</td>
<td>Port used by SMI-S Provider Host</td>
</tr>
<tr>
<td>SMI-S Protocol</td>
<td>Protocol used to connect to the SMI-S provider</td>
</tr>
<tr>
<td>SMI-S Namespace</td>
<td>SMI-S namespace</td>
</tr>
<tr>
<td>Username</td>
<td>User name for the SMI-S Provider Host</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SMI-S Provider Host</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
<tr>
<td>Number of SMI-S Connection Retries</td>
<td>Number of SMI-S connection retry attempts</td>
</tr>
</tbody>
</table>

### Infinidat InfiniBox data source

The Infinidat InfiniBox (HTTP) data source is used to collect information from the Infinidat InfiniBox storage. You must have access to the InfiniBox Management Node.

### Terminology

OnCommand Insight acquires the following inventory information from the InfiniBox data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive</td>
<td>Disk</td>
</tr>
<tr>
<td>InfiniBox</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Pool</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>Vendor/Model Term</td>
<td>Insight Term</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>FC Port</td>
<td>Port</td>
</tr>
<tr>
<td>Filesystem</td>
<td>Internal Volume</td>
</tr>
<tr>
<td>Filesystem</td>
<td>FileShare</td>
</tr>
<tr>
<td>Filesystem Exports</td>
<td>Share</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfiniBox Host</td>
<td>IP address or fully-qualified domain name of the InfiniBox Management Node</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for InfiniBox Management Node</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the InfiniBox Management Node</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port</td>
<td>TCP Port used to connect to InfiniBox Server (default 443 )</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Connection Timeout</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
</tbody>
</table>

**Microsoft Azure compute data source**

OnCommand Insights uses the Azure compute data collector to acquire inventory and performance data from Azure compute instances.

**Requirements**

You need the following information to configure this data collector:

- Port requirement: 443 HTTPS
- Azure Management Rest IP (management.azure.com)
- Azure service principal client ID (user account)
- Azure service principal authentication key (user password)
- Azure service principal authentication key (user password)

You need to set up an Azure account for Cloud Insights discovery. Once the account is properly configured and you register the application in Azure, you will have the credentials required to discover the Azure instance with Cloud Insights. The following link describes how to set up the account for discovery: [https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal](https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal)

**Configuration**

Enter data into the data source fields according to the table below:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Service Principal Client ID</td>
<td>Sign-in ID to Azure</td>
</tr>
<tr>
<td>Azure tenant ID</td>
<td>Microsoft tenant ID</td>
</tr>
<tr>
<td>Azure Service Principal Authentication Key</td>
<td>Login authentication key</td>
</tr>
<tr>
<td>I understand Microsoft bills me for API requests</td>
<td>Check this to verify your understanding that Microsoft bills you for API requests made by Insight polling.</td>
</tr>
</tbody>
</table>

**Advanced Configuration**

Enter data into the data source fields according to the table below:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>The default is 60</td>
</tr>
<tr>
<td>HTTP connection and socket timeout (sec)</td>
<td>The default is 300</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>The default is 300</td>
</tr>
</tbody>
</table>

**Microsoft Hyper-V data source**

For configuration, the Microsoft Hyper-V (WMI) data source requires the IP address or the resolvable DNS name for the physical host (hypervisor).

**Terminology**

OnCommand Insight acquires the following inventory information from the Hyper-V data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual hard Disk</td>
<td>Virtual Disk</td>
</tr>
<tr>
<td>Host</td>
<td>Host</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Cluster Shared Volumes (CSV), Partition Volume</td>
<td>Data Store</td>
</tr>
<tr>
<td>Internet SCSI Device, Multi Path SCSI LUN</td>
<td>LUN</td>
</tr>
<tr>
<td>Fiber Channel Port</td>
<td>Port</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- Administrative-level user account
- Windows Management Instrumentation (WMI) command, which is the default that is installed by Windows

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Host IP Address</td>
<td>The IP address or fully-qualified domain name for the physical host (hypervisor)</td>
</tr>
<tr>
<td>User Name</td>
<td>Administrator user name doe the hypervisor</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the hypervisor</td>
</tr>
<tr>
<td>NT Domain</td>
<td>The DNS name used by the nodes in the cluster</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection Timeout (ms)</td>
<td>Connection timeout (default 60000 ms)</td>
</tr>
</tbody>
</table>

### NetApp Clustered Data ONTAP data source

This data source should be used for storage systems using Clustered Data ONTAP, and requires an administrator account used for read-only API calls.

### Terminology

OnCommand Insight acquires the following inventory information from the Clustered Data ONTAP data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Raid Group</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Aggregate</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>LUN</td>
<td>Volume</td>
</tr>
<tr>
<td>Volume</td>
<td>Internal Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

### Requirements

- Administrator account used for read-only API calls
- Target IP is the cluster management LIF
- Username (with read-only role name to ontapi application to the default Vserver) and password to log into NetApp cluster
• Port requirements: 80 or 433
• License requirements: FCP license and mapped/masked volumes required for discovery

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp Management IP</td>
<td>IP address or fully-qualified domain name of the NetApp cluster</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the NetApp cluster</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the NetApp cluster</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

### NetApp Clustered Data ONTAP for Unified Manager data source

This data source collects ONTAP 8.1.x data from the Unified Manager (UM) 6.0+ database. Using this data source, Insight discovers all clusters configured and populated in UM. For efficiency, Insight does not call ZAPIs on the cluster itself. Performance is not supported in this data source.

### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Manager IP</td>
<td>IP address or fully-qualified domain name of the Unified Manager</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the Unified Manager</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Unified Manager</td>
</tr>
<tr>
<td>Port</td>
<td>Port used for communication with the Unified Manager (default 3306)</td>
</tr>
</tbody>
</table>

### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 15 minutes)</td>
</tr>
<tr>
<td>Exclude Clusters</td>
<td>Comma-separated list of cluster IPs to exclude</td>
</tr>
</tbody>
</table>

### NetApp Data ONTAP operating in 7-Mode data source

For storage systems using Data ONTAP software operating in 7-Mode, you should use the ONTAPI data source, which uses the CLI to obtain capacity numbers.

### Terminology

OnCommand Insight acquires the following inventory information from the NetApp Data ONTAP 7-Mode data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:
<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Raid Group</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Filer</td>
<td>Storage</td>
</tr>
<tr>
<td>Filer</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Aggregate</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>LUN</td>
<td>Volume</td>
</tr>
<tr>
<td>Volume</td>
<td>Internal Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- IP address of the FAS storage controller and partner
- Port 443
- User name and password for the controller and the partner
- FCP license and mapped or masked volumes required for OnCommand Insight discovery
- CIFS or NFS licenses and CIFS shares or NFS exports required for OnCommand Insight NAS discovery

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address of Filer</td>
<td>IP address or fully-qualified domain name for the NetApp Filer</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the NetApp Filer</td>
</tr>
<tr>
<td>Password</td>
<td>password for the NetApp Filer</td>
</tr>
<tr>
<td>Address of HA Partner Filer in Cluster</td>
<td>IP address or fully-qualified domain name for the HA Partner Filer</td>
</tr>
<tr>
<td>User Name of HA Partner Filer in Cluster</td>
<td>User name for the NetApp HA Partner Filer</td>
</tr>
<tr>
<td>Password of HA Partner Filer in Cluster</td>
<td>password for the NetApp HA Partner Filer</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Choose connection type</td>
</tr>
<tr>
<td>Connection Port</td>
<td>Port used for NetApp API</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>
Storage systems connection

As an alternative to using the default administrative user for this data source, you can configure a user with administrative rights directly on the NetApp storage systems so that this data source can acquire data from NetApp storage systems.

Connecting to NetApp storage systems requires that the user, who is specified when acquiring the main pfiler (on which the storage system exists), meet the following conditions:

- The user must be on vfiler0 (root filer/pfiler).
  Storage systems are acquired when acquiring the main pfiler.
- The following commands define the user role capabilities:
  - "api-*": Use this to allow OnCommand Insight to execute all NetApp storage API commands. This command is required to use the ZAPI.
  - "login-http-admin": Use this to allow OnCommand Insight to connect to the NetApp storage via HTTP. This command is required to use the ZAPI.
  - "security-api-vfiler": Use this to allow OnCommand Insight to execute NetApp storage API commands to retrieve vFiler unit information.
  - "cli-options": For "options" command and used for partner IP and enabled licenses.
  - "cli-lun": Access these command for managing LUNs. Displays the status (LUN path, size, online/offline state, and shared state) of the given LUN or class of LUNs.
  - "cli-df": For "df -s", "df -r", "df -A -r" commands and used to display free space.
  - "cli-ifconfig": For "ifconfig -a" command and used for getting filer IP address.
  - "cli-rcf": For "rcf /etc/netgroup" command and used for getting netgroups.
  - "cli-date": For "date" command and used to get full date for getting Snapshot copies.
  - "cli-snap": For "snap list" command and used for getting Snapshot copies.

If cli-date or cli-snap permissions are not provided, acquisition can finish, but Snapshot copies are not reported.

To acquire a 7-Mode data source successfully and generate no warnings on the storage system, you should use one of the following command strings to define your user roles. The second string listed here is a streamlined version of the first:

```
login-http-admin,api-* ,security-api-vfiler,cli-rcf,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-* ,security-api-vfiler,cli-

NetApp E-Series data source

The NetApp E-Series data source collects inventory and performance information. There are two possible configurations (firmware 6.x and firmware 7.x+), and they both have the same values.

Terminology

OnCommand Insight acquires the following inventory information from the NetApp E-Series data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:
<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive</td>
<td>Disk</td>
</tr>
<tr>
<td>Volume Group</td>
<td>Disk Group</td>
</tr>
<tr>
<td>Storage Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Volume Group</td>
<td>Storage Pool</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- The IP address of each controller on the array
- Access validation by pinging the IP address of both controllers on the array

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comma-separated list of Array SANtricity Controller IPs</td>
<td>IP addresses and/or fully-qualified domain names for the array controllers</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 30 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (up to 3600 seconds)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**NetApp Host and VM File Systems data source**

You can use the NetApp Host and VM File Systems data source to retrieve file system details and storage resource mappings for all Microsoft Windows host and VM (virtual machine) file systems and for all supported Linux VMs (those that are virtually mapped only) existing in the Insight server that are annotated with the configured Compute Resource Group (CRG).

**General Requirements**

- This feature must be purchased separately.
  You can contact your Insight representative for assistance.

- You should check the Insight support matrix to verify that your host or virtual machine operating system is supported.
  To verify that links from file systems to storage resources are created, check that the relevant storage or virtualization vendor type and version report the volume or virtual disk identification data required.

**Microsoft Windows Requirements**

- This data source uses Window Management Instrumentation (WMI) data structures to retrieve data.
This service must be operational and available remotely. In particular, port 135 must be accessible and must be opened if behind a firewall.

- Windows domain users must have the appropriate permissions to access WMI structures.
- Administrator permissions are required.
- Dynamic TCP ports assigned 1024-65535 for Windows 2003 and older
- Ports 49152–65535 for Windows 2008

**Note:** As a general rule, when trying to use a firewall between Insight, an AU, and this data source, you should consult with your Microsoft team to identify the ports they believe will be required.

**Linux Requirements**

- This data source uses a Secure Shell (SSH) connection to execute commands on Linux VMs. The SSH service must be operational and available remotely. In particular, port 22 must be accessible and must be opened if behind a firewall.
- SSH users must have sudo permissions to execute read-only commands on Linux VMs. You must use the same password to log in to SSH and to answer any sudo password challenge.

**Usage Recommendations**

- You should annotate a group of hosts and virtual machines that have common operating system credentials using the same Compute Resource Group annotation. Each group has an instance of this data source discovering file system details from those hosts and virtual machines.
- If you have an instance of this data source for which the success rate is low (for example, OnCommand Insight is discovering file system details for only 50 of 1000 hosts and virtual machines in a group), you should move the hosts and virtual machines for which discovery is successful into a separate Compute Resource Group.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Operating system user with appropriate rights to retrieve file system data</td>
</tr>
<tr>
<td></td>
<td>For Windows operating system users, this must include the domain prefix.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the operating system user</td>
</tr>
<tr>
<td>Compute Resource Group</td>
<td>Annotation value used to flag host and virtual machines for the data source discovers file systems.</td>
</tr>
<tr>
<td></td>
<td>A blank value indicates that the data source discovers file systems for all hosts and virtual machines not currently annotated with any Compute Resource Group.</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory poll interval (min)</td>
<td>Interval between inventory polls (default 360 minutes)</td>
</tr>
</tbody>
</table>
NetApp SolidFire data source

The NetApp SolidFire data source supports both iSCSI and Fibre Channel SolidFire configurations, for both inventory and performance collection.

The SolidFire data source utilizes the SolidFire REST API. The acquisition unit where the data source resides needs to be able to initiate HTTPS connections to TCP port 443 on the SolidFire cluster management IP address. The data source needs credentials capable of making REST API queries on the SolidFire cluster.

Terminology

OnCommand Insight acquires the following inventory information from the NetApp SolidFire data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive</td>
<td>Disk</td>
</tr>
<tr>
<td>Cluster</td>
<td>Storage</td>
</tr>
<tr>
<td>Node</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>Fibre Channel Port</td>
<td>Port</td>
</tr>
<tr>
<td>Volume Access Group, LUN Assignment</td>
<td>Volume Map</td>
</tr>
<tr>
<td>iSCSI Session</td>
<td>Volume Mask</td>
</tr>
</tbody>
</table>

Note: These are common terminology mappings only and might not represent every case for this data source.

Requirements

The following are requirements for configuring this data source:

- Management Virtual IP Address
- Read-only username and credentials
- Port 443

Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Virtual IP Address (MVIP)</td>
<td>Management Virtual IP address of the SolidFire Cluster</td>
</tr>
<tr>
<td>User Name</td>
<td>Name used to log into the SolidFire cluster</td>
</tr>
<tr>
<td>Password</td>
<td>Password used to log into the SolidFire cluster</td>
</tr>
</tbody>
</table>
Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>TCP Port</td>
<td>TCP Port used to connect to SolidFire Server (default 443)</td>
</tr>
<tr>
<td>Connection Timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

OpenStack data source

The OpenStack (REST API / KVM) data source collects information about OpenStack hardware instances. This data source collects inventory data for all OpenStack instances, and optionally, VM performance data.

Requirements

The following are requirements for configuring the OpenStack data source.

• IP address of the OpenStack controller

• OpenStack admin role credentials and sudo access to the Linux KVM hypervisor.

  Note: If you are not using the admin account or admin equivalent privileges, you need to use trial and error to identify the default policies to relax for your data source userid.

• For performance collection the OpenStack Ceilometer module must be installed and configured. Configuring the Ceilometer is done by editing the `nova.conf` file for each hypervisor and then restart the Nova Compute service on each hypervisor. The option name changes for different releases of OpenStack:

  • Icehouse
  • Juno
  • Kilo
  • Liberty
  • Mitaka
  • Newton
  • Ocata

• For CPU stats, "compute_monitors=ComputeDriverCPUMonitor" needs to be turned on in `/etc/nova/nova.conf` on compute nodes.

• Port requirements:
  • 5000 for http and 13000 for https, for the Keystone service
  • 22 for KVM SSH
  • 8774 for Nova Compute Service
  • 8776 for Cinder Block Service
  • 8777 for Ceilometer Performance Service
  • 9292 for Glance Image Service
Note: The port binds to the specific service, and the service may run on the controller or another host in larger environments.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenStack Controller IP Address</td>
<td>IP address or fully-qualified domain name of the OpenStack Controller</td>
</tr>
<tr>
<td>OpenStack Administrator</td>
<td>User name for an OpenStack Admin</td>
</tr>
<tr>
<td>OpenStack Password</td>
<td>Password used for the OpenStack Admin</td>
</tr>
<tr>
<td>OpenStack Administrator Tenant</td>
<td>OpenStack Administrator Tenant</td>
</tr>
<tr>
<td>KVM Sudo User</td>
<td>KVM Sudo User name</td>
</tr>
<tr>
<td>Choose 'Password' or 'OpenSSH Key File' to specify credential type</td>
<td>The credential type used to connect to the device via SSH</td>
</tr>
<tr>
<td>Full Path to Inventory Private Key</td>
<td>Full Path to Inventory Private Key</td>
</tr>
<tr>
<td>KVM Sudo Password</td>
<td>KVM Sudo Password</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable hypervisor inventory discovery through SSH</td>
<td>Check this to enable hypervisor inventory discovery through SSH</td>
</tr>
<tr>
<td>OpenStack Admin URL port</td>
<td>OpenStack Admin URL port</td>
</tr>
<tr>
<td>Use HTTPS</td>
<td>Check to use secure HTTP</td>
</tr>
<tr>
<td>HTTP Connection Timeout (sec)</td>
<td>Timeout for HTTP connection (default 300 seconds)</td>
</tr>
<tr>
<td>SSH Port</td>
<td>Port used for SSH</td>
</tr>
<tr>
<td>SSH Process Wait Timeout (sec)</td>
<td>SSH process timeout (default 30 seconds)</td>
</tr>
<tr>
<td>SSH Process Retries</td>
<td>Number of inventory retry attempts</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
</tbody>
</table>

**Pure Storage FlashArray data source**

The Pure Storage FlashArray (HTTP) data source is used to collect information from the Pure Storage Flash Array. Insight supports both inventory and performance collection.

**Terminology**

OnCommand Insight acquires the following inventory information from the Pure Storage FlashArray data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive (SSD)</td>
<td>Disk</td>
</tr>
<tr>
<td>Vendor/Model Term</td>
<td>Insight Term</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Array</td>
<td>Storage</td>
</tr>
<tr>
<td>Controller</td>
<td>Storage Node</td>
</tr>
<tr>
<td>Volume</td>
<td>Volume</td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td>LUN Map (Host, Host Group, Target Port)</td>
<td>Volume Map, Volume Mask</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlashArray Host</td>
<td>IIP address or fully-qualified domain name of FlashArray Management Server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the FlashArray Management Server</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the FlashArray Management Server</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Type</td>
<td>Management Server</td>
</tr>
<tr>
<td>TCP Port</td>
<td>TCP Port used to connect to FlashArray Server (default 443)</td>
</tr>
<tr>
<td>Connection Timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 60 minutes)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**QLLogic FC Switch data source**

For configuration, the QLogic FC Switch (SNMP) data source requires the network address for the FC Switch device, specified as an IP address, and an SNMP read-only community string used to access the device.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSurfer Switch</td>
<td>IP address or fully-qualified domain name for the SANSurfer switch</td>
</tr>
<tr>
<td>SNMP version</td>
<td>SNMP version</td>
</tr>
<tr>
<td>SNMP community</td>
<td>SNMP Community String</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the SANSurfer switch</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the SANSurfer switch</td>
</tr>
</tbody>
</table>
### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 15 minutes)</td>
</tr>
<tr>
<td>SNMP Auth Protocol</td>
<td>SNMP authentication protocol (SNMPv3 only)</td>
</tr>
<tr>
<td>SNMP Retries</td>
<td>Number of SNMP retry attempts</td>
</tr>
<tr>
<td>SNMP Timeout (ms)</td>
<td>SNMP timeout (default 5000 ms)</td>
</tr>
<tr>
<td>Enable Trapping</td>
<td>Select to enable trapping</td>
</tr>
<tr>
<td>Minimum Time Between Traps (sec)</td>
<td>Minimum time between acquisition attempts triggered by traps (default 10 seconds)</td>
</tr>
<tr>
<td>Fabric Name</td>
<td>Fabric name to be reported by the data source. Leave blank to report the fabric name as WWN.</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

### Red Hat (RHEV) data source

The Red Hat Enterprise Virtualization (REST) data source collects information about RHEV instances via HTTPS.

#### Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEV Server IP Address</td>
<td>IP address or fully-qualified domain name of the RHEV server</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the RHEV server</td>
</tr>
<tr>
<td>Password</td>
<td>Password used for the RHEV server</td>
</tr>
</tbody>
</table>

#### Advanced configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Communication Port</td>
<td>Port used for HTTPS communication to RHEV</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
</tbody>
</table>

### Violin Flash Memory Array data source

The Violin 6000-Series Flash Memory Array (HTTP) data source collects network information for analysis and validation from Violin 6000-series flash memory arrays.

#### Terminology

OnCommand Insight acquires the following inventory information from the Violin 6000-Series Flash Memory Array data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violin Intelligent Memory Module (VIMM)</td>
<td>Disk</td>
</tr>
<tr>
<td>Vendor/Model Term</td>
<td>Insight Term</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Container</td>
<td>Storage</td>
</tr>
<tr>
<td>Memory Gateway</td>
<td>Storage Node</td>
</tr>
<tr>
<td>LUN</td>
<td>Volume</td>
</tr>
<tr>
<td>Initiator, Initiator Group, Target</td>
<td>Volume Map, Volume Mask</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**

- You need a read-only user name and password to the storage.
- Validate access with a web browser using the storage IP address.

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or FQDN of Violin Memory Array Master Gateway</td>
<td>IP address or fully-qualified domain name of the Violin Memory Array Master Gateway</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the Violin Memory Array Master Gateway</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Violin Memory Array Master Gateway</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication Port</td>
<td>Port used for communication with Violin array</td>
</tr>
<tr>
<td>HTTPS Enabled</td>
<td>Select to use HTTPS</td>
</tr>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection timeout (sec)</td>
<td>Connection timeout (default 60 seconds)</td>
</tr>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

**VMware vSphere data source**

The VMware vSphere (Web Services) data source collects ESX Host information and requires read-only privileges on all objects within the Virtual Center.

**Terminology**

OnCommand Insight acquires the following inventory information from the VMware vSphere data source. For each asset type acquired by Insight, the most common terminology used for this asset is shown. When viewing or troubleshooting this data source, keep the following terminology in mind:

<table>
<thead>
<tr>
<th>Vendor/Model Term</th>
<th>Insight Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Disk</td>
<td>Disk</td>
</tr>
<tr>
<td>Vendor/Model Term</td>
<td>Insight Term</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Host</td>
<td>Host</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>Data Store</td>
<td>Data Store</td>
</tr>
<tr>
<td>LUN</td>
<td>LUN</td>
</tr>
<tr>
<td>Fiber Channel Port</td>
<td>Port</td>
</tr>
</tbody>
</table>

**Note:** These are common terminology mappings only and might not represent every case for this data source.

**Requirements**
- Read-only privileges on all objects within the Virtual Center.
- SDK access on the Virtual Center server
- Validate access by logging in to Virtual Center Client using your user name and password.
- Verify that the SDK is enabled by entering
telnet <vc_ip> 443.

- This data source uses the VMware Infrastructure (VI) SDK 2.5.0

**Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Center Address</td>
<td>Network address for the Virtual Center or vSphere server, specified as an IP (nnn.nnn.nnn.nnn format) address or as a host name that can be resolved through DNS.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name for the VMware server.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the VMware server.</td>
</tr>
</tbody>
</table>

**Advanced configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Poll Interval (min)</td>
<td>Interval between inventory polls (default 20 minutes)</td>
</tr>
<tr>
<td>Connection Timeout (ms)</td>
<td>Connection timeout (default 60000 ms)</td>
</tr>
<tr>
<td>Filter VMs by</td>
<td>Choose how to filter VMs</td>
</tr>
<tr>
<td>Choose 'Exclude' or 'Include' to specify a list</td>
<td>Specify whether to include or exclude the VM list below when collecting data</td>
</tr>
<tr>
<td>List of VMs to filter (Comma Separated, or Semicolon Separated If Comma Is Used in the Value)</td>
<td>Comma-separated or semicolon-separated list of VMs to include or exclude from polling</td>
</tr>
<tr>
<td>Number of Retries for Requests to vCenter</td>
<td>Number of vCenter Request retry attempts</td>
</tr>
<tr>
<td>Communication Port</td>
<td>Port used for Vmware server</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Poll Interval (sec)</td>
<td>Interval between performance polls (default 300 seconds)</td>
</tr>
</tbody>
</table>

### Changing data source credentials

If multiple data sources of the same type are sharing a username and password, you can change the password for all devices in the group at the same time.

**Steps**

1. On the Insight toolbar, click Admin.
   
   The Data sources list opens.

2. Click the Actions button and select the Change credentials option.

3. In the Credentials Management dialog box, select one of the data source groups from the list.
   
   The Edit icon, a pen on a sheet of paper, becomes active to the right.

4. Click Edit.

5. Enter the new password and confirm it.

### Changes causing data collection problems

If you are experiencing data collection problems in OnCommand Insight, changes in your environment are a likely cause. As a general maintenance rule, you should accommodate any changes in your environment in Insight as well.

You can use this checklist to identify changes to your network that might be causing problems:
• Have you changed any passwords? Were those passwords changed in Insight?

• Did you remove a device from your network? You must also remove the device from OnCommand Insight to prevent it from being rediscovered and reintroduced.

• Did you upgrade infrastructure software (such as HP CommandView EVA or EMC Solutions Enabler)?
  Ensure that the appropriate versions of the client tools are installed on the acquisition unit. If data source failures persist, you need to contact technical support to request assistance and possibly a data source patch.

• Are all of your OnCommand Insight acquisition units using the same OnCommand Insight version? If the Remote Acquisition Units and local acquisition unit are running different OnCommand Insight versions, install the same version on all units to correct the data collection problem.
  If you need to install a new version of OnCommand Insight on all of the acquisition units, go to the support site and download the correct version.

• Have you changed any domain names or added a new domain? You must update your Device Resolution (formerly Auto Resolution) methods.

Examining one data source in detail

If you see that a data source has failed or slowed, you might want to examine a detailed summary of information for that data source to determine the cause of the problem. Data sources with conditions requiring your attention are marked with a solid red circle.

Steps

1. On the Insight toolbar, click Admin.
   The Data sources list opens. Any listed data sources with potential problems are marked with a solid red circle. The most serious problems are at the top of the list.

2. Select the data source that is causing concern.

3. Click the data source name link.

4. On the data source summary page, check the information in any of these sections:
   • Event timeline
     Lists events tied to the current status shown in the Data sources list. Events in this summary are displayed per device. Errors are shown in red. You can position your mouse pointer on timeline items to display additional information.
   • Devices reported by this data source
     Lists the types of devices, their IP addresses, and links to more detailed information for each device.
   • Changes reported by this data source (last 3 weeks)
     Lists any devices that were added or removed or had a change to the configuration.

5. After examining the data source information, you might want to perform one of these operations using the buttons at the top of the page:
   • Edit the description of the data source to correct the problem.
   • Poll again forces polling to reveal if the problem was persistent or intermittent.
   • Postpone data source polling for 3, 7, or 30 days to give you time to research the problem and stop the warning messages.
• **Install a patch** on the data source to correct the problem.

• Prepare an **Error report** for technical support.

• **Delete** the data source from your Insight monitoring environment.

**Researching a failed data source**

If a data source has the "Inventory failed!" or "Performance failed!" message and a High or Medium Impact, you need to research this problem using the data source summary page with its linked information.

**Steps**

1. Click the linked **Name** of the data source to open the Summary page.

2. On the Summary page, check the **Comments** area to read any notes left by another engineer who might also be investigating this failure.

3. Note any performance messages.

4. If there is a patch being applied to this data source, click link to check the **patch page** to see if that has caused the problem.

5. Move your mouse pointer over the segments of the **Event timeline** graph to display additional information.

6. Select an error message for a Device and displayed below the Event timeline and click the **Error details** icon that displays to the right of the message.

   The Error details include the text of the error message, most likely causes, information in use, and suggestions of what can be tried to correct the problem.

7. In the Devices reported by this data source area, you might filter the list to display only devices of interest, and you can click the linked **Name** of a device to display the **asset page** for that device.

8. To return to previously displayed pages, use one of these techniques:

   • Click the browser back arrow.

   • Right-click the back arrow to display a list of the pages and select the page you want.

9. To display detailed information about other resources, click other linked names.

10. When you return to the data source summary page, check the **Changes** area at the bottom of the page to see if recent changes caused the problem.

**Controlling data source polling**

After making a change to a data source, you might want it to poll immediately to check your changes, or you might want to postpone the data collection on a data source for one, three, or five days while you work on a problem.

**Steps**

1. Click **Admin** and navigate to the data source list view

2. Select the data source for which you want to control the polling.

3. Click the data source name link.
4. On the data source summary page, check the information and click one of these two polling options:
   - Poll again to force the data source to collect data immediately.
   - Postpone and select the length of the polling delay from 3, 7, or 30 days.

After you finish
If you postponed the data collection on a data source and want to restart collection, click Resume on the summary page.

Editing data source information
You can quickly edit data source setup information.

Steps
1. Click Admin and navigate to the data source list view
2. Locate the data source that you want to edit.
3. Use one of these methods to begin the changes:
   - Click Edit data source to the right of the selected data source.
   - Click the linked name of the selected data source and click Edit.
   Either method opens the Edit data source dialog box.
4. Make the desired changes and Click Save.

Editing information for multiple data sources
You can edit most of the information for multiple data sources of the same vendor and model at one time. For example, if these data sources share a user name and password, you can change the password in one place and thereby update the password for all the selected data sources.

About this task
Options that you cannot edit for the selected data sources appear dimmed or are not displayed in the Edit data source dialog box. Additionally, when an option displays a value of Mixed, it indicates that the value for the option varies between the selected data sources. For example, if the Timeout (sec) option for two selected data sources is Mixed, one data source could have a timeout value of 60 and the other could have a value of 90; therefore, if you change this value to 120 and save the changes to the data sources, the timeout setting for both data sources becomes 120.

Steps
1. Click Admin and navigate to the data source list view
2. Select the data sources you want to modify. Selected data sources must belong to same vendor, model and acquisition unit.
3. Click the Actions button and select the Edit option.
4. In the edit dialog, change any of the Settings as needed.
5. Click the Configuration link to change any of the basic options for the data sources.
6. Click the **Advanced Configuration** link to change any of the advanced options for the data sources.

7. Click **Save**.

**Mapping data source tags to annotations**

When a data source is configured to poll tag data, Insight automatically sets annotation values for an existing Insight annotation with the same name as a tag.

When the Insight annotation exists before the tags are enabled in the data source, the data source tag data is automatically added to the Insight annotation.

When you create an annotation after the tag is enabled, initial polling of the data source does not automatically update the annotation. There is a delay in the time it takes to replace or populate the Insight annotation. To avoid the delay, you can force the tag to annotation update by postponing and then resuming the data source.

**Deleting a data source**

If you have removed a data source from your environment, you must also delete it from the OnCommand Insight monitoring environment.

**Steps**

1. On the Insight toolbar, click **Admin**.
   
   The Data sources list opens.

2. Select the data source that you want to delete.

3. Click the linked data source name.

4. Check the information for the selected data source on the summary page to be certain that it is the one you want to delete.

5. Click **Delete**.

6. Click **OK** to confirm the operation.

**What data source patches are**

Data source patches fix issues with existing patches and also enable you to easily add new data source types (vendors and models). For each data source type in your network, you can upload data source patches. You can also install, test, and manage the patching process. However, only one patch can be active for a data source type at a time.

For each patch, you can perform these tasks:

- Check the before and after comparison of each data source receiving the patch.
- Write comments to explain decisions or summarize research.
- Make changes to a data source that is not responding well to the patch.
- Approve the patch to be committed to your Insight server.
- Roll back a patch that is not operating as you intended.
• Replace a failing patch with a different one.

**Applying a data source patch**

Data source patches are periodically available and enable you to fix issues with an existing data source, add a data source for a new vendor, or add a new model for a vendor.

**Before you begin**

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

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Patches**.
3. From the Actions button, select **Apply patch**.
4. In the **Apply data source patch** dialog box, click **Browse** to locate the `.patch` file.
5. Inspect the **Patch name**, **Description**, and **Impacted data source types**.
6. If the selected patch is correct, click **Apply Patch**.
   
   If you are applying a patch that fixes issues with a data source, all data sources of the same type are updated with the patch and you must approve the patch. Patches that do not affect any configured data sources are automatically approved.

**After you finish**

If you are applying a patch that adds a data source for a new vendor or a new model, you must add the data source after applying the patch.

**Installing a patch on one type of data source**

After uploading a data source patch, you can install it on all of the data sources of the same type.

**Before you begin**

You must have uploaded a patch file that you want to install on one type of data source.

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Patches**.
3. From the Actions button, select **Apply patch**.
4. In the **Apply data source patch** dialog box, click **Browse** to locate the uploaded patch file.
5. Check the **Patch name**, **Description**, and **Impacted data source types**.
6. If the selected patch is correct, click **Apply Patch**.
   
   All data sources of the same type are updated with this patch.
Managing patches

You can review the current status of all of the data source patches being applied to your network. If you want to perform an action on a patch, you can click the linked name in the Patches currently under review table.

Before you begin
You must have already uploaded and be installing at least one patch.

Steps
1. On the Insight toolbar, click Admin.
2. Click Patches.
   If no patches are being installed, the table of Patches currently under review is empty.
3. In Patches currently under review, check the status of the data source patches currently being applied.
4. To examine the details associated with a specific patch, click the linked name of the patch.
5. For the selected patch, you might click any of these options to perform the next action on the patch:
   • Approve patch commits the patch to the data sources.
   • Rollback removes the patch.
   • Replace patch enables you to select a different patch for those data sources.

Committing a data source patch

You use the information in the Patches summary to decide if the patch is performing as expected and then commit the patch to your network.

Before you begin
You have installed a patch and need to decide if the patch is successful and should be approved.

Steps
1. On the Insight toolbar, click Admin.
2. Click Patches.
   If no patches are being installed, the Patches currently under review is empty.
3. In Patches currently under review, check the status of the data source patches currently being applied.
4. To examine the details associated with a specific patch, click the linked name of the patch.
5. In the Patches summary information, shown in this example, check the Recommendation and Comments to assess the progress on the patch.
6. Check the Data sources affected table to see the status of each affected data source before and after the patch.

If you are concerned that there is a problem with one of the data sources being patched, click the linked Name in the Data sources affected table.

7. If you conclude that the patch should be applied to that type of data source, click Approve.

The data sources are changed and the patch is removed from Patches currently under review.

**Rolling back a data source patch**

If a data source patch is not working in the manner you expected, you can roll it back. Rolling back a patch deletes it, and restores the previous version as it was before this patch was applied.

**Steps**

1. On the Insight toolbar, click Admin.

2. Click Patches.

3. In Patches currently under review, click the linked name of the patch that appears to be unsuccessful.

4. On the Patches page for the data source, examine this information:
   
   • **Summary** describes when the patch was applied, the affected data sources, and comments about the patch from you or other members of your team.

   • **Affected data sources** lists all of the data sources being patched and includes a comparison of the before and after patching status.

5. To display the details for a data source that is not successfully processing the patch, click the linked Name.
   
   a. Check the summary information.

   b. Check the Event timeline to see any configuration or performance data that might be affecting this data source.

6. If you conclude that the patch is not going to be successful, click the browser back arrow to return to the Patches summary page.

7. Click Roll back to remove that patch.
If you know of a different patch that is more likely to be successful, click Replace patch and upload the new patch.
Device resolution

You need to discover all of the devices you want to monitor with OnCommand Insight. Discovery is necessary in order to accurately track performance and inventory in your environment. Typically the majority of devices in your environment are discovered through automatic device resolution.

**Note:** If you are performing an upgrade and have inactive Auto Resolution rules in the system you are upgrading from, these rules will be deleted during the upgrade. To preserve inactive Auto Resolution rules, activate the rules (check the box) before the upgrade is performed.

After you install and configure data sources, devices in your environment, including switches, storage arrays and your virtual infrastructure of hypervisors and VMs are identified. However, this does not normally identify 100% of the devices in your environment.

After data source type devices have been configured, best practice is to leverage device resolution rules to help identify the remaining unknown devices in your environment. Device resolution can help you resolve unknown devices as the following device types:

- physical hosts
- storage arrays
- tapes
- switches

Devices remaining as “unknown” after device resolution are considered generic devices, which you can also show in queries and on dashboards.

The rules created in turn will automatically identify new devices with similar attributes as they are added to your environment. In some cases, Device resolution also allows for manual identification bypassing the device resolution rules for undiscovered devices within Insight.

Incomplete identification of devices can result in issues including:

- Incomplete paths
- Unidentified multipath connections
- The inability to group applications
- Inaccurate topology views
- Inaccurate data in the Data warehouse and reporting

The Device resolution feature (Manage > Device resolution) includes the following tabs, each of which plays a role in device resolution planning and viewing results:

- “FC identify” contains a list WWNs and port information of Fibre Channel devices that were not resolved through automatic device resolution. The tab also identifies the percentage of devices that have been identified.

- “IP identify” contains a list of devices accessing CIFs shares and NFS shares that were not identified through automatic device resolution. The tab also identifies the percentage of devices that have been identified.

- “Auto resolution rules” contains the list of rules that are run when performing Fibre channel device resolution. These are rules you create to resolve unidentified Fibre channel devices.

- “Preferences” provides configuration options that you use to customize device resolution for your environment.
**Before you begin**

You need to know how your environment is configured before you define the rules for identifying devices. The more you know about your environment the easier it will be to identify devices.

You need to answer questions similar to the following to help you create accurate rules:

- Does your environment have naming standards for zones or hosts and what percentage of these are accurate?
- Does your environment use a switch alias or storage alias and do they match the host name?
- Does your environment use an SRM tool and can you use it to identify host names? What coverage does the SRM provide?
- How often do naming schemes change in your environment?
- Have there been any acquisitions or mergers that introduced different naming schemes?

After analyzing your environment, you should be able to identify what naming standards exist that you can expect to reliably encounter. The information you gathered might be represented graphically in a figure similar to the following:

In this example the largest number of devices are reliably represented by storage aliases. Rules that identify hosts using storage aliases should be written first, rules using switch aliases should be written next, and the last rules created should use zone aliases. Due to the overlap of the use of zone aliases and switch aliases, some storage alias rules might identify additional devices, leaving less rules required for zone aliases and switch aliases.
Steps to defining devices in your environment

Typically, you would use workflow similar to the following to identify devices in your environment. Identification is an iterative process and might require multiple steps of planning and refining rules.

Note: If you have unidentified devices (otherwise known as “unknown” or generic devices) in your environment and you subsequently configure a data source that identifies those devices upon polling, they will no longer be displayed or counted as generic devices.
Planning device resolution rules for your environment

Using rules to identify devices in your environment is typically an iterative process that requires a thorough analysis of your environment and the creation of multiple rules to identify as many devices as possible. The best case scenario is to set a goal to identify 100% of the devices in your environment.

The most efficient order for rules is to place the most restrictive rules first, resulting in most entries not pattern matching, with the process proceeding to less restrictive rules. This allows Insight to apply more patterns to each entry increasing the possibility of patterns matching and of positive host identification.

When you create rules, your objective should be to create rules that address the largest number of unidentified devices possible. For example, creating rules that follow a pattern of coverage similar to the following is far more efficient that creating 30 rules with lower percentages of coverage:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Percentage of coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule 1</td>
<td>60%</td>
</tr>
<tr>
<td>Rule 2</td>
<td>25%</td>
</tr>
<tr>
<td>Rule 3</td>
<td>8%</td>
</tr>
<tr>
<td>Rule 4</td>
<td>4%</td>
</tr>
<tr>
<td>Rule 5</td>
<td>1%</td>
</tr>
</tbody>
</table>

Creating device resolution rules

You create device resolution rules to identify hosts, storage, and tapes that are not automatically identified currently by OnCommand Insight. The rules that you create identify devices currently in your environment and also identify similar devices as they are added to your environment.

About this task

When you create rules you start by identifying the source of information that the rule runs against, the method used to extract information, and whether DNS lookup is applied to the results of the rule.

<table>
<thead>
<tr>
<th>Source that is used to identify the device</th>
<th>Method that is used to extract the device name from the source</th>
<th>DNS lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td>• SRM aliases for hosts</td>
<td>• As is (extract a name from an SRM)</td>
<td>Specifies if you use DNS to verify the host name.</td>
</tr>
<tr>
<td>• Storage alias containing an embedded host or tape name</td>
<td>• Delimiters</td>
<td></td>
</tr>
<tr>
<td>• Switch alias containing an embedded host or tape name</td>
<td>• Regular expressions</td>
<td></td>
</tr>
<tr>
<td>• Zone names containing an embedded host name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
You create rules in the Auto Resolution Rules tab. The following steps describe the rule creation process.

**Steps**

1. Click **Manage > Device resolution**

2. In the **Auto resolution rules** tab, click +Add
   
   The New Rule screen is displayed.
   
   **Note:** The New Rule screen includes a ? icon, that provides help and examples for creating regular expressions.

3. In the **Type** list select the device you want to identify.
   
   You can select Host or Tape.

4. In the **Source** list, select the source you want to use to identify the host.
   
   Depending on the source you chose, Insight displays the following response:
   
   - Zones lists the zones and WWN that need to be identified by Insight.
   - SRM lists the unidentified aliases that need to be identified by Insight.
   - Storage alias lists storage aliases and WWN that need to be identified by Insight.
   - Switch alias lists the switch aliases that need to be identified by Insight.

5. In the **Method** list select the method you want to employ to identify the host.

<table>
<thead>
<tr>
<th>Source</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRM</td>
<td>“As is”, “Delimiters”, “Regular expressions”</td>
</tr>
<tr>
<td>Storage alias</td>
<td>“Delimiters”, or “Regular expressions”</td>
</tr>
<tr>
<td>Switch alias</td>
<td>“Delimiters”, or “Regular expressions”</td>
</tr>
<tr>
<td>Zones</td>
<td>“Delimiters”, or “Regular expressions”</td>
</tr>
</tbody>
</table>

- Rules using “Delimiters” require the delimiters and the minimum length of the host name. The minimum length of the host name is number of characters that Insight should use to identify a host. Insight performs DNS lookups only for host names that are this long or longer. For rules using Delimiters, the input string is tokenized by the delimiter and a list of host name candidates is created by making several combinations of the adjacent token. The list is then sorted, largest to smallest. For example, for vipsnq03_hba3_emc3_12ep0 the list would result in the following:
  
  - vipsnq03_hba3_emc3_12ep0
  - vipsnq03_hba3_emc3
  - hba3_emc3_12ep0
  - vipsnq03_hba3
  - emc3_12ep0
  - hba3_emc3
  - vipsnq03
  - 12ep0
○ emc3
○ hba3

- Rules using “Regular expression” require a regular expression, the format, and cases sensitivity selection.

6. Click to run all rules, or click the down-arrow in the button to run the rule you created (and any other rules that have been created since the last full run of AR.)

Result
The results of the rule run are displayed in the FC identify tab.

Starting an automatic device resolution update
A device resolution update commits manual changes that have been added since the last full automatic device resolution run. Running an update can be used to commit and run only the new manual entries made to the device resolution configuration. No full device resolution run is performed.

Steps
1. Log into the Insight web UI.
2. Click Manage > Device Resolution
3. In the Device resolution screen, click the down-arrow in the Run AR button.
4. Click Update to start the update.

Rule assisted manual identification
This feature is used for special cases where you want to run a specific rule or a list of rules (with or without a one-time reordering) to resolve unknown hosts, storage, and tape devices or group of them.

Before you begin
You have a number of devices that have not been identified and you also have multiple rules that successfully identified other devices.

About this task
Note: If your source only contains part of a host or device name, use a regular expression rule and format it to add the missing text.

Steps
1. Log into the OnCommand Insight web UI.
2. Click Manage > Device resolution
3. Click the FC Identify tab.
   The system displays the identified and unidentified devices.
4. Select multiple unidentified devices.
5. Click Identify > Set host resolution or > Set tape resolution
   The system displays the Identify screen which contains a list of all of the rules that successfully identified devices.
6. Change the order of the rules to an order that meets your needs. 
   The order of the rules are changed in the Identify screen, but are not changed globally.

7. Select the method that that meets your needs. 
   OnCommand Insight executes the host resolution process in the order in which the methods 
   appear, beginning with those at the top. 
   When rules that apply are encountered, rule names are shown in the rules column and identified 
   as manual.

**Fibre Channel device resolution**

The FC Identify screen displays the WWN and WWPN of Fibre Channel devices whose hosts have 
not been identified by automatic device resolution. The screen also displays any devices that have 
been resolved by manual device resolution.

Devices that have been resolved by manual resolution contain a status of “OK” and identify the rule 
used to identify the device. Missing devices have a status of “Unidentified”. The total coverage for 
identification of devices is listed on this page.

You perform bulk actions by selecting multiple devices on the left-hand side of the FC identify 
screen. Actions can be performed on a single device by hovering over a device and selecting the 
identify or unidentify buttons on the far right of the list.

The Total coverage link displays a list of the "number of devices identified/number of devices 
available" for your configuration:

- SRM alias
- Storage alias
- Switch alias
- Zones
- User defined

**Adding a Fibre Channel device manually**

You can manually add a Fibre Channel device to OnCommand Insight using the manual add feature 
available in the Device resolution FC Identify tab. This process might be used for pre-identification 
of a device that is expected to be discovered in the future.

**Before you begin**

To successfully add a device identification to the system you need to know the WWN or IP address 
and the device name.

**About this task**

You can add a Host, Storage, Tape or Unknown Fibre Channel device manually.
**Steps**

1. Log in to the Insight web UI
2. Click Manage > Device resolution
3. Click the FC Identify tab.
4. Click the add button.
   The Add Device dialog is displayed
5. Enter the WWN or IP address, the device name, and select the device type.

**Result**

The device you enter is added to the list of devices in the FC Identify tab. The “Rule” is identified as Manual.

**Importing Fibre Channel device identification from a CSV file**

You can manually import Fibre Channel device identification into OnCommand Insight Device Resolution feature using a list of devices in a CSV file.

**Before you begin**

You must have a correctly formatted CSV file in order to import device identifications directly into the Device Resolution feature. The CSV file for Fibre Channel devices requires the following information:

<table>
<thead>
<tr>
<th>WWN</th>
<th>IP</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
</table>

**Note:** As a best practice, it is recommended to first export the FC Identify information to a CSV file, make your desired changes in that file, and then import the file back into FC Identify. This ensures that the expected columns are present and in the proper order.

To import FC Identify information:

**Steps**

1. Log into the Insight web UI.
2. Click Manage > Device Resolution
3. Select the FC identify tab.
4. Click Identify > Identify from file
5. Navigate to the folder containing your CSV files for import and select the desired file.

   The devices you enter are added to the list of devices in the FC Identify tab. The “Rule” is identified as “Manual”.

**Exporting Fibre Channel device identifications to a CSV file**

You can export existing Fibre Channel device identifications to a CSV file from the OnCommand Insight device resolution feature. You might want to export a device identification so that you can
modify it and then import it back into Insight where it is then used to identify devices that are similar to those originally matching the exported identification.

**About this task**

This scenario might be used when devices have similar attributes that can be easily edited in the CSV file and then imported back into the system.

When you export a Fibre Channel device identification to a CSV file, the file contains the following information in the order shown:

<table>
<thead>
<tr>
<th>WWN</th>
<th>IP</th>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
</table>

**Steps**

1. Log into the Insight web UI.
2. Click **Manage > Device Resolution**
3. Select the **FC identify** tab.
4. Select the Fibre Channel device or devices whose identification you want to export.
5. Click the export icon.
6. Chose if you want to open the CSV file or save the file.

**IP device resolution**

The IP Identify screen displays any iSCSI and CIFS or NFS shares that have been identified by automatic device resolution or by manual device resolution. Unidentified devices are also shown. The screen includes the IP address, Name, Status, iSCSI node, and share name for devices. The percentage of devices that have been successfully identified is also displayed.

**Adding IP devices manually**

You can manually add an IP device to OnCommand Insight using the manual add feature available in the IP Identify screen.

**Steps**

1. Log in to the Insight web UI.
2. Click **Manage > Device resolution**
3. Click the **IP Identify** tab.
4. Click the add button.
   
   The Add Device dialog is displayed
5. Enter the address, IP address, and a unique device name.
**Result**

The device you enter is added to the list of devices in the IP Identify tab.

**Importing IP device identification from a CSV file**

You can manually import IP device identifications into the Device Resolution feature using a list of device identifications in a CSV file.

**Before you begin**

You must have a correctly formatted CSV file in order to import device identifications. The CSV file for IP devices requires the following information:

<table>
<thead>
<tr>
<th>Address</th>
<th>IP</th>
<th>Name</th>
</tr>
</thead>
</table>

**Note:** As a best practice, it is recommended to first export the IP Identify information to a CSV file, make your desired changes in that file, and then import the file back into IP Identify. This ensures that the expected columns are present and in the proper order.

To import IP Identify information:

**Steps**

1. Log into the Insight web UI.
2. Click **Manage > Device Resolution**
3. Select the **IP identify** tab.
4. Click **Identify > Identify from file**
5. Navigate to the folder containing your CSV files for import and select the desired file.

The devices you enter are added to the list of devices in the IP Identify tab.

**Exporting IP device identification to a CSV file**

You can export existing IP device identifications from Insight using the Device Resolution feature. You might want to export a device identification so that you can modify it and then import it back into Insight so that it can be used to identify devices that are similar to those in the exported identification.

**About this task**

When you export an IP device identification to a CSV file, the file contains the following information in the order shown:

<table>
<thead>
<tr>
<th>Address</th>
<th>IP</th>
<th>Name</th>
</tr>
</thead>
</table>

**Steps**

1. Log into the Insight web UI.
2. Click **Manage > Device Resolution**
3. Select the **IP Identify** tab.
4. Select the IP device or devices whose identification you want to export.
5. Click the export icon.
6. Chose if you want to open the CSV file or save the file.

**Setting options in the Preferences tab**

The device resolution preferences tab lets you create an auto resolution schedule, specify storage and tape vendors to include or exclude from identification, and set DNS lookup options.

**Auto resolution schedule**

An auto resolution schedule can specify when automatic device resolution is run:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every</td>
<td>Use this option to run automatic device resolution on intervals of days, hours, or minutes.</td>
</tr>
<tr>
<td>Every day</td>
<td>Use this option to run automatic device resolution daily at a specific time.</td>
</tr>
<tr>
<td>Manually</td>
<td>Use this option to only run automatic device resolution manually.</td>
</tr>
<tr>
<td>On every environment change</td>
<td>Use this option to run automatic device resolution whenever there is a change in the environment.</td>
</tr>
</tbody>
</table>

If you specify manually, nightly automatic device resolution is disabled.

**DNS processing options**

DNS processing options allow you to select the following features:

- When DNS lookup result processing is enabled, you can add a list of DNS names to append to resolved devices.
- You can select “Auto resolution of IPs:” to enables automatic host resolution for iSCSI initiators and hosts accessing NFS shares by using DNS lookup. If this is not specified, only FC-based resolution is performed.
- You can choose to allow underscores in host names and to use a "connected to" alias instead of the standard port alias in results.

**Including or excluding specific storage and tape vendors**

You can include or exclude specific storage and tape vendors for automatic resolution. You might want to exclude specific vendors if you know, for example, that a specific host will become a legacy host and should be excluded from your new environment. You can also re-add vendors that you earlier excluded but no longer want excluded.

**Regular expression examples**

If you have selected the regular expression approach as your source naming strategy, you can use the regular expression examples as guides for your own expressions used in the OnCommand Insight automatic resolution methods.

**Formatting regular expressions**

When creating regular expressions for OnCommand Insight automatic resolution, you can configure output format by entering values in a field named FORMAT.
The default setting is \\1, which means that a zone name that matches the regular expression is replaced by the contents of the first variable created by the regular expression. In a regular expression, variable values are created by parenthetical statements. If multiple parenthetical statements occur, the variables are referenced numerically, from left to right. The variables can be used in the output format in any order. Constant text can also be inserted in the output, by adding it to the FORMAT field.

For example, you might have the following zone names for this zone naming convention:

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_solaris_FC1

And you might want the output to be in the following format:

[hostname]-[data center]-[device type]

To do this, you need to capture the host name, data center, and device type fields in variables, and use them in the output. The following regular expression would do this:


Because there are three sets of parentheses, the variables \1, \2 and \3 would be populated.

You could then use the following format to receive output in your preferred format:

\2-\1-\3

Your output would be as follows:

hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris

The hyphens between the variables provide an example of constant text that is inserted in the formatted output.

**Example 1 showing zone names**

In this example, you use the regular expression to extract a host name from the zone name. You could create a regular expression if you have something similar to the following zone names:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

The regular expression that you could use to capture the host name would be:

The outcome is a match of all zones beginning with S that are followed by any combination of digits, followed by an underscore, the alphanumeric hostname (myComputer1Name), an underscore or hyphen, the capital letters HBA, and a single digit (0-9). The hostname alone is stored in the $1 variable.

The regular expression can be broken into its components:

- "S" represents the zone name and begins the expression. This matches only an "S" at the beginning of the zone name.
- The characters [0-9] in brackets indicate that what follows "S" must be a digit between 0 and 9, inclusive.
- The + sign indicates that the occurrence of the information in the preceding brackets has to exist 1 or more times.
- The _ (underscore) means that the digits after S must be followed immediately by only an underscore character in the zone name. In this example, the zone naming convention uses the underscore to separate the zone name from the host name.
- After the required underscore, the parentheses indicate that the pattern contained within will be stored in the $1 variable.
- The bracketed characters [a-zA-Z0-9] indicate that the characters being matched are all letters (regardless of case) and numbers.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The bracketed characters [_-] (underscore and dash) indicate that the alphanumeric pattern must be followed by an underscore or a dash.
- The letters HBA in the regular expression indicate that this exact sequence of characters must occur in the zone name.
- The final set of bracketed characters [0-9] match a single digit from 0 through 9, inclusive.

**Example 2**

In this example, skip up to the first underscore "_", then match E and everything after that up to the second "_", and then skip everything after that.

Zone: Z_E2FHDBS01_E1NETAPP

Hostname: E2FHDBS01

RegExp: .*?_E.*?_.*?

**Example 3**

The parentheses "( )" around the last section in the Regular Expression (below) identifies which part is the hostname. If you wanted VSAN3 to be the host name, it would be: [a-zA-Z0-9]+([a-zA-Z0-9]+).*

Zone: A_VSAN3_SR48KENT_A_CX2578_SPA0

Hostname: SR48KENT


**Example 4 showing a more complicated naming pattern**

You could create a regular expression if you have something similar to the following zone names:
The regular expression that you could use to capture these would be:

```
([a-zA-Z0-9]*)_.*
```

The \1 variable would contain only myComputerName123 after being evaluated by this expression.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The bracketed characters \[a-zA-Z0-9\] mean that any letter (regardless of case) or digit will match.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The _ (underscore) character in the regular expression means that the zone name must have an underscore immediately following the alphanumeric string matched by the preceding brackets.
- The . (period) matches any character (a wildcard).
- The * (asterisk) indicates that the preceding period wildcard may occur 0 or more times.
  In other words, the combination .* indicates any character, any number of times.

**Example 5 showing zone names without a pattern**

You could create a regular expression if you have something similar to the following zone names:

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

The regular expression that you could use to capture these would be:

```
(.*?)_.*
```

The \1 variable would contain myComputerName (in the first zone name example) or myComputerName123 (in the second zone name example). This regular expression would thus match everything prior to the first underscore.

The regular expression can be broken into its components:

- The parentheses indicate that the pattern contained within will be stored in the \1 variable.
- The .* (period asterisk) match any character, any number of times.
- The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.
- The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.
- The _.* character matches the first underscore found and all characters that follow it.

**Example 6 showing computer names with a pattern**

You could create a regular expression if you have something similar to the following zone names:
• Storage1_Switch1_myComputerName123A_A1_FC1
• Storage2_Switch2_myComputerName123B_A2_FC2
• Storage3_Switch3_myComputerName123T_A3_FC3

The regular expression that you could use to capture these would be:

```
.*(.*?)\((?:[a-zA-Z0-9]+)[ABT]_.*
```

Because the zone naming convention has more of a pattern, we could use the above expression, which will match all instances of a hostname (myComputerName in the example) that ends with either an A, a B, or a T, placing that hostname in the \1 variable.

The regular expression can be broken into its components:

• The .* (period asterisk) match any character, any number of times.

• The ? character makes the match non-greedy. This forces it to stop matching at the first underscore, rather than the last.

• The underscore character matches the first underscore in the zone name.

• Thus, the first .*?_ combination matches the characters Storage1_ in the first zone name example.

• The second .*?_ combination behaves like the first, but matches Switch1_ in the first zone name example.

• The parentheses indicate that the pattern contained within will be stored in the \1 variable.

• The bracketed characters [a-zA-Z0-9-] mean that any letter (regardless of case) or digit will match.

• The * (asterisk) following the brackets indicates that the bracketed characters occur 0 or more times.

• The bracketed characters in the regular expression [ABT] match a single character in the zone name which must be A, B, or T.

• The _ (underscore) following the parentheses indicates that the [ABT] character match must be followed up an underscore.

• The .* (period asterisk) match any character, any number of times.

Example 7

Zone: myComputerName123_HBA1_Symml_FA1
Hostname: myComputerName123
RegExp: ([a-zA-Z0-9]+)_.*

Example 8

This example finds everything before the first _.

Zone: MyComputerName_HBA1_Symml_FA1
Example 9
This example finds everything after the 1st _ and up to the second _.
Zone: Z_MyComputerName_StorageName
Hostname: MyComputerName
RegExp: (.*)_.*

Example 10
This example extracts "MyComputerName123" from the zone examples.
Zone: Storage1_Switch1_MyComputerName123A_A1_FC1
Storage2_Switch2_MyComputerName123B_A2_FC2
Storage3_Switch3_MyComputerName123T_A3_FC3
Hostname: MyComputerName123
RegExp: .*/.*(.*?).*/.*?

Example 11
Zone: Storage1_Switch1_MyComputerName123A_A1_FC1
Hostname: MyComputerName123A
RegExp: .*/.*(.*?).*/.*?

Example 12
The ^ (circumflex or caret) inside square brackets negates the expression, for example, [^Ff] means anything except uppercase or lowercase F, and [^a-z] means everything except lowercase a to z, and in the case above, anything except the _. The format statement adds in the "." to the output host name.
Zone: mhs_apps44_d_A_10a0_0429
Hostname: mhs-apps44-d
RegExp: (\[^_\]+)_([^_]+)_.*?

Example 13
In this example, the storage alias is delimited by "\" and the expression needs to use "\" to define that there are actually "\" being used in the string, and that those are not part of the expression itself.
Storage Alias: \Hosts\E2DOC01C1\E2DOC01N1
Hostname: E2DOC01N1
RegExp: \\.*?\\.*?\\(.\*)

Example 14
This example extracts "PD-RV-W-AD-2" from the zone examples.
**Example 15**

The format setting in this case adds the "US-BV-" to the hostname.

**Zone:** SRV_USBVM11_F1

**Hostname:** US-BV-M11

**RegExp:** SRV_USBV([A-Za-z0-9]+)_F[12]

**Format:** US-BV-\1
Maintaining Insight

Whether you are new to Insight and have a new system to set up, or your system has been operating for some time, you must take steps to maintain smooth operation of Insight and your network. The key maintenance concept is that changes in your network usually need to be accommodated in Insight.

These are the most common maintenance tasks:

- Maintaining Insight backups
- Updating expired Insight licenses
- Coordinating data source patches
- Updating the Insight version on all acquisition units
- Deleting removed data sources from Insight

Managing Insight

OnCommand Insight monitors your environment, enabling you to research potential problems before a crisis is reported. The Assets Dashboard provides summary pie charts, heat maps for IOPS, and an interactive chart of the top 10 utilized storage pools.

Steps

1. Open the Insight Assets Dashboard and move your cursor over the pie charts to examine the asset distribution in these three charts:
   - Capacity by Vendor shows the total raw capacity for storage by each vendor.
   - Capacity by Tier shows the total useable capacity for each storage tier.
   - Switch Ports pie chart shows the manufacturers of ports and shows the percentage of ports used.

2. View Facts About Your Environment to see information about your environment's used capacity, the capacity's efficiency, consumed FC resources, and virtual infrastructure statistics.

3. Position your cursor over a storage pool bar in the Top 10 Utilized Pools chart to view the used and unused capacity of the storage pool.

4. Click any asset name appearing in large text (which indicates that the asset has issues) in the Storage IOP heat map to display a page summarizing the current state of that asset.

5. In the lower right corner of the Assets Dashboard, click any asset name appearing in large text (which indicates the asset has issues) in the Virtual Machine IOPS heat map to display a page summarizing the current state of the asset.

6. On the Insight toolbar, click Admin.

7. Note any areas showing solid red circles.
   - In the OnCommand Insightweb UI, potential problems are marked with a solid red circle.

8. Click Data Sources to examine a list of all monitored data sources.
Examine any data source with a **Status** column containing a message with a solid red circle and with an **Impact** listed as High or Medium. These are at the top of the table. The problems with those data sources affect a significant portion of your network, which you need to address.

9. Click **Acquisition Units** to note the status for each IP address running Insight and to restart an acquisition unit, if necessary

10. Click **Health** to see high-level instance monitoring of the Insight servers.

### Monitoring OnCommand Insight system health

You should periodically check the current status of your Insight system components by viewing the health page, which shows the status of each component and alerts you when there is an issue.

**Steps**

1. Log in to the Insight web UI.

2. Click **Admin** and select **Health**.
   
The Health page is displayed.

3. View the summary of the current status of the components paying particular attention to any attention status in the **Details** column that is preceded by a red circle, which indicates an issue that requires your immediate attention.

The Health page displays information about any or all of the following Insight components based on your system configuration:

<table>
<thead>
<tr>
<th>Component</th>
<th>Test</th>
<th>Details</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>Inventory data</td>
<td>Status of local acquisition unit</td>
<td>“OK” if number of concurrently-polling data sources is less than 75% of</td>
</tr>
<tr>
<td></td>
<td>processing</td>
<td></td>
<td>execution pool maximum (default maximum is 30).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Acquisition is busy” if usage is greater than 75%, and recommends</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>increasing polling interval or adding more remote acquisition units.</td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>Engine capacity</td>
<td>Count of applications monitored for anomaly detection</td>
<td>Number and percentage of applications being monitored out of 48 possible</td>
</tr>
<tr>
<td>Engine</td>
<td></td>
<td></td>
<td>applications.</td>
</tr>
<tr>
<td>Component</td>
<td>Test</td>
<td>Details</td>
<td>Displays</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Anomaly Detection Engine</td>
<td>Engine status</td>
<td>Status of anomaly detection engine</td>
<td>“OK” if no errors are detected, otherwise displays information about any error found. See the prelert.log file for more information.</td>
</tr>
<tr>
<td>DWH</td>
<td>Backup</td>
<td>Status of Data Warehouse scheduled backup</td>
<td>“OK” and the last successful DWH backup time if DWH scheduled backup is enabled. Otherwise, displays information about any error found.</td>
</tr>
<tr>
<td>DWH</td>
<td>ETL</td>
<td>Status of Data Warehouse ETL</td>
<td>“OK” and the last successful DWH build time if no errors. Otherwise, displays information about any error found.</td>
</tr>
<tr>
<td>Server</td>
<td>ASUP</td>
<td>Status of ASUP</td>
<td>“ASUP Enabled” and the last successful phonehome time if available. “ASUP Failed” if phonehome is enabled but encountered a problem. &quot;Invalid backup location&quot; if backup directory is not valid. Displays the last successful phonehome time as well as time of the last failed attempt if available. “ASUP Disabled” if phonehome is disabled.</td>
</tr>
<tr>
<td>Component</td>
<td>Test</td>
<td>Details</td>
<td>Displays</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>----------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server</td>
<td>Auto resolution</td>
<td>Status of automatic device resolution</td>
<td>“OK” if no errors. “Auto resolution is blocked” if identification errors prevent resolution progress. “Low success rate” if less than 75% of generic devices could be identified.</td>
</tr>
<tr>
<td>Server</td>
<td>Elasticsearch</td>
<td>Status of elastic search data store</td>
<td>“OK” if no errors. “Service unavailable” if unable to connect to elastic search service. &quot;Cluster mode detected&quot; if more than one node is detected. &quot;High memory utilization&quot; if heap space used is more than 85%. &quot;Status: RED&quot; indicates an error reported by elastic search. Displays information about the error and recommends contacting customer support.</td>
</tr>
<tr>
<td>Server</td>
<td>CPU</td>
<td>Insight CPU usage</td>
<td>“OK” if CPU load is less than 65%. “System CPU load is high. Reduce your CPU load.” if CPU load is greater than 65%.</td>
</tr>
<tr>
<td>Server</td>
<td>Disk space</td>
<td>Status of disk space</td>
<td>Free disk space, disk space in use by Insight, and recommended disk space reserved for Insight. “Low Disk Space” if disk utilization is more than 80%.</td>
</tr>
<tr>
<td>Component</td>
<td>Test</td>
<td>Details</td>
<td>Displays</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>--------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server</td>
<td>EventBus</td>
<td>Status of EventBus</td>
<td>“EventBus is empty” if EventBus queue is empty, otherwise displays status of EventBus queue.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Server            | Inventory data processing | Status of inventory data processing capability of Insight server | “OK” if Insight server is not busy.  
“Server is busy” if the server is busy at least 75% of the time for the last hour.  
Recommends not adding more data sources and recommends splitting the environment to several servers. |
|                   |                           |                                                              |                                                                                                   |
| Server            | MySQL                     | Status of MySQL database                                    | “OK” if no problems are detected.  
“The database is having performance issues. Some queries are taking too long to run” if the number of slow queries is more than 5%.  
“The database log file grew more than <size> in the past hour. Check MySQL log file” if the error log grows to more than 20 KB. |
|                   |                           |                                                              |                                                                                                   |
| Server            | Performance archive       | Status of performance archive                                | “Performance archive is enabled” or “Performance archive is not enabled”.                         |
|                   |                           |                                                              |                                                                                                   |
| Server            | Physical memory           | Status of physical memory                                    | “OK” if memory usage is less than 85%.  
“Memory usage is high. Reduce your overall memory footprint for system stability” if memory usage is greater than 85%. |
<p>| | | | |
|                   |                           |                                                              |                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Component</th>
<th>Test</th>
<th>Details</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Service pack</td>
<td>Service pack availability</td>
<td>Displays whether a service pack is available for Insight. If a service pack is available, displays instructions.</td>
</tr>
<tr>
<td>Server</td>
<td>Usage information</td>
<td>Status of sending of usage information</td>
<td>Displays whether sending of usage information to NetApp is enabled or disabled. Recommends enabling if disabled. Displays last attempted or last successful send time. Displays information on any problems encountered.</td>
</tr>
<tr>
<td>Server</td>
<td>Violation</td>
<td>Status of open violations</td>
<td>“OK” if the number of open violations is less than 75% of the violations limit. “Maximum number of open violations allowed is &lt;number&gt;” if the number of open violations is greater than 75% of the violations limit. Recommends reviewing performance policy configuration. “Violation manager is blocked” if the number of open violations is at the violations limit. Note that the violation manager cannot create new violations and recommends reviewing performance policy configuration.</td>
</tr>
</tbody>
</table>
### Component Test Details Displays

<table>
<thead>
<tr>
<th>Component</th>
<th>Test</th>
<th>Details</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Weekly backup</td>
<td>Status of weekly backup</td>
<td>“OK” if weekly backup is enabled, otherwise displays “Weekly backup is not enabled”.</td>
</tr>
</tbody>
</table>

**Note:** If the anomaly detection engine displays an error, see the prelert.log file in the following location for more information:

- **Windows:** disk drive: \install directory\SANscreen\Wildfly\Standalone\Logs
- **Linux:** /var/log/netapp/oci/wildfly/

#### Deleting inactive devices

Deleting devices that are inactive helps keep your data cleaner and easier to navigate.

**About this task**

To delete inactive devices from Insight, do the following:

**Steps**

1. Create a new query or open an existing query.
2. Choose either the *generic device, host, storage, switch,* or *tape* asset type.
3. Add a filter for **Is active**, and set the filter to **No**.
   - The results table displays only assets that are not active.
4. Select the devices that you want to delete.
5. Click the **Actions** button and select **Delete Inactive Devices**.
   - Your inactive devices are deleted and will no longer be displayed in Insight.

#### Auditing system and user activities

If you want to locate unexpected changes, you can view an audit trail of the OnCommand Insight system and its user activities.

**About this task**

Insight generates audit entries for any user activities that affect the storage network or its management, including the following:

- Logging in
- Authorizing or unauthorizing a path
- Updating an authorized path
- Setting global policies or thresholds
- Adding or removing a data source
• Starting or stopping a data source
• Updating data source properties
• Adding, editing, or deleting a task
• Removing an application group
• Identifying or changing the identification for a device
• Create a user
• Delete a user
• Modify a user (Guest à Admin)
• Logout of a user (either forced logout or manual logout)
• Deleting an acquisition unit
• Update License
• Enabling backup
• Disabling Backup
• Enabling ASUP (Enabling Proxy on same page is reported in audit log)
• Disabling ASUP (Disabling Proxy on same page is reported in audit log)
• Security - re-key, change system passwords.
• Removing/adding annotations on assets

Steps
1. Open Insight in your browser.
2. Click Admin and select Audit.
   The Audit page displays the audit entries in a table.
3. You can view the following details in the table:
   Time
   Date and time that the changes were made
   User
   Name of user associated with the audit entry
   Role
   User account's role, which is guest, user, or administrator
   IP
   IP address associated with the audit entry
   Action
   Type of activity in the audit entry
   Details
   Details of the audit entry
   If there is a user activity that affects a resource, such as a data source or an application, the details include a link to the resource's landing page.
**Note:** When a data source is deleted, the user activity details related to the data source no longer contain a link to the data source’s landing page.

4. You can display audit entries by choosing a particular time period (1 hour, 3 hours, 24 hours, 3 days, and 7 days), with Insight showing a maximum number of 1000 violations for the selected time period.

You can click a page number below the table to browse through data by page if there is more data than fits on a single page.

5. You change the sort order of the columns in a table to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header; to return to the default sort order, click any other column header.

By default, the table displays the entries in descending order.

6. You can use the **filter** box to show only the entries you want in the table.

**Example**

To see only the audit entries by the user *izzyk*, type *izzyk* in the **filter** box.

---

**Monitoring the violations in your network**

When Insight generates violations due to the thresholds set in performance policies, you can view them using the Violations Dashboard. The dashboard lists all the violations that occur in your network and enables you to locate and address issues.

**Steps**

1. Open OnCommand Insight in your browser.

2. On the Insight toolbar, click **Dashboards** and select **Violations Dashboard**.

   The Violations Dashboard displays.

3. You can use the **Violations By Policies** pie chart in the following ways:
   - You can position your cursor over any slice of a chart to display the percentage of the total violations that occurred for a particular policy or metric.
   - You can click a slice of a chart to “enlarge” it, which enables you to emphasize and study more carefully that slice by moving it away from the rest of the chart.
   - You can click the icon in the upper-right corner to display the pie chart in full screen mode, and click again to minimize the pie chart.

   A pie chart can contain a maximum of five slices; thus, if you have six policies that generate violations, Insight combines the fifth and sixth slices into an “Others” slice. Insight assigns the most violations to the first slice, the second most violations to the second slice, and so on.

4. You can use the **Violations History** chart in the following ways:
   - You can position your cursor over the chart to display the total number of violations that occurred at a particular time and the number that occurred out of the total for each specified metric.
   - You can click a legend label to remove the data associated with the legend from the chart. Click on the legend to display the data again.
• You can click the icon in the upper-right corner to display the chart in full screen mode, and click again to minimize the pie chart.

5. You can use the Violations Table in the following ways:

• You can click the icon in the upper-right corner to display the table in full screen mode, and click again to minimize the pie chart.
  If your window size is too small, then the Violations Table displays only three columns; however, when you click , additional columns (up to seven) display.

• You can display violations for a particular time period (1h, 3h, 24h, 3d, 7d, and 30d), with Insight showing a maximum number of 1000 violations for the selected time period.

• You can use the filter box to show only the violations you want.

• You can change the sort order of the columns in a table to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header; to return to the default sort order, click any other column header.
  By default, the table displays the violations in descending order.

• You can click a violation in the ID column to display the asset page for the duration of the violation.

• You can click the resource links (for example, storage pool and storage volume) in the Description column to display the asset pages associated with those resources.

• You can click the performance policy link in the Policy column to display the Edit Policy dialog box.
  You might want to adjust the thresholds for a policy if you feel it generates too few or too many violations.

• You can click a page number to browse through data by page if there is more data than fits on a single page.

• You can click to dismiss the violation.

Acquisition unit status

The status of the Insight acquisition units connected to your server is displayed in the Admin > Acquisition Units table. If a unit in the list has a solid red circle in the description, that unit has a serious problem that you must investigate. You can select an entry in this table and restart that acquisition unit.

The Acquisition Units table displays this information for each unit:

• Name

• IP

• Status is the operating status of the acquisition unit.

• Last reported displays last time a data source connected to the acquisition unit reported.

If you position your pointer over one of the units in the table, you can click the Restart Acquisition Unit icon to restart that unit.
Restoring the Insight database

To restore your Insight database from a verified backup file, use the Troubleshooting options. This operation completely replaces your current OnCommand Insight data.

**Before you begin**

**Best practice:** Before restoring your OnCommand Insight database, use the manual backup process to create a copy of the current database. Check the backup file you plan to restore be certain that it was a successful backup containing the files you want to restore.

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Troubleshooting**.
3. In the Restore a database section, select the backup file you want to restore from the **Select Backup** menu.
4. Click **Restore**.
5. On the warning that all data will be replaced, click **OK**.

The status of the restore activity is displayed on the restore page.

Updating expired licenses

If one or more of your Insight licenses expired, you can update the licenses quickly using the same procedure as you did to install the licenses originally.

**Steps**

1. In a text editor, such as Notepad, open the new license file you received from NetApp Support and copy the license key text to your Windows Clipboard.
2. Open OnCommand Insight in your browser.
3. Click on **Admin** on the toolbar.
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.
   
   This operation adds your new licenses to any currently active Insight licenses.

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 usage section. Proxy must be properly configured and enabled for your environment.

**Licenses no longer compliant**

If you notice the "Not Compliant" message on your Insight Licenses page, Insight is managing more terabytes than your company licensed.

The "Not Compliant" message means your company paid for fewer terabytes than Insight is currently managing. The difference between the managed terabytes and the licensed number of terabytes is shown beside the non-compliance message.

The operation of your Insight system is not affected, but you should contact your NetApp representative to increase your license coverage and update the appropriate license.

**Replacing licenses for older Insight versions**

If you have purchased a new Insight version that is not backward compatible with your older version of the product, you must replace the older licenses with the new licenses.

When you are installing the new licenses, you must select the **Replace** operation before you save the license key text.

**Applying a service pack**

Periodically, service packs are available, which you can apply to take advantage of fixes and enhancements to OnCommand Insight.

**Before you begin**

- You must have downloaded the service pack file (for example, `7.2service_pack_1.patch`) from the NOW site.
- You must have approved all patches.

**Steps**

1. On the Insight toolbar, click **Admin**.

2. Click **Patches**.

3. From the Actions button, select **Apply patch**.

4. In the **Apply data source patch** dialog box, click **Browse** to locate the service pack file.
5. Inspect the **Patch name**, **Description**, **Impacted data source types**, which shows if any data sources are affected, and **Details**, which describes the enhancements that the service pack contains.

6. If the selected service pack is correct, click **Apply Patch**.
   Service packs are approved automatically; no further action is required.

### Preparing a special troubleshooting report

Insight sends information to NetApp Customer Support automatically through the ASUP system you set up after installing the software. However, you might want to create a troubleshooting report and open a case with the Support team for a specific problem.

You can use tools in Insight to perform a manual Insight backup, bundle the logs, and send that information to NetApp Customer Support.

### Manually backing up the OnCommand Insight database

If you enabled weekly backups for the OnCommand Insight database, you are automatically generating copies that you can use to restore the database, if necessary. If you need to create a backup before a restore operation, or to send to NetApp technical support for assistance, you can create a backup .zip file manually.

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Troubleshooting**.
3. In the Send/Collect data section, click **Backup**.
4. Click **Save File**.
5. Click **OK**.

### Bundling logs for Support

When troubleshooting a problem with Insight software, you can quickly generate a zip file (using the "gz" format) of the logs and acquisition recordings to send to NetApp Customer Support.

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Troubleshooting**.
3. In the Send / Collect data section, click **Bundle logs**.
4. Click **Save File**.
5. Click **OK**.

### Sending information to NetApp Support

The NetApp automated support (ASUP) facility sends troubleshooting information directly to the NetApp Customer Support team. You can force a special report to be sent.

**Steps**

1. On the Insight toolbar, click **Admin**.
2. Click **Setup**.
3. Click the **Backup/ASUP** tab.
4. In the Send/Collect data area, click **Send ASUP now** to submit your logs, recordings, and backup to NetApp Support.

---

**Scrubbing data for transfer to support**

Customers who have secure environments need to communicate with NetApp Customer Service to troubleshoot problems that arise without compromising their database information. The OnCommand Insight Scrub utilities allow you set up a comprehensive dictionary of keywords and patterns so that you can "cleanse" sensitive data and send scrubbed files to Customer Support.

**Steps**

1. In the web UI, click **Admin** and select **Troubleshooting**.
2. At the bottom of the page in the Other tasks area, click the **Scrub utilities** link.
3. There are several scrub sections: Lookup in Dictionary, Scrub data, and Build dictionary, Custom keywords, and Regular expressions.
4. In the **Lookup in dictionary** section, Enter a code to display the value it replaces, or enter a value to see the code that replaces it. Note: before you can do a lookup, you must **Build** the dictionary to identify values to scrub from the support data.
5. To add your own keywords to scrub from the support data, in the **Custom keywords** section, click **Actions > Add custom keyword**. Enter a keyword and click **Save**. The keyword is added to the dictionary.
6. Expand **Patterns (regexp)**. Click **Add** to get the dialog box for entering a new pattern.
7. To use a regular expression to identify words or phrases to scrub, enter a pattern or patterns in the **Regular expressions** section. Click **Actions > Add regular expression**, enter a Name for the pattern and the Regular expression in the fields and click **Save**. The information has been added to the dictionary.

**Note:** Patterns must be encompassed by round parentheses to identify a regular expression capturing group.
8. In the **Build dictionary** section, click **Build** to initiate compilation of the dictionary of all words identified as sensitive from the OnCommand Insight database.

On completion, you see a prompt informing you the revised dictionary is available. The Database description includes a line indicating how many keywords are in the dictionary. Check your keywords in the dictionary for accuracy. If you find problems and want to rebuild the dictionary, click **Reset** on the Database block to remove all keywords collected from the OnCommand Insight database from the dictionary. As the prompt advises, no other keywords will be deleted. Return to the Scrub utilities and enter your Custom Keywords again.

9. After you create a Scrub dictionary, you can use it to scrub a log, XML, or other text file to make the data anonymous.

10. To scrub a log, XML, or other text file, in the **Scrub data** section, Browse to locate the file and click **Scrub file**.

## Advanced troubleshooting

To complete your OnCommand Insight configuration, you must use the advanced troubleshooting tools. These tools run in the browser and are opened from the **Admin > Troubleshooting** page.

To open the advanced troubleshooting tools in the browser, click the **Advanced Troubleshooting** link at the bottom of the page.

The advanced troubleshooting tools allow you to view various reports, system information, installed packages, and logs, as well as perform numerous actions such as restarting the server or acquisition units, update DWH annotations, and import annotations.

See the Advanced Troubleshooting page for all available options.

## Configuring the number of hours to ignore dynamic data

You can configure the number of hours during which OnCommand Insight ignores updating dynamic data, such as used capacity. If the default of six hours is used and no configuration changes occur, reports will not be updated with dynamic data until after the default number of hours. This option improves performance because this option defers updates when only the dynamic data changes.

### About this task

If a value is set for this option, OnCommand Insight will update dynamic data based on the following rules:

- If no configuration changes occur but capacity data changes, data will not be updated.
- Dynamic data (other than configuration changes) will be updated only after the timeout specified in this option.
- If configuration changes occur, configuration and dynamic data is updated.

Dynamic data impacted by this option includes the following:

- Capacity violation data
- File Systems Allocated Capacity and Used Capacity
- Hypervisor
  - Virtual Disk Used Capacity
  - Virtual Machine Used Capacity
- Internal Volume
• Data Allocated Capacity
• Data Used Capacity
• Deduplication Savings
• Last Known Access Time
• Last Snapshot Time
• Other Used Capacity
• Snapshot Count
• Snapshot Used Capacity
• Total Used Capacity

• iSCSI Session Initiator IPs, Target Session ID, and Initiator Session ID
• Qtree Quota Used Capacity
• Quota Used Files and Used Capacity
• Storage Efficiency Technology, Gain/Loss, and Potential Gain/Loss
• Storage Pool
  • Data Used Capacity
  • Deduplication Savings
  • Other Used Capacity
  • Snapshot Used Capacity
  • Total Used Capacity
• Volume
  • Deduplication Savings
  • Last Known Access Time
  • Used Capacity

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. Click the Advanced settings tab, in the Acquisition Dynamic Attributes section enter the number of hours that OnCommand Insight should ignore dynamic data for Acquisition Dynamic Attributes.
4. Click Save.
5. (Optional) To restart the acquisition unit, click the Restart Acquisition Unit link.

Restating the local acquisition unit reloads all of the OnCommand Insight data source views. This change is applied during the next poll, so you do not have to restart the Acquisition Unit.
Generating logs for Customer Support

If requested by Customer Support, generate a server, acquisition, or remote log for troubleshooting purposes.

About this task
If NetApp Customer Support requests, use this option to generate the logs.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click Advanced Troubleshooting.
3. On the next page in the Advanced menu, click the Troubleshooting link.
4. Click the Logs tab and select the log file to download.
   A dialog box opens allowing you to open the log or save the log locally.

Displaying system information
You can display the Microsoft Windows IP configuration information about the system on which OnCommand Insight server is deployed.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. On the Advanced Troubleshooting page, click the Reports tab.
4. Click System Information.
   The Windows IP configuration includes information such as the host name, DNS, IP address, subnet mask, OS information, memory, boot device, and connection name.

Listing installed OnCommand Insight components
You can display a list of the installed OnCommand Insight components including, among others, inventory, capacity, dimensions, and the Data Warehouse views. Customer Support might ask you for this information, or you might want to see what software versions were installed and when they were installed.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. On the Advanced Troubleshooting page, click the Reports tab.
4. Click Installed Software Packages.
Calculating the number of database objects

To determine the number of objects in the OnCommand Insight database, use the Calculate Scale feature.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. On the Advanced Troubleshooting page, click the Reports tab.
4. Click Calculated Scale.

Restarting the OnCommand Insight Server

When you restart the OnCommand Insight Server, refresh the page and log into the OnCommand Insight Portal again.

About this task
Note: Both of these options should only be used upon request by NetApp Customer Support. There is no confirmation prior to restart.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. On the next page in the Advanced menu, click the Actions tab.
4. Click Restart Server.

Moving MySQL data using the migrate option

You can use migrate MySQL data directory to a different directory. You can retain the current data directory. You can use the migrate option on the Troubleshooting menu or you can use the command line. This procedure describes how to use the Troubleshooting > Migrate MySQL data option.

About this task
If you retain the current data directory, it will be kept as a backup and renamed.

Steps
1. In the web UI, click Admin and select Troubleshooting.
2. Click Advanced Troubleshooting.
3. Select the Actions tab.
4. Select Migrate MySQL Data.
5. Enter the path to which you want to migrate the data.
6. To retain the existing data directory, check Keep existing data directory.
7. Click Migrate.
Moving MySQL data using the command line

You can use migrate MySQL data directory to a different directory. You can retain the current data directory. You can use the migrate option on the Troubleshooting menu or alternatively, you can use the command line. This procedure describes how to use the command line.

About this task

If you retain the current data directory, it will be kept as a backup and renamed.

You can use the Migrate MySQL Data utility or you can use a `java -jar mysqldatamigrator.jar` option in the OnCommand Insight path of `\bin\mysqldatamigrator` where the following parameters should be used:

- Mandatory parameters
  - `-path`
    - The new data path to which the data folder will be copied.

- Optional parameters
  - `-myCnf <my.cnf file>`
    - The path for the .cnf file. The default is `<install path>\mysql\my.cnf`. Use this flag only if a non-default MySQL is used.
  - `-doBackup`
    - If this flag is set, the current data folder will be renamed but not deleted.

Step

1. Access the command line tool here: `<installation path>\bin\mysqldatamigrator\mysqldatamigrator.jar`

Example usage

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

Forcing annotation updates

If you have changed the annotations and want to use them in reports immediately, use one of the force annotation options.

Steps

1. In the web UI, click Admin and select Troubleshooting.
2. On the bottom of the page, click the Advanced Troubleshooting link.
3. Click the Actions tab.
4. Select one of these options:
   - **Update DWH Annotations** to force the update of annotations in data warehouse to be used for reports.
   - **Update DWH Annotations (incl. deleted)** to force an annotations update (including deleted objects) in the data warehouse to be used for reports.
Configuring Client settings

You can configure options for the OnCommand Insight Java UI Client on the server.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. In the Advanced menu on the next page, click the Advanced Settings tab.
4. In the Acquisition Dynamic Attributes enter the number of hours to ignore dynamic attribute changes.
5. In the Configure Client Settings enter the following information.
   - **Initial Heap Size** is the size of the heap that is created when the VM (Virtual Machine) is started to run the client. This number is used to construct the -Xms<size> parameter to java. Decreasing this number means Java takes up less memory when it starts up. (However, it is then more likely that Java will need to reallocate the heap when it exceeds this number, which is an expensive operation, so you do not want to make this number too small.)
   - **Max Heap Size** is the largest that Java will allow the heap to grow in the VM that is running the client. This number is used to construct the -Xmx<size> parameter to java.
   - **Log Level** controls the amount of detail that is generated in the client logs. There are two possible values:
     - INFO - generates a "normal" amount of information.
     - DEBUG - generates more detailed information to the client log to help with debugging.
6. Configure your data source alerts.
7. Configure the Login Warning Message displayed by the client.
8. Click Save.

Checking the status of server resources

This option displays the OnCommand Insight Server's information including server memory, disk space, OS, and CPU and OnCommand Insight database information including innoDB data size and the disk free space where the database resides.

Steps
1. On the Insight toolbar, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the OnCommand Insight Portal link.
3. On the next page in the Advanced menu, click the Troubleshooting link.
4. Click Server Resources Status.
   - For advanced OnCommand Insight users: The administrator can run some SQL tests to check the database and server's response time from the button at the end of the information summary. This option displays a warning if server resource is low.
Finding ghost data sources

If you have removed a device but the device data remains, you can locate any ghost data sources so that you can remove them.

Steps

1. In the web UI, click Admin and select Troubleshooting.
2. At the bottom of the page in the Other tasks area, click the Advanced Troubleshooting link.
3. On the Reports tab, click the Ghost Data Sources link.

OnCommand Insight produces a list of originators with their device information.

Adding a missing disk model

If acquisition fails due to an unknown disk model, you can add the missing disk model to the new_disk_models.txt file and run acquisition again.

About this task

As part of a poll of a storage device by OnCommand Insight acquisition, the disk models on the storage device are read. If a vendor has added new disk models to their array that Insight doesn't know about, or if there is a mismatch between the model number Insight looks for and the one returned by the storage device, acquisition of that data source will fail with an error. In order to prevent these errors, it is necessary to update the disk model information known to Insight. New disk models are added to Insight with updates, patches and maintenance releases. However, you may decide to update this information manually instead of waiting for a patch or update.

Because OnCommand Insight reads the disk model file every five minutes, any new data model information you enter is updated automatically. You do not need to restart the server for the changes to take effect, but you can opt to restart the server and any remote acquisition units (RAUs) to have the changes take effect before the next update.

Disk model updates are added to the new_disk_models.txt file located in the <SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war directory. Understand the information needed to describe your new disk model before updating the new_disk_models.txt file. Inaccurate information in the file produces incorrect system data and could result in failed acquisition.

Follow these instructions to manually update Insight disk models:

Steps

1. Locate the proper information for your disk model.
2. Using a text editor, open the new_disk_models.txt file.
3. Add the required information for the new data source.
4. Save the file in the <SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war directory on your server.
5. Back up the new_disk_models.txt file to a safe location. During any subsequent OnCommand Insight upgrade, this file will be overwritten. If your disk model information is not present in the upgraded file, you will need to re-enter it.
Locating required information for new disk model

To locate the disk model information, identify the vendor and model number and run an Internet search.

About this task

Locating disk model information is as simple as running an internet search. Be sure to note the vendor name and disk model number before searching.

Steps

1. It is recommended to use an advanced internet search for the vendor, model, and document type “PDF” to find the vendor's data sheet and/or installation guide for the drive. These data sheets are usually the best source for vendor disk information.

2. Vendor specifications do not always provide all of the necessary information based on the full model number. It is often useful to search for different parts of the model number string on the vendor's site to locate all of the information.

3. Locate the disk vendor name, full model number, disk size and speed, and the interface type in order to define the new disk model in OnCommand Insight. You can use the following table as a guide to help note this information as you find it:

<table>
<thead>
<tr>
<th>For this field:</th>
<th>Which is:</th>
<th>Enter this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model number (aka Key)</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Vendor</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Disk speed (RPM)</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Size (in GB)</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Interface Type (select one)</td>
<td>Required</td>
<td>ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, OTHER</td>
</tr>
<tr>
<td>Seek time in ms</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Maximum transfer rate in MB/sec</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Interface transfer rate in MB/sec</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Link to vendor/model information</td>
<td>Optional but recommended</td>
<td></td>
</tr>
</tbody>
</table>

4. Enter that information into the new_disk_models.txt file. See Content of the new_disk_models.txt file on page 198 for format, order, and examples.

Content of the new_disk_models.txt file

The new_disk_models.txt file has required and optional fields. The fields are comma separated, so do not use commas within the fields.

All fields are required except for seek time, transfer rates and additional_info. If available, include the vendor/model website link in the additional_info field.

Using a text editor, enter the following information in this order, separated by commas, for each new disk model you wish to add:
1. **key**: use the model number (required)
2. **vendor**: name (required)
3. **model number**: full number (usually the same value as in "key") (required)
4. **rpm of the disk**: for example 10000 or 15000 (required)
5. **size**: capacity in GB (required)
6. **interface type**: ATA, SATA, FC, SAS, FATA, SSD, OTHER (required)
7. **seek time**: in ms (optional)
8. **potential transfer rate**: the potential transfer rate in MB/sec. Maximum transfer rate of the disk itself. (optional)
9. **interface transfer rate**: the rate to and from the host in MB/sec (optional).
10. **Additional Info**: Any additional information you want to capture. Best practice is to enter the link to the vendor page where the specs are found, for reference (optional)

For any optional fields left blank, be sure to include the comma.

<table>
<thead>
<tr>
<th>Examples (each on one line with no spaces):</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,</td>
</tr>
<tr>
<td>X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,<a href="https://storage.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxy.pdf">https://storage.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxy.pdf</a></td>
</tr>
</tbody>
</table>
Monitoring your environment

Insight helps you to prevent problems in your environment and troubleshoot potential problems quickly.

Asset page data

Asset pages provide performance troubleshooting data and present summary information about a base asset (such as a virtual machine or a volume) and the related assets it uses (such as storage pools, storage nodes, and connected switch ports), with links to additional information.

Beginning with OnCommand Insight 7.3.1, all asset pages have a Main page and an Additional data page. On the Main page are a summary of the asset and different sections for charts, topology and other information. The Additional data page allows you to configure a customizable dashboard page for the current asset type.

A solid red circle next to a line or message on the asset page main tab indicates potential issues with the monitored environment.

Types of asset pages

Asset pages summarize the current status of an asset and contain links to additional information about the asset and its related assets.

OnCommand Insight provides asset pages for the following assets:

- Virtual machine
- Volume
- Internal volume
- Physical host
- Storage pool
- Storage
- Datastore
- Hypervisor
- Application
- Storage node
- Qtree
- Disk
- VMDK
- Port
- Switch
- Fabric
- Object storage (for example, Atmos, Centera, Amazon S3)
- Zone
Mapping and Masking information can be viewed in tables on Zone, Volume, VM, and Host/Hypervisor asset pages.

**Note:** Summary information is available for object storage assets; however, you can only access this information from the Data sources detail page.

**Searching your environment for specific assets**

You can locate information about specific assets by using the search facility. For example, if a system user contacts the storage administrator with a complaint about a particular server, the administrator can search the server name and display an asset page summarizing the status and supplying additional linked information.

**Steps**

1. Open the OnCommand Insight web UI.
2. On the toolbar, click the search icon.
   - The **Search assets** box is displayed.
3. Enter the name of an asset or a portion of the name.
4. Select the resource you want from the search results.
   - The asset page for that resource is displayed.

**Advanced search techniques**

Multiple search techniques can be used to search for data or objects in your monitored environment.

**Wildcard search**

You can perform multiple character wildcard search using the * character. For example, applic*n would return application.

**Phrases used in search**

A phrase is a group of words surrounded by double quotation marks; for example, "PAW VNX LUN 5". You can use double quotes to search for documents that contain spaces in their names or attributes.

**Boolean Operators**

Using Boolean operators, you can combine multiple terms to form a more complex query.

**OR**

- The OR operator is the default conjunction operator.
  - If there is no Boolean operator between two terms, the OR operator is used.
- The OR operator links two terms and finds a matching document if either of the terms exists in a document.
  - For example, “storage OR netapp” searches for documents that contain either “storage” or “netapp”.
- High scores are given to documents that match most of the terms.
AND

You can use the AND operator to find documents in which both the search terms exist in a single document. For example, “aurora AND netapp” searches for documents that contain both “storage” and “netapp”.

You can use the symbol && instead of the word AND.

NOT

When you use the NOT operator, all the documents that contain the term after NOT are excluded from the search results. For example, “storage NOT netapp” searches for documents that contain only “storage” and not “netapp”.

You can use the symbol ! instead of the word NOT.

Prefix and suffix search

- As soon as you start typing a search string, the search engine does a prefix and suffix search to find the best match.
- Exact matches are given a higher score than a prefix or suffix match. The score is calculated based on the distance of the search term from the actual search result. For example, we have three storages: “aurora”, “aurora1”, and “aurora11”. Searching for “aur” will return all three storages. However, the search result for “aurora” will have the highest score because it has the closest distance to the prefix search string.
- The search engine also searches for terms in reverse order, which allows you to perform a suffix search. For example, when you type “345” in the search box, the search engine searches for “345”.
- Search is case-insensitive.

Search using indexed terms

Searches that match more of the indexed terms result in higher scores.

The search string is split into separate search terms by space. For example, the search string “storage aurora netapp” is split into three keywords: “storage”, “aurora”, and “netapp”. The search is performed using all three terms. The documents that match most of these terms will have the highest score. The more information you provide, the better are the search results. For example, you can search for a storage by its name and mode.

The UI displays the search results across categories, with the three top results per category. If you did not find a document that you were expecting, you can include more terms in the search string to improve the search results.

The following table provides a list of indexed terms that can be added to the search string.

<table>
<thead>
<tr>
<th>Category</th>
<th>Indexed terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>• “storage”</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td></td>
<td>• vendor</td>
</tr>
<tr>
<td></td>
<td>• model</td>
</tr>
<tr>
<td>Category</td>
<td>Indexed terms</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| StoragePool    | • “storagepool”  
• name  
• name of the storage  
• IP addresses of the storage  
• serial number of the storage  
• storage vendor  
• storage model  
• names for all associated internal volumes  
• names for all associated disks |
| Internal Volume| • “internalvolume”  
• name  
• name of the storage  
• IP addresses of the storage  
• serial number of the storage  
• storage vendor  
• storage model  
• name of the storage pool  
• names of all associated shares  
• names of all associated applications and business entities |
| Volume         | • “volume”  
• name  
• label  
• names of all internal volumes  
• name of the storage pool  
• name of the storage  
• IP addresses of the storage  
• serial number of the storage  
• storage vendor  
• storage model |
<table>
<thead>
<tr>
<th>Category</th>
<th>Indexed terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Node</td>
<td>• “storagenode”&lt;br&gt;• name&lt;br&gt;• name of the storage&lt;br&gt;• IP addresses of the storage&lt;br&gt;• serialnumber of the storage&lt;br&gt;• storage vendor&lt;br&gt;• storage model</td>
</tr>
<tr>
<td>Host</td>
<td>• “host”&lt;br&gt;• name&lt;br&gt;• IP addresses&lt;br&gt;• names of all associated applications and business entities</td>
</tr>
<tr>
<td>Datastore</td>
<td>• “datastore”&lt;br&gt;• name&lt;br&gt;• virtual center IP&lt;br&gt;• names of all volumes&lt;br&gt;• names of all internal volumes</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>• “virtualmachine”&lt;br&gt;• name&lt;br&gt;• DNS name&lt;br&gt;• IP addresses&lt;br&gt;• name of the host&lt;br&gt;• IP addresses of the host&lt;br&gt;• names of all datastores&lt;br&gt;• names of all associated applications and business entities</td>
</tr>
<tr>
<td>Category</td>
<td>Indexed terms</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Switches (regular and NPV)</td>
<td>• “switch”</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• wwn</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td></td>
<td>• serial number</td>
</tr>
<tr>
<td></td>
<td>• model</td>
</tr>
<tr>
<td></td>
<td>• domain ID</td>
</tr>
<tr>
<td></td>
<td>• name of the fabric</td>
</tr>
<tr>
<td></td>
<td>• wwn of the fabric</td>
</tr>
<tr>
<td>Application</td>
<td>• “application”</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td></td>
<td>• tenant</td>
</tr>
<tr>
<td></td>
<td>• line of business</td>
</tr>
<tr>
<td></td>
<td>• business unit</td>
</tr>
<tr>
<td></td>
<td>• project</td>
</tr>
<tr>
<td>Tape</td>
<td>• “tape”</td>
</tr>
<tr>
<td></td>
<td>• IP address</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td></td>
<td>• serial number</td>
</tr>
<tr>
<td></td>
<td>• vendor</td>
</tr>
<tr>
<td>Port</td>
<td>• “port”</td>
</tr>
<tr>
<td></td>
<td>• wwn</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
<tr>
<td>Fabric</td>
<td>• “fabric”</td>
</tr>
<tr>
<td></td>
<td>• wwn</td>
</tr>
<tr>
<td></td>
<td>• name</td>
</tr>
</tbody>
</table>

**Determining data source acquisition status**

Because data sources are the primary source of information for Insight, it is imperative that you ensure that they remain in a running state.
The ability to see the data source acquisition status is available on every asset page for all assets that are directly acquired. Either of the following acquisition scenarios can occur, in which the status is displayed in the upper right corner of the asset page:

- Acquired successfully from data source
  Displays the status “Acquired xxxxx”, where xxxxx indicates the most recent acquisition time of the asset's data sources.

- There is an acquisition error.
  Displays the status “Acquired xxxxx”, where xxxxx indicates the most recent acquisition time of the asset's one or more data sources with 📦. When you click 📦, a window displays each data source for the asset, the data source's status, and the last time data was acquired. Clicking a data source displays the data source's detail page.

If an asset is not directly acquired, no status is displayed.

Asset page sections

An asset page displays several sections containing information relevant to the asset. The sections that you see depend on the type of asset.

Summary

The Summary section on an asset page displays a summary of information about the particular asset and shows issues related to the asset, indicated by a red circle, with hyperlinks to additional information about related assets and to any performance policies assigned to the asset.

The following example shows some of the types of information available in the Summary section of an asset page for a virtual machine. Any item with a solid red circle next to it indicates potential issues with the monitored environment.
Using the Summary section

You can view the Summary section to see general information about an asset. Specifically, it is helpful to see if any metrics (for example, memory, capacity, and latency) or any performance policies are cause for concern, which OnCommand Insight indicates by displaying a red circle next to the metric or performance policy.

Steps

1. Log in to the OnCommand Insight web UI.

2. Locate an asset page by doing either of the following:
   
   • On the Insight toolbar, click 🔍, type in the name of the asset, and then select the asset from the list.

   • Click Dashboards, select Assets Dashboard, locate an asset name, and click it.

   The asset page displays.

   Note: The information that displays in the Summary section depends on the type of asset page you are viewing.

3. You can click any of the asset links to view their asset pages.

   For example, if you are viewing a storage node, you can click a link to view the asset page of the storage it is associated with or click to view the asset page of the HA partner.

4. You can view the metrics associated with the asset.
A red circle next to a metric indicates that you might need to diagnose and resolve potential problems.

**Note:** You may notice that volume capacity might show greater than 100% on some storage assets. This is due to metadata related to the capacity of the volume being part of the consumed capacity data reported by the asset.

5. If applicable, you can click a performance policy link to view the performance policy or policies associated with the asset.

   If a red circle appears next to a performance policy, this indicates an asset has crossed the performance policy’s defined threshold. You should examine the performance policy to further diagnose the issue.

**Topology**

The Topology section, if applicable to an asset, enables you to see how a base asset is connected to its related assets.

The following shows an example of what might display in the Topology section of a virtual machine asset page.

![Topology Diagram]

If the topology for the asset is larger than will fit in the section, the **Click link to see the topology** hyperlink is displayed instead.

**Using the Topology section**

The Topology section enables you to view how the assets in your network are connected to each other and display information about related assets.

**Steps**

1. Log in to the OnCommand Insight web UI.

2. Locate an asset page by doing either of the following:

   - On the Insight toolbar, click **Q** and type in the name of the asset, and then select the asset from the list.
   - Click **Dashboards**, select **Assets Dashboard**, locate an asset name, and click it.

   The asset page displays. You can find the Topology section in the upper right-hand corner of the asset page.

   If the topology for the asset is larger than will fit in the section, click the **Click link to see the topology** hyperlink.

3. To view more information about the base asset’s related assets, position your cursor over a related asset in the topology and click its name, which displays its asset page.
User Data

The User Data section of an asset page displays and enables you to change any user-defined data such as applications, business entities, and annotations.

The following shows an example of what might display in the User Data section of a virtual machine asset page when an application, business entity, and annotation are assigned to the asset:

Using the User Data section to assign or modify applications

You can assign applications running in your environment to certain assets (host, virtual machines, volumes, internal volumes, and hypervisors). The User Data section enables you to change the application assigned to an asset or assign an application or additional applications to an asset.

Steps

1. Log in to the OnCommand Insight web UI.
2. Locate an asset page by doing either of the following:
   - On the Insight toolbar, click , type in the name of the asset, and then select the asset from the list.
   - Click Dashboards, select Assets Dashboard, locate an asset name, and click it.

The asset page displays.
3. You can do the following:
   - To view the asset page for the application, click the application's name.
   - To change the application assigned or to assign an application or additional applications, position your cursor over the application name, if an application is assigned, or over None, if no application is assigned, click , type to search for an application or select one from the list, and then click .

If you choose an application that is associated with a business entity, the business entity is automatically assigned to the asset. In this case, when you place your cursor over the business entity name, the word derived displays. 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.

   - To remove an application, click .
**Using the User Data section to assign or modify business entities**

You can define business entities to track and report on your environment data at a more granular level. The User Data section in an asset page enables you to change the business entity assigned to an asset or remove a business entity from an asset.

**Steps**

1. Log in to the OnCommand Insight web UI.
2. Locate an asset page by doing either of the following:
   - On the Insight toolbar, click ![search](search_icon), type in the name of the asset, and then select the asset from the list.
   - Click **Dashboards**, select **Assets Dashboard**, locate an asset name, and click it.

   The asset page displays.
3. You can do the following:
   - To change the entity assigned or to assign an entity, click ![edit](edit_icon) and select an entity from the list.
   - To remove a business entity, click ![remove](remove_icon).

   **Note:** You cannot remove an entity that is derived from an application that is assigned to the asset.

**Using the User Data section to assign or modify annotations**

When customizing OnCommand Insight to track data for your corporate requirements, you can define specialized notes, called *annotations*, and assign them to your assets. The User Data section of an asset page displays annotations assigned to an asset and also enables you to change the annotations assigned to that asset.

**Steps**

1. Log in to the OnCommand Insight web UI.
2. Locate an asset page by doing either of the following:
   - On the Insight toolbar, click ![search](search_icon), type in the name of the asset, and then select the asset from the list.
   - Click **Dashboards**, select **Assets Dashboard**, locate an asset name, and click it.

   The asset page displays.
3. In the **User Data** section of the asset page, click ![add](add_icon).

   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**.
The annotation is assigned to the asset. You can later filter assets by annotation using a query. If you want to group assets by annotations, you must use the Java UI.

7. If you want to change the value of the annotation after you assign it, click \[\text{_modify_annotation}\] 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.

### Anomalies

The Anomalies section, which displays only on an application asset page when the anomaly detection engine is installed, enables you to identify the normal operating workload range for an application and identify when changes in performance are outside of expected levels.

Anomaly analysis provides proactive visibility into the infrastructure supporting business critical applications and informs you of performance anomalies before they become service disruptions. The application anomaly detection engine ingests performance metrics collected by Insight and identifies anomalies in the application infrastructure. Anomalies are items, events or observations that do not conform to an expected pattern or other items. You use anomaly detection to:

- Monitor selected critical applications.
- Identify significant changes in the application infrastructure behavior.
- Track an application through the entire stack and across multiple counters.
- Diagnose the cause of periodically recurring events in an application workload.
- Provide a more comprehensive set of information compared to data from performance counters using static threshold values.
- Improved reactive mode monitoring with end to end view of the topology and the ability to focus on the most anomalous behaviors in a data set.

### Using the Anomalies section

The Anomalies section, which displays only on an application asset page, provides insight into the application infrastructure and enables you to identify abnormal behaviors that could result in service disruptions.

### Steps

1. Turn anomaly monitoring on for the desired application and allow it to collect data.

2. While the anomaly detection engine is running, you can view the following information in the **Anomalies** section of the application asset page:

   - The anomaly detection score is shown by a blue bar, representing a score between 0 and 100. Scoring is performed resource-by-resource and counter-by-counter resulting in an overall significance score for the entire application infrastructure.

   - Application assets view
     Located below the anomaly detection score, this shows how all the assets contribute to the current anomaly score. If an asset is not contributing significantly to the anomaly score, it is represented by \[\text{no_contribution}\]. If the asset is contributing to the significance of the anomaly score, either 1, 2, or three blue bars appear, for example, \[\text{one_blue_bar}\]. The values represented by the number of bars indicate the significance of that asset’s contribution to the anomaly score as follows: 1 bar = 1-33; 2 bars = 34-67; 3 bars = 68-100.
Assets that are assigned to an application (hosts, virtual machines, volumes, internal volumes, and hypervisors) and also assets in the infrastructure that are somehow connected to the assigned assets (for example, nodes, ports, and so on) contribute to the anomaly detection score. Both assets that contribute and those that do not contribute to the specific anomaly are displayed, because the data from the assigned application resources may flow through them. If there are more than 60 assets of one type, the More button displays, which you can click to display the remaining assets. That status of those remaining assets, for example, , appears next to the More button. This example indicates that of a total of 129 assets not shown, 124 of those assets did not contribute to the anomaly score; however, five of those assets did contribute some level of significance to the anomaly score.

- Anomaly graph

The anomaly graph displays the highest anomaly score, indicated by the orange circle, for the time range (3 hours, 24 hours, 3 days, 7 days, 30 days, or a custom time range) selected for the application asset page. You can drag your pointer over the chart to see the anomaly scores, indicated by a blue circle, for other points during the time range and then click the blue circle, which will update the application assets view to display the assets that contributed to the score at that point in time.

3. To aid you in troubleshooting asset performance, you can add an asset from the application assets view to the expert view chart in the application asset page by doing the following:
   a. Click an asset icon in the applications assets view.
      
      The following displays: The name of the asset, which is a hyperlink to its asset page, the metric that contributed to the anomaly, the significance of the asset’s contribution, and a button that enables you to add the asset to the expert view chart.
      
   b. Click .
      
      The asset is added to the expert view chart.

Expert view

The Expert View section of an asset page enables you to view a performance sample for the base asset based on any number of applicable metrics in context with a chosen time period (3 hours, 24 hours, 3 days, 7 days, or a custom time period) in the performance chart and any assets related to it.

The following is an example of the Expert View section in a volume asset page:

You can select the metrics you want to view in the performance chart for the time period selected. The Resources section shows the name of the base asset and the color representing the base asset in the performance chart. If the Top Correlated section does not contain an asset you want to view in the performance chart, you can use the Search assets box in the Additional resources section to locate the asset and add it to the performance chart. As you add resources, they appear in the Additional resources section.
Also shown in the Resources section, when applicable, are any assets related to the base asset in the following categories:

- **Top correlated**
  Shows the assets that have a high correlation (percentage) with one or more performance metrics to the base asset.

- **Top contributors**
  Shows the assets that contribute (percentage) to the base asset.

- **Greedy**
  Shows the assets that take away system resources from the asset through sharing the same resources, such as hosts, networks, and storage.

- **Degraded**
  Shows the assets that are depleted of system resources due to this asset.

**Expert View metric definitions**

The Expert View section of an asset page displays several metrics based on the time period selected for the asset. Each metric is displayed in its own performance chart. You can add or remove metrics and related assets from the charts depending on what data you want to see.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BB credit zero Rx, Tx</td>
<td>Number of times the receive/transmit buffer-to-buffer credit count transitioned to zero during the sampling period. This metric represents the number of times the attached port had to stop transmitting because this port was out of credits to provide.</td>
</tr>
<tr>
<td>BB credit zero duration Tx</td>
<td>Time in milliseconds during which the transmit BB credit was zero during the sampling interval.</td>
</tr>
<tr>
<td>Cache hit ratio (Total, Read, Write) %</td>
<td>Percentage of requests that result in cache hits. The higher the number of hits versus accesses to the volume, the better is the performance. This column is empty for storage arrays that do not collect cache hit information.</td>
</tr>
<tr>
<td>Cache utilization (Total) %</td>
<td>Total percentage of cache requests that result in cache hits</td>
</tr>
<tr>
<td>Class 3 discards</td>
<td>Count of Fibre Channel Class 3 data transport discards.</td>
</tr>
<tr>
<td>CPU utilization (Total) %</td>
<td>Amount of actively used CPU resources, as a percentage of total available (over all virtual CPUs).</td>
</tr>
<tr>
<td>CRC error</td>
<td>Number of frames with invalid cyclic redundancy checks (CRCs) detected by the port during the sampling period</td>
</tr>
<tr>
<td>Frame rate</td>
<td>Transmit frame rate in frames per second (FPS)</td>
</tr>
<tr>
<td>Frame size average (Rx, Tx)</td>
<td>Ratio of traffic to frame size. This metric enables you to identify whether there are any overhead frames in the fabric.</td>
</tr>
<tr>
<td>Frame size too long</td>
<td>Count of Fibre Channel data transmission frames that are too long.</td>
</tr>
<tr>
<td>Frame size too short</td>
<td>Count of Fibre Channel data transmission frames that are too short.</td>
</tr>
<tr>
<td>I/O density (Total, Read, Write)</td>
<td>Number of IOPS divided by used capacity (as acquired from the most recent inventory poll of the data source) for the Volume, Internal Volume or Storage element. Measured in number of I/O operations per second per TB.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IOPS (Total, Read, Write)          | Number of read/write I/O service requests passing through the I/O channel or a portion of that channel per unit of time (measured in I/O per sec) |}
| IP throughput (Total, Read, Write) | Total: Aggregated rate at which IP data was transmitted and received in megabytes per second.  
Read: IP Throughput (Receive): Average rate at which IP data was received in megabytes per second.  
Write: IP Throughput (Transmit): Average rate at which IP data was transmitted in megabytes per second. |}
| Latency (Total, Read, Write)       | Latency (R&W): Rate at which data is read or written to the virtual machines in a fixed amount of time.  
The value is measured in megabytes per second.  
Latency: Average response time from the virtual machines in a data store.  
Top Latency: The highest response time from the virtual machines in a data store. |}
| Link failure                       | Number of link failures detected by the port during the sampling period. |
| Link reset Rx, Tx                   | Number of receive or transmit link resets during the sampling period.  
This metric represents the number of link resets that were issued by the attached port to this port. |}
| Memory utilization (Total) %       | Threshold for the memory used by the host. |
| Partial R/W (Total) %              | Total number of times that a read/write operation crosses a stripe boundary on any disk module in a RAID 5, RAID 1/0, or RAID 0 LUN.  
Generally, stripe crossings are not beneficial, because each one requires an additional I/O. A low percentage indicates an efficient stripe element size and is an indication of improper alignment of a volume (or a NetApp LUN).  
For CLARiiON, this value is the number of stripe crossings divided by the total number of IOPS. |}
| Port errors                        | Report of port errors over the sampling period/given time span. |
| Signal loss count                  | Number of signal loss errors.  
If a signal loss error occurs, there is no electrical connection, and a physical problem exists. |}
| Swap rate (Total Rate, In rate, Out rate) | Rate at which memory is swapped in, out, or both from disk to active memory during the sampling period. This counter applies to virtual machines. |}
| Sync loss count                    | Number of synchronization loss errors.  
If a synchronization loss error occurs, the hardware cannot make sense of the traffic or lock onto it. All the equipment might not be using the same data rate, or the optics or physical connections might be of poor quality.  
The port must resynchronize after each such error, which impacts system performance. Measured in KB/sec. |}
<p>| Throughput (Total, Read, Write)    | Rate at which data is being transmitted, received, or both in a fixed amount of time in response to I/O service requests (measured in MB per sec). |</p>
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout discard frames - Tx</td>
<td>Count of discarded transmit frames caused by timeout.</td>
</tr>
<tr>
<td>Traffic rate (Total, Read, Write)</td>
<td>Traffic transmitted, received, or both received during the sampling period, in mebibytes per second.</td>
</tr>
<tr>
<td>Traffic utilization (Total, Read, Write)</td>
<td>Ratio of traffic received/transmitted/total to receive/transmit/total capacity, during the sampling period.</td>
</tr>
<tr>
<td>Utilization (Total, Read, Write) %</td>
<td>Percentage of available bandwidth used for transmission (Tx) and reception (Rx).</td>
</tr>
<tr>
<td>Write pending (Total)</td>
<td>Number of write I/O service requests that are pending.</td>
</tr>
</tbody>
</table>

**Using the Expert View section**

The Expert view section enables you to view performance charts for an asset based on any number of applicable metrics during a chosen time period, and to add related assets to compare and contrast asset and related asset performance over different time periods.

**Steps**

1. Log in to the OnCommand Insight web UI.
2. Locate an asset page by doing either of the following:
   - On the Insight toolbar, click ☰, type in the name of the asset, and then select the asset from the list.
   - Click **Dashboards**, select **Assets Dashboard**, locate an asset name, and click it.

The asset page displays. By default, the performance chart shows two metrics for time period selected for the asset page. For example, for a storage, the performance chart shows latency and total IOPS by default. The Resources section displays the resource name and an Additional resources section, which enables you to search for assets. Depending on the asset, you might also see assets in the Top correlated, Top contributor, Greedy, and Degraded sections.

3. You can click **Select metrics to show**, and select a metric to add a performance chart for a metric.
   A performance chart is added for the selected metric. The chart displays the data for the selected time period. You can change the time period by clicking on another time period in the top left-hand corner of the asset page.
   You can perform the step again, and click to clear a metric. The performance chart for the metric is removed.

4. You can position your cursor over the chart and change the metric data that displays by clicking either of the following, depending on the asset:
   - **Read** or **Write**
   - **Tx** or **Rx**

   **Total** is the default.

5. You can drag your cursor over the data points in the chart to see how the value of the metric changes over the time period selected.

6. In the **Resources** section, you can do any of the following, if applicable, to add any related assets to the performance charts:
• You can select a related asset in the Top correlated, Top contributors, Greedy, or Degraded sections to add data from that asset to the performance chart for each selected metric. Assets must have a minimum 15% correlation or contribution to be shown. After you select the asset, a color block appears next to the asset to denote the color of its data points in the chart.

• For any asset shown, you can click the asset name to display its asset page, or you can click the percentage that the asset correlates or contributes to the base asset to view more information about the assets relation to the base asset. For example, clicking the linked percentage next to a top correlated asset displays an informational message comparing the type of correlation that asset has with the base asset.

• If the Top correlated section does not contain an asset you want to display in a performance chart for comparison purposes, you can use the Search assets box in the Additional resources section to locate other assets.

After you select an asset, it displays in the Additional resources section. When you no longer want to view information about the asset, click 

Related Assets

If applicable, an asset page displays a Related Assets section. For example, a volume asset page might show information about assets like Storage Pools, Connected switch ports, and Compute Resources. Each section comprises a table that lists any of the related assets in that category, with links to their respective asset pages, and several performance statistics related to the asset.

Using the Related Assets section

The Related Assets section enables you to view any of the assets that are related to the base asset. Each related asset is displayed in a table along with pertinent statistics for the asset. You can export the asset information, view the asset statistics in the Expert View performance charts, or show a chart that displays statistics for only related assets.

Steps

1. Log in to the OnCommand Insight web UI.

2. Locate an asset page by doing either of the following:

   • On the Insight toolbar, click , type in the name of the asset, and then select the asset from the list.
   • Click Dashboards, select Assets Dashboard, locate an asset name, and click it.

   The asset page displays.

3. To control how assets display in the table:

   • Click the name of any asset to display its asset page.
   • Use the filter box to show only specific assets.
   • Click a page number to browse through the assets by page if there are more than five assets in the table.
   • Change the sort order of the columns in a table to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.
   • Add a related asset to any performance chart in the Expert View section by placing your cursor over the related asset and clicking .
4. To export the information displayed in the table to a .CSV file:
   a. Click .
   b. Click Open with and then OK to open the file with Microsoft Excel and save the file to a specific location, or click Save file and then OK to save the file to your Downloads folder.
      All of the object attributes for the columns currently selected for display are exported to the file. Only the attributes for the displayed columns will be exported. Note that only the first 10,000 rows of the table are exported.

5. To display the related asset information in a chart below the table, click and do any of the following:
   - Click Read, Write, or Total to change the metric data that displays. Total is the default.
   - Click to select a different metric.
   - Click to change the chart type. Line chart is the default.
   - Move your cursor over the data points in the chart to see how the value of the metric changes over the time period selected for each related asset.
   - Click a related asset in the chart legend to add it to or remove it from the chart.
   - Click a page number in the related asset table to view other related assets in the chart.
   - Click to close the chart.

Violations

You can use the Violations section of an asset page to see the violations, if any, that occur in your environment as a result of a performance policy assigned to an asset. Performance policies monitor your network thresholds and enable you to 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.

The following example shows a Violations section that displays on an asset page for a hypervisor:

Using the Violations section

The Violations section enables you to view and manage any of the violations that occur in your network as the result of a performance policy assigned to an asset.

Steps

1. Log in to the OnCommand Insight web UI.
2. Locate an asset page by doing either of the following:
   - On the Insight toolbar, click , type in the name of the asset, and then select the asset from the list.
   - Click Dashboards, select Assets Dashboard, locate an asset name, and click it.
The asset page displays. The Violations section displays the time the violation occurred and a description of the threshold that was crossed, along with a hyperlink to the asset on which the violation occurred (for example “2 violations for ds-30 with Latency - Total > 50”).

3. You can perform any of the following optional tasks:
   - Use the **filter** box to show only specific violations.
   - Click a page number to browse through the violations by page if there are more than five violations in the table.
   - Change the sort order of the columns in a table to either ascending (up arrow) or descending (down arrow) by clicking the arrow in the column header.
   - Click the asset name in any description to display its asset page; a red circle indicates issues that need further investigation. You can click the performance policy, which displays the Edit Policy dialog box, to review the performance policy and make changes to the policy if necessary.
   - Click ⌫ to remove a violation from the list if you determine the issue is no longer a cause for concern.

### Customizable asset page

Additional data can be displayed in customizable widgets on each asset page. Customizing the page for an asset applies the customization to the pages for all assets of that type.

You customize asset page widgets by performing the following actions:

1. Add a widget to the page
2. Create a query or expression for the widget to showcase desired data
3. Choose a filter if desired
4. Choose a rollup or grouping method
5. Save the widget
6. Repeat for all desired widgets
7. Save the asset page

You can also add variables to the custom asset page that can be used to further refine your showcased data in widgets. In addition to regular variables, each asset type can use a set of "$this" variables to quickly identify resources directly related to the current asset, for example, all virtual machines hosted by the same hypervisor that hosts the current virtual machine.

This custom asset page is unique for each user as well as for each asset type. For example, if User A creates a custom asset page for a virtual machine, that custom page will display for any virtual machine asset page, for that user.

Users can only view, edit, or delete custom asset pages that they create.

Custom asset pages are not included in Insight's export/import functionality.
Understanding "$this" variables

Special variables on an asset's "Additional data" customizable page allow you to easily showcase additional information that is directly related to the current asset.

About this task

To use the “$this” variables in widgets on your asset's customizable landing page, follow the steps below. For this example, we will add a table widget.

Note: “$this” variables are only valid for an asset's customizable landing page. They are not available for other Insight dashboards. The available “$this” variables varies according to asset type.

Steps

1. Navigate to an asset page for an asset of your choosing. For this example, let's choose a Virtual Machine (VM) asset page. Query or search for a VM and click on the link to go to that VM's asset page.

   The asset page for the VM opens.

2. Click on the Change view: > Additional Virtual Machine data drop-down to go to that asset's customizable landing page.

3. Click on the Widget button and choose Table widget.

   The Table widget opens for editing. By default, all storages are shown in the table.

4. We want to show all virtual machines. Click on the asset selector and change Storage to Virtual Machine.

   All virtual machines are now shown in the table.

5. Click on the Column selector button and add the hypervisor name field to the table.

   The hypervisor name is shown for each VM in the table.

6. We only care about the hypervisor that hosts the current VM. Click on the Filter by field's + button and select hypervisor name.

7. Click on Any and select the $this.host.name variable. Click the check button to save the filter.
8. The table now shows all the VM's hosted by the current VM's hypervisor. Click **Save**.

**Result**

The table that you created for this virtual machine asset page will be displayed for any VM asset page you display. The use of the `$this.host.name` variable in the widget means that only the VM's owned by the current asset's hypervisor will be displayed in the table.

**Balancing network resources**

To resolve balancing issues, use the asset pages to find the problems and identify high capacity volumes that are underused.

**Steps**

1. Open the Assets Dashboard in your browser.
2. In the Virtual Machines IOPS heat map, you notice the name of a VM in very large print that often reports problems.
3. Click the VM name to display the asset page.
4. Check for error messages in the summary.
5. Check the performance charts and particularly the top correlated resources to locate any volumes that might be in contention.
6. Add volumes to the performance chart to compare the patterns of activity and display more asset pages for other resources involved in the problem.
7. Scroll to the bottom of the asset page to see lists of all of the resources associated with the VM. Note any VMDKs running at high capacity. This is likely causing the contention.
8. To resolve the balancing problem, identify a resource that is under-utilized to receive the load from an over-utilized resource or remove a less demanding application from the heavily used resource.
Examining network performance

You can examine your storage environment performance and identify under-utilized and over-utilized resources and identify risks before they turn into problems.

Insight helps you to resolve or prevent performance and availability problems that are revealed through the collected storage data.

You can use Insight to perform these performance management tasks:

- Monitor performance across your environment
- Identify resources influencing the performance of other devices

Analyzing slow PC performance

If you receive calls from network users complaining that their computers are running slowly, you need to analyze host performance and identify the affected resources.

Before you begin

In this example, the caller gave the host name.

Steps

1. Open Insight in your browser.
2. Enter the host name in the Search assets box and click the host name in the search results. The asset page for the resource opens.
3. On the asset page for the host, examine the performance charts in the center of the page. You might want to show different types of data in addition to the Latency and IOPS that are usually pre-selected. Click the check boxes for other types of data, such as Throughput, Memory, CPU, or IP Throughput depending on the device type.
4. To display a description of a point on a chart, position the mouse pointer over the point.
5. You might also want to change the time range with the selection at the top of the page to be 3 hours up to 7 days or All of the available data.
6. Examine the list of Top correlated resources to see if there are other resources with the same pattern of activity as the base resource.
   a. Click a linked percentage beside a correlated resource to see if the correlated activity pattern is for IOPS or CPU for the base resource and another resource.
   b. Click the check box for a correlated resource to add its data to the performance charts.
   c. Click the linked name of the correlated resource to display its asset page.
7. For a VM, as in this example, locate the storage pool in the Top correlated resources and click the storage pool name.
Analyzing correlated resources

When you are researching performance problems and you open the asset page for a device, you should use the Top correlated resources list to refine data displayed in the performance charts. A resource with a high percentage indicates that resource has similar activity to the base resource.

About this task

You are investigating a performance problem and opened the asset page for a device.

Steps

1. In the Top correlated resources list, the first resource is the base resource. The correlated resources in the list are ranked by percentage of correlated activity to the first device. Click the linked percentage of correlation to see the details. In this example, the 70% correlation is in Utilization, so both the base resource and this correlated resource have equally high utilization.

   ![Correlation Chart]

2. To add a correlated resource to the performance charts, select the check box in the Top correlated resources list for the resource you want to add. By default each resource provides the Total data available, but you can select only Read or only Write data from the menu on the check box.

   Each resource in the charts has a different color so that you can compare the performance measurements for each resource. Only the appropriate type of data is plotted for the selected measurement metrics. For example, CPU data does not include Read or Write metrics, so only Total data is available.

3. Click the linked name of the correlated resource to display its asset page.

4. If you do not see a resource listed in the Top correlated resources that you believe should be considered in the analysis, you can use the Search assets box to find that resource.
Fibre Channel environment monitoring

Using OnCommand Insight's Fibre Channel asset pages, you can monitor the performance and inventory of the fabrics in your environment and be aware of any changes that might cause issues.

Fibre Channel asset pages

Insight's asset pages present summary information about the resource, its topology (the device and its connections), performance charts, and tables of associated resources. You can use the fabric, switch, and port asset pages to monitor your Fibre Channel environment. Particularly helpful when troubleshooting a Fibre Channel issue is the performance chart for each port asset, which shows the traffic for the selected top contributor port. Additionally, you can also show buffer-to-buffer credit metrics and port errors in this chart, with Insight displaying a separate performance chart for each metric.

Performance policies for port metrics

Insight enables you to create performance policies to monitor your network for various thresholds and to raise alerts when those thresholds are crossed. You can create performance polices for ports based on available port metrics. 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.

Time-to-live (TTL) and downsampled data

Starting with OnCommand Insight 7.3, data retention or time-to-live (TTL) has been increased from 7 to 90 days. Because that means much more data is processed for charts and tables and the potential for tens of thousands of datapoints, data is downsampled before being displayed.

Downsampling provides a statistical approximation of your data in charts, giving you an efficient overview of data without having to display every data point, while maintaining an accurate view of your collected data.

Why is downsampling needed?

Insight 7.3 increases the time-to-live (TTL) for data to 90 days. This means an increase in the amount of processing needed to prepare data for display in charts and graphs. In order to allow charts to display quickly and efficiently, data is downsampled in a manner that keeps the overall shape of a chart without needing to process every single data point for that chart.

Note: No actual data is lost during downsampling. You can choose to view actual data for your chart instead of downsampled data by following the steps illustrated below.

How downsampling works

Data is downsampled under the following conditions:

- When your selected time range includes 7 days of data or less, no downsampling occurs. Charts display actual data.
- When your selected time range includes more than 7 days of data but less than 1,000 data points, no downsampling occurs. Charts display actual data.
- When your selected time range includes more than 7 days of data and more than 1,000 data points, data is downsampled. Charts display approximated data.
The following examples show downsampling in action. The first illustration shows latency and IOPS charts on a Datastore asset page for a 24-hour period, as shown by selecting 24h on the asset page's time selector. You can also see the same data by selecting Custom and setting the time range to the same 24-hour period.

Since we are choosing a time range of less than 7 days and we have less than 1,000 data points to chart, the data displayed is actual data. No downsampling occurs.

However, if you are viewing data by choosing either 30d on the asset page time selector, or by setting a custom time range of more than 7 days (or in the event that Insight has collected more than 1,000 data samples for the time period chosen), the data is downsampling before being displayed. When you zoom in on a downsampling chart, the display continues to show the approximated data.

**Note:** When you zoom in on a downsampling chart, the zoom is a digital zoom. The display continues to show the approximated data.

You can see this in the following illustration, where the time range is first set to 30d, and the chart is then zoomed in to show the same 24-hour period as above.
The downsampled charts are showing the same 24-hour period as the “actual” charts above, so the lines follow the same general shape, allowing you to quickly spot interesting peaks or valleys in your performance data.

**Note:** Due to the way data is approximated for downsampling, chart lines may be off slightly when comparing downsampled vs. actual data, to allow for better alignment in the graphs. However, the difference is minimal and does not affect the overall accuracy of the data displayed.

**Violations on downsampled charts**

When viewing downsampled charts, be aware that violations are not shown. To see violations, you can do one of two things:

- View the actual data for that time range by selecting Custom in the asset page time selector, and entering a range of time less than 7 days. Hover over each red dot. The tooltip will show the violation that occurred.
- Note the time range and find the violation(s) in the Violation Dashboard.

**Pruning of inventory history**

Starting with version 7.3.2, Insight keeps inventory (foundation) change history for 90 days. Previous versions of Insight kept all inventory change history from the time of installation. Following an upgrade from an older version of Insight, older inventory history is pruned down to and then kept at 90 days.

After upgrading to the current version of OnCommand Insight, history is pruned to the most recent 90 days. Insight prunes the history in 30-day chunks occurring once a day, starting with the oldest, until 90 days’ worth of history remains. Then, history is pruned daily, to keep only 90 days’ worth of inventory change history.
NAS path for VMs

OnCommand Insight 7.3 supports NAS paths for Virtual Machines to storage shares. These paths are similar to NAS paths for hosts to storage shares. When a VM’s IP address is allowed to access a share, a NAS path is created.

NAS paths for virtual machines are displayed on the Internal Volumes landing page. This page contains a Guest Mounted Storage Resources widget which identifies the Internal Volumes that VMs have access to.

- NAS paths are created when virtual machines have access to the backend shares. There is no acknowledgment of whether the virtual machines access the shares or not.
- Correlation calculation is based on latencies and IOPs, and do not include cases where VMs have NAS paths to the backend storage.
- User can query the share by initiator IP address, but querying by path is not supported.

The Compute Resources table of the Internal Volume now also displays VM’s with NAS paths. For each VM, CPU and memory, utilization and performance data is provided.

Data warehouse impact

Changes to the Data Warehouse that are present after upgrading to OnCommand Insight 7.3 include the following:

- The dwh_inventory.nas_logical table is removed from the Inventory data mart and replaced with a view.
  Any Insight 7.2.x reports containing the NFS path table are preserved.
- The dwh_inventory.nas_cr_logical table is added to the Inventory data mart and includes the following:
  - Compute resource
  - Internal volume
  - Storage
  - NAS share

Capacity as Time Series

With OnCommand Insight 7.3.1, capacity information is reported and charted as time series data.

Previously, capacity information acquired from data sources has been exclusively "point-in-time" (PIT) data, meaning it could not be used in charts as time series data. Now, capacity values for assets can be used as time series data in the following ways:

- Graphed in tables, widgets, expert views, and any place where time series data is displayed
- Applied to performance thresholds with violations using existing semantics
- Used in expressions with other performance counters where appropriate

Note that if you upgrade from a previous version of Insight, previous PIT capacity values used in queries or in filters for custom dashboards will be replaced with time series capacity data. This may result in small changes in the way that capacity data is reported or filtered when compared to the equivalent data in previous Insight versions.
Copyright

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—
graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an
electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and
disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR
IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE,
WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice.
NetApp assumes no responsibility or liability arising from the use of products described herein,
except as expressly agreed to in writing by NetApp. The use or purchase of this product does not
convey a license under any patent rights, trademark rights, or any other intellectual property rights of
NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents,
or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to
NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable,
worldwide, limited irrevocable license to use the Data only in connection with and in support of the
U.S. Government contract under which the Data was delivered. Except as provided herein, the Data
may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written
approval of NetApp, Inc. United States Government license rights for the Department of Defense are
limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
# Index

"$this" variables
- on asset pages 219

**A**
- accessing
  - Violations Dashboard 185
  - web UI 11
- acquisition
  - recordings for Support 189
  - restarting units 186, 191
- acquisition failure
  - missing disk model 197
- acquisition unit
  - introduction 8
- acquisition units
  - monitoring health of 178
- Additional data
  - on asset pages 218
- administrators
  - changing user passwords 21
  - experience level 9
  - permissions 16
- Amazon AWS EC2
  - data source 98
- annotation
  - assigning to assets 80
  - data source tags 155
- annotation rules
  - deleting 78
  - modifying 77
  - predefined storage tiers 76
  - setting for automatic annotation assignment 75
  - setting precedence 77
- annotations
  - asset pages 210
  - assigning 210
  - assigning costs to 72
  - assigning multiple, using queries 86
  - assignment of 71
  - configuring tier rules for automatic assignment 76
  - creating custom 72
  - default annotation rules 76
  - default types 69
  - defining 69
  - definition and purpose 69
  - deleting 75
  - importing 78
  - importing and exporting 91
  - manually assigning to assets 74
  - modifying 74, 210
  - predefined storage tiers 76
  - removing multiple, using queries 86
  - updating changes for reports 195
  - using the User Data section to assign or modify 210
  - viewing on an asset page 210

**Anomalies section**
- on asset pages 63, 211
- anomaly detection
  - about 61
  - enabling 62
  - introduction 8
  - monitoring status 64
- anomaly detection engine
  - monitoring health of 178
- application
  - enabling anomaly detection for 62
- applications
  - assigning to assets 58, 209
  - defining 57
  - deleting 59
  - editing 58
- AR
  - introduction 160
- AR rules
  - getting started 161
- architecture
  - OnCommand Insight 8
- archive
  - enabling 51
  - loading 51
- archiving
  - performance data, daily 50
- asset page
  - Topology section 208
- asset pages
  - "$this" variables 219
  - Additional data in 218
  - annotations 210
  - Anomalies section 63, 211
  - business entities and 210
  - correlated resources 222
  - data source acquisition status 205
  - Expert View metrics 213
  - Expert View section 212
  - opening from heat maps 177
  - opening from search results 201
  - performance analysis 221
  - performance troubleshooting data 200
  - Related Assets sections 216
  - sections of 206
  - Summary section 206
  - Topology section 208
  - types of 200
  - User Data section 209
  - Violations section 217
- asset topology
  - viewing 208
- assets
  - assigning annotations to multiple 80
  - assigning applications to 58
  - manually assigning annotations to 74
  - multiple, adding business entities to 68
- Assets Dashboard
  - heat maps 220
  - monitoring system 177
- assets, related
viewing in the Related Assets section 216
assigning
  annotations 71
  business entities to assets 67
assurance violations
  configuring notifications 54
ASUP
  configuring 55
  process 189
ASUP messages
  recommendation to use HTTPS 55
auditing
  user activities 183
authentication
  LDAP 16
  user 16
auto resolution
  introduction 160
automatic resolution (AR) methods
  examples of regular expressions 170
automatic storage tiering
  configuring rules 76
Autosupport (ASUP) package
  what's included in 56
azure
  data source 136

B
backup
  archiving performance data 50
  what's included in 49
backups
  configuring automatic 49
  performing manually 189
  restoring 187
balancing
  network resources 220
best practices
  backup directories 49
  changing default passwords 11
  defining annotation types before annotation rules 76
  limited number of administrators 16
  restoring OCI database 187
business entities
  adding to multiple assets 68
  application data 57
  assigning to assets 67
  business unit 66
  creating 67
  hierarchy 66
  line of business 66
  on asset pages 210
  project 66
  removing from multiple assets 68
  tenant 66

C
CAC
  browser requirements 35
  client configuration for 35
Cognos configuration for 37, 39
Data Warehouse configuration for 36
  enabling on Linux 36
  host configuration for 33
capacity
  as time series 226
  VMDKs 220
certificate login
  browser requirements 35
  client configuration for 35
  Cognos configuration for 37, 39
  Data Warehouse configuration for 36
  host configuration for 33
  importing certificates 46
certificates
  Cognos 39
  Cognos configuration for 37, 39
  installing 46
  installing new 46
  replacing, after installation 46
  support 33
change encryption key 26
charts
  and downsampled data 223
cloning
data sources 96
Cognos
  certificate login 37, 39
  certificates 39
Cognos 11
  certificates 43, 45
comments
  how to send feedback about documentation 229
committing
data source patches 157
configuration
  advanced 196
  advanced tools 191
  changes 152
  testing data sources 97
configuring
  ASUP 55
  data sources 94
  email 52
  Insight 11
  Java UI Client 196
  performance policy evaluation precedence 90
  performance violation notifications 54
  SNMP notifications 52
  syslog 53
  users in LDAP 19
Configuring Insight for 17
copy
table values 87
cost
  assigning to annotations 72
  creating
    business entities 67
    custom annotations 72
    performance policies 88
    queries 82
  creating annotation rules
    for automatic annotation assignment 75
custom annotations creating 72
custom asset pages asset types used in 81
custom dashboards importing and exporting 91
Customer Support configuring information sent to 55
Dashboard, Violations accessing 185
dashboards asset types used in 81
data collection coordinating changes between your environment and Insight 151
options 94
Data Domain EMC data source 109
data source
Microsoft 136
tags 155
data source acquisition status on asset pages 205
data sources acquisition status on asset pages 205
adding 94
adding new, by patch 95
approving patches 157
changing passwords for a group 151
cloning to quickly add 96
deleting 155
editing multiple setup information 154
editing setup information 154
examining detailed summaries 152
finding serious problems 177
importing 95
installing a patch 156
installing new 93
locating ghost data 197
managing 93
managing patches 157
patching groups 155
permissions to change 16
polling 153
researching failures 153
rolling back patches 158
setting up 93
support matrix 93
testing configurations 97
vendor-specific configuration information 97
data sources, supported
3PAR InServ Firmware (SSH) 97
Amazon AWS EC2 98
Brocade Brocade Enterprise Fabric Connectivity Manager 99
Brocade FC Switch Firmware (SSH) 100
Brocade Sphereon/Intrepid Switch (SNMP) 102
Cisco FC Switch Firmware (SNMP) 103
Dell Compellent Storage Center 105
EMC Celerra (SSH) 106
EMC CLARiiON (NaviCLI) 107
EMC Data Domain 109
EMC ECC StorageScope 110
EMC Isilon 110
EMC RecoverPoint 111
EMC Solutions Enabler (CLI) with SMI-S Performance 112
EMC VNX (SSH) 115
EMC VNXe 115
EMC VPLEX 117
EMC XtremIO (HTTP) 118
Fujitsu Eternus 119
HDS (HiCommand Device Manager) 120
Hitachi NAS (HNAS) 123
HP (CommandView AE) 124
HP EVA Storage (SSSU) 126
Huawei OceanStor 128
IBM DS (CLI) 129
IBM PowerVM 130
IBM SVC (SSH) 131
IBM Tivoli Monitoring 133
IBM TotalStorage DS4000 134
IBM XIV (CLI) 134
Infinidat InfiniBox (HTTP) 135
Microsoft Hyper-V (WMI) 137
NetApp Clustered Data ONTAP 138
NetApp clustered Data ONTAP Unified Manager (UM) 139
NetApp Data ONTAP operating in 7-Mode 139
NetApp E-Series 141
NetApp Host and VM File Systems 142
NetApp SolidFire 144
OpenStack 145
Pure Storage FlashArray (HTTP) 146
QLogic FC Switch (SNMP) 147
Red Hat (RHEV) 148
Violin Memory 6000-Series Flash Memory Array (HTTP) 148
VMware vSphere (Web Services) 149
Data Warehouse certificate login configuration 36
introduction 8
security configuration 22
Data Warehouse server monitoring health of 178
databases automatic weekly backups 49
backing up 189
OnCommand Insight 187
SQL 194
default 22
defining applications 57
delete 183
deleting
annotation rules 78
annotations 74, 75
applications 59
data sources 155
performance policies 91
queries 85
users 16
deleting inactive 183
device discovery 160
device identifications exporting 167
device resolution
adding a device manually 166, 168
DNS options 170
exporting devices from a CSV file 169
exporting FC device identifications 167
exporting IP devices 169
FC identify 166
importing devices from a CSV file 167, 169
importing Fibre channel devices 167
importing IP devices 169
introduction 160
manual 165
manually identifying devices 168
planning rules 163
preferences 170
rule assisted manual 165
update 165
device resolution options 170
device resolution rules
creating, introduction 163
devices
data source setup 93
deleting inactive 151
examining performance 221
disk models
locating vendor information 198
text file format 198
DNS 170
documentation
how to receive automatic notification of changes to 229
how to send feedback about 229
downsampling
of data in charts 223

E
editing
annotations 74
applications 58
data source setups 154
multiple data source setups 154
performance policies 90
user accounts 21
editing multiple applications
using queries 85
e-mail
changing user 21
configuring for receiving Insight reports 52
prerequisites 51
to deliver reports 51

EMC
Data Domain data source 109
RecoverPoint data source 111
EMU
viewing collected data 61
viewing data 61
See also Ethernet monitoring unit
error messages
data source 153
non-compliant licenses 188
Ethernet
monitoring 59, 60
Ethernet monitoring
introduction 59
Ethernet monitoring unit 60
evaluation precedence
performance policies 89
events
data source 152
exclamation mark
meaning of in user interface 152
Expert View metrics
asset pages 213
Expert View section
asset pages 212
populating the performance chart 215
viewing the performance chart 215
exporting
user data 91
exporting to .CSV file
queries 84
expressions, regular
examples for AR 170

F
feedback
how to send comments about documentation 229
Fibre Channel
adding devices manually 166
Fibre Channel environment
monitoring 223
files
backing up 189
license 12
restoring OCI database 187
firewall
OnCommand Insight architecture 8
for customer support 190
foundation
pruning of history 225

H
heat maps
showing high IOPS 177
host resolution
introduction 160
HTTPS
recommended protocol for ASUP 55
I

IBM Cognos
  introduction 8
importing
  annotations 78
data sources 95
user data 91
inactive devices 183
information
  how to send feedback about improving documentation 229
Insight
  backups 49
  component list 193
data source patches 155
data source setup requirements 93
license types 13
licenses 187
licenses, installing 12
list of common maintenance tasks 177
logging in 11
maintenance 151
number of database objects 194
overview 8
status 177
Insight reports
  configuring email for 52
insight server
  restart 191
Insight server
  backup vault 22
  change encryption key 22
  reset 22
  restore vault 22
  security configuration 22
  update password 22
installed software packages
  displaying 191
installing
  licenses 12
  service packs 188
inventory history
  pruning 225
IOPS
  heat map 220
IP devices
  adding devices manually 168
IPIdentify
  manually identifying iSCSI devices 168
L

landing page
  NFS traffic
    volumes 61
    NFSv3 activity 61
LDAP
  authentication 16
  rediscover user 22
  requirements for smart card and certificate login 33
users 19, 21
LDAP(s) 17

licenses
  for Insight 13
  installing 12
  not compliant 188
  replacing older versions 188
  types 13
  updating expired 187
Linux
  enabling CAC 36
log files
  accessing 191
login
  certificate 33
  Smart Card 33
logs
  audit 183
  creating a zip file for Support 189
  generate for Customer Support 193
  syslog 54

M

maintenance
  coordinating changes between your environment and Insight 151
maintenance tasks
  list of most common 177
managing
  performance policies 87
missing disk model
  acquisition failure 197
  adding missing disk models 197
modifying
  annotation rules 77
  annotations 74
  data source setup 154
  multiple data source setups 154
  queries 85
monitoring
  anomalies 61
  applications 61
  data sources 93
  Fibre Channel environment 223
  Insight component health 178
  violations 185
monitoring your environment
  using asset annotations 69
moving
  MySQL data 194
  MySQL data with command line 195
MySQL
  migrating data 194

N

NAS path
  for virtual machines 226
NetApp Customer Support
  bundling logs for troubleshooting 189
  preparing troubleshooting report 189
  sending data to 189
network
balancing resources 220
performance 221
system information 193
network configuration
Ethernet monitoring unit 60
network maintenance
list of most common tasks 177
NFSv3
monitoring 59
notifications
performance violations 54
notifications, SNMP
configuring 52

O
OCI
See OnCommand Insight
OnCommand Insight
architecture 8
firewall-friendly architecture 8
managing data sources 93
overview 8
setup tasks 11

P
password
internal user 29
match 29
passwords
changing for data source groups 151
changing user 21
coordinating changes 151
dwh_internal 30
edit connector 30
encrypted for ASUP 55
inventory 30
LDAP 19
new users 16
patches
adding new data source by 95
approving 157
coordinating changes between your environment and Insight 151
data source, managing 157
groups of data sources 155
installing data source 156
new data source, installing 93
rolling back 158
performance
adding new policies 88
alerts in syslog 53
analyzing slow client computers 221
correlated resources 222
examining network 221
monitoring 200
performance analysis
skills required 9
performance chart
using 215
performance charts
correlated resources 222
zooming in 221
performance data archive
enabling 51
loading 51
performance policies
configuring evaluation precedence 90
creating 88
deleting 91
editing 90
evaluation precedence 89
identifying violations 207
managing 87
performance policy
application 64
performance troubleshooting data
asset pages 200
performance violations
configuring notifications 54
planning
your data source support 93
policies
importing and exporting 91
performance 88
polling
data sources 153
postpone
data source polling 153
precedence
setting for annotation rules 77
pruning
of inventory history 225

Q
queries
adding business entities to multiple assets using 68
asset types used in 81
assigning multiple annotations 86
creating 82
deleting 85
editing multiple applications 85
exporting to .CSV file 84
importing and exporting 91
modifying 85
removing multiple annotations 86
removing multiple applications 85
viewing 83

R
RAU
security configuration 22
RecoverPoint
EMC data source 111
red circle
meaning of in the user interface 177
regular expressions
examples for AR 170
Related Assets section
viewing related assets 216
Related Assets sections
on asset pages 216
removing
  data sources 155
  user account 22
removing multiple applications
  using queries 85
reporting
  customized with annotations 69
Reporting
  introduction 8
resources
  searching for 201
  top correlated 221, 222
restart
  insight server 191
restarting
  acquisition units 186
  data source polling 153
  Insight servers 194
restoring
  backups 187
resume
  data source polling 153
roles
  users 16
rules
  for device resolution 163
  introduction to device resolution 163
S
scaling
  determine number of database objects 194
scrubbing data 190
search
  advanced techniques 201
  boolean 201
  keywords 201
  wildcard 201
searching
  correlated resources 222
  environment assets 201
  for host 221
sections of
  asset pages 206
security
  data warehouse 28
  EMU 26
  Insight server 24
  LAU 25
  RAU 26
  user roles 16
self-signed certificates
  installing 46
servers
  backup 49
  LDAP 19
  monitoring health of 178
  restarting OnCommand Insight 194
Service Level annotation
  assigning cost to 72
service packs
  applying 188
setting hours to ignore data updates
  configuration 60, 97, 152, 191, 196
setting up
  Insight 11
  licenses 12
smart card
  client configuration for 35
  Cognos, configuration for 37, 39
  Data Warehouse configuration for 36
  host configuration for 33
Smart Card
  support 33
SNMP
  configuring notifications 52
software
  anomaly detection 61
solid red circle
  meaning 186
status
  anomaly detection monitoring 64
storage
  predefined tier annotations 76
storage and tape vendors
  including or excluding 170
suggestions
  how to send feedback about documentation 229
Summary section
  identifying metric issues 207
  identifying performance policy violations 207
  on asset pages 206
  viewing general asset information 207
Switch Level annotation
  assigning cost to 72
syslog
  configuring 53
  contents 54
T
tables
  copying values 87
terabytes
  licensed 188
terminology
  Amazon 98
testing
  added data sources 94
  data source configurations 97
Tier annotation
  assigning cost to 72
tiers
  predefined annotations 76
time series
  capacity data as 226
time-to-live (TTL)
  downsampling explained 223
Topology section
  asset pages 208
  viewing an asset's topology 208
tracking data
  using asset annotations 69
troubleshooting
  data collection problems 151
database backup 189
locating ghost data 197
locating your environment resources 201
preparing a special report 189
restoring OnCommand Insight 187
sending report to Support 189
server resources status 196
tools 191
using audit log 183
your environment 200
zipping logs for Support 189
Twitter
  how to receive automatic notification of documentation changes 229
types of
  asset pages 200

U
update
device resolution rules 165
user data
  importing and exporting 91
User Data section
  asset pages 209
  using to assign or modify annotations 210
users
  auditing activities 183
  authenticated from LDAP 19
  changing passwords 21
  defining 16
  deleting 22
  editing accounts 21
  experience level 9
  roles 16

V
vendors
  finding disk model information 198
  supported data sources 97
viewing
  annotations assigned to an asset 210
  applications assigned to an asset 209
  asset topology 208
  business entity assigned to an asset 210
  queries 83
viewing an asset’s Topology
  Topology section 208
viewing related assets
  Related Assets section 216
viewing violations
  Violations section 217
violations
  by policy 185
  changes in syslog 53
  configuring
    assurance violation notifications 54
    history 185
    in syslog 54
    monitoring 185
    SNMP notifications of 52
Violations Dashboard
  accessing 185
Violations section
  on asset pages 217
  viewing violations 217
VMDK
  resources list 220
VMs
  NAS path 226

W
web UI
  access data source support matrix 93
  accessing 11
  advanced troubleshooting tools 191
  introduction 8
widgets
  asset types used in 81