OnCommand® Insight 7.2.3

Installation Guide

For Microsoft® Windows®

October 2016 | 215-11627_A0
doccomments@netapp.com

NetApp®

Contents

OnCommand Insight overview

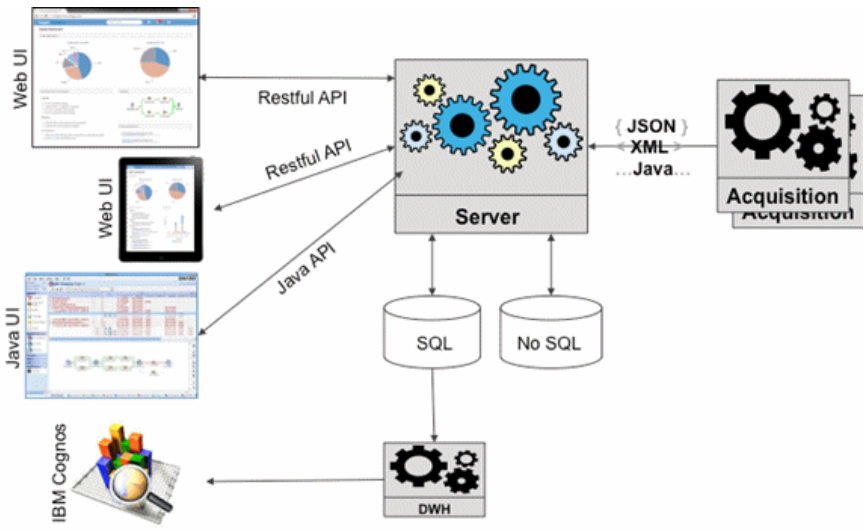
OnCommand Insight enables you to simplify operational management of complex private and hybrid cloud and virtual IT environments. Insight is a single solution to enable cross-domain, multi-vendor resource management and analysis across networks, storage, and servers in physical and virtual environments.

Insight provides a “single pane of glass” for reporting on storage costs and provides the transparency needed to make decisions about performance and efficiency.

Insight architecture

OnCommand Insight enables you to administer your product easily, using a streamlined system architecture that includes the Insight Server, a collection engine, web-based and Java UIs, and data warehousing.

The major components of the Insight architecture are shown in this diagram and described after it:



OnCommand Insight Server

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

Acquisition units

The Insight collection engine is built of one or more acquisition units. Each acquisition unit is a service running in the network that accesses (through modules called *data sources*) and collects data from different devices in the data center. Information collected by the acquisition units is then sent to the server (in an XML, JSON, or native Java format) for analysis.

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

Web UI

The HTML5 web-based user interface (UI) for Insight enables you to set up your monitoring environment and data sources. You then use the web UI Asset Dashboard and asset pages to identify and research potential problems.

Java UI

This is the OnCommand Insight user interface (UI) or Client. You can use the Java UI to research issues like Fibre Channel mappings in your environment.

Data Warehouse (DWH)

Consolidates and prepares data for reporting for one or multiple installations of Insight. This includes history, trending, inventory, chargeback, show back and presenting the data in different ways to enable long-term planning of the data center's infrastructure.

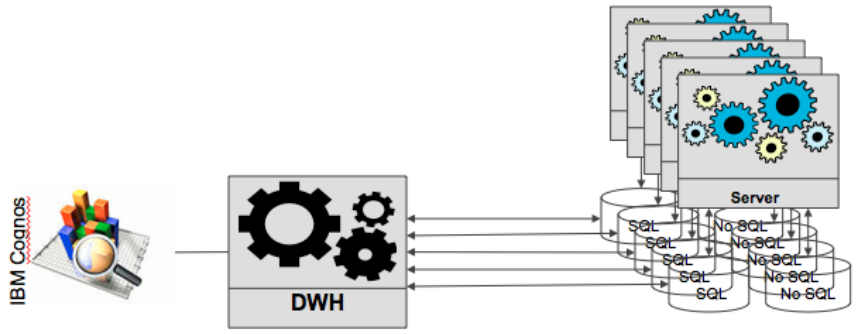
IBM Cognos

This software is a reporting engine that provides a user interface for creating enterprise-level reports.

Insight Data Warehouse architecture

In a large environment, the OnCommand Insight Data Warehouse (DWH) consolidates data across different installations and hence different Insight data centers.

As shown in this diagram, the architecture enables users to view their entire environment and generate meaningful reports through a “single pane of glass” interface:

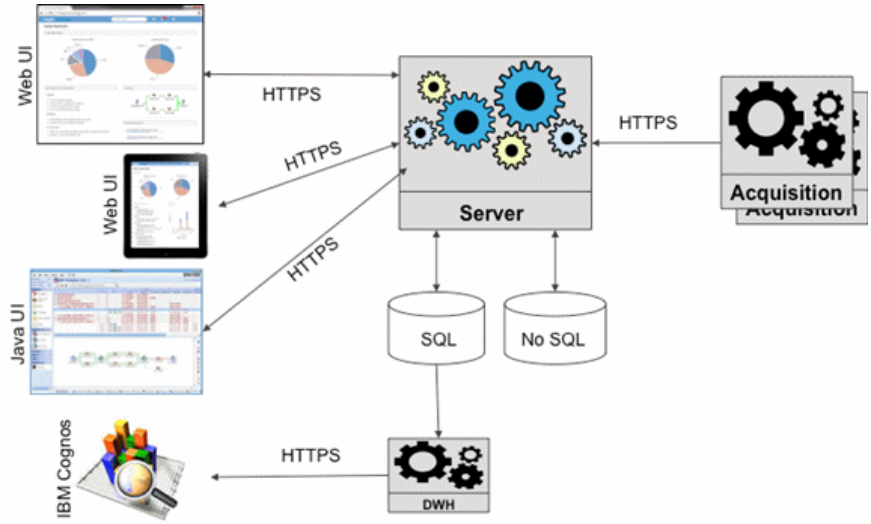


Firewall-friendly architecture

The OnCommand Insight architecture enables you to easily create firewalls around the product so that your assets are more secure.

As shown in the diagram, the architecture has these firewall features:

- All OCI clients use HTTPS to communicate with the server.
- The acquisition units enable only *outgoing* HTTPS connections; no ports are opened on the acquisition unit processes.



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.

Where to find more information about OnCommand Insight

For comprehensive, up-to-date information about OnCommand Insight, use these resources.

- The OnCommand Insight Web page:
  http://www.netapp.com/us/products/management-software/oncommand-insight/
- The OnCommand Insight documentation page:

http://mysupport.netapp.com/documentation/productlibrary/index.html?productID=60983

- The NetApp support site:
  http://mysupport.netapp.com
- IBM Cognos documentation on the web:
  http://www.ibm.com/analytics/us/en/technology/cognos-software/
- The NetApp automation storefront where you can download from an extensive collection of NetApp and User-community submitted report templates for OnCommand Insight.
  https://automationstore.netapp.com
- OnCommand Insight Discussion Forum:
  https://forums.netapp.com/welcome

For information available from the Reporting portal, you can access the OnCommand Insight On-line Help. The help includes access to the Data Warehouse database schema.

Installation prerequisites

Before you install OnCommand Insight, you must download the current software version, acquire the appropriate license, and set up your environment.

Important: If you are installing in a Microsoft Windows 2008 or 2008 R2 environment, and OnCommand Insight fails to install, showing the message `There is a problem with this Windows Installer package`, you might need to disable the User Account Control (UAC) before starting the OnCommand Insight installation.

Before installing OnCommand Insight, ensure that you have the following:

- OnCommand Insight software files in the downloaded installation package for the current version
- A license to operate the downloaded OnCommand Insight version
- The minimum hardware and software environment
  The current product might consume additional hardware resources (due to enhanced OnCommand Insight product functionality) that were not consumed with earlier versions of the OnCommand Insight product.
- A deployment plan that includes the hardware and network configurations for the OnCommand Insight Server, Data Warehouse and Reporting, remote acquisition units, and the Client
- Java 8 for the OnCommand Insight Java UI
- Disabled virus scan software
  If you cannot disable the software, exclude the `sanscreen` directory from the scan.

Planning the deployment

To ensure a successful deployment, you must consider certain system elements before you install OnCommand Insight.

About this task

Planning your Insight deployment includes considering these system elements:

- Insight architecture
- Your network components to be monitored
- Insight installation prerequisites and server requirements
- Insight web browser requirements

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/*.

Device identification and data source planning

As part of your deployment planning, you should collect information about the devices in your environment.

You need the following software, connectivity, and information about each device in your environment:

- IP address or hostname resolvable by the OCI server
- Login name and password
- Type of access to the device, for example, controller and management station

  Note: Read-only access will be sufficient for most devices, but some devices require administrator permissions.

- Port connectivity to the device depending on data source port requirements
- For switches, SNMP read-only community string (user ID or password to give access to the switches)
- Any third-party software required on the device, for example, Solutions Enabler.
- See the "Vendor-specific data source reference" in the web UI Help or in the *OnCommand Insight Configuration and Administration Guide* for more information on data source permissions and requirements.

Network traffic generated by OnCommand Insight

The network traffic that OnCommand Insight generates, the amount of processed data traversing the network, and the load that OnCommand Insight places on devices differ based on many factors.

The traffic, data, and load differ across environments based on the following factors:

- The raw data
- Configuration of devices
- Deployment topology of OnCommand Insight
- Different inventory and performance data source polling intervals, which can be reduced to allow for slow devices to be discovered or bandwidth to be conserved

The raw configuration data that OnCommand Insight collects can vary significantly.

The following example illustrates how the configuration data can vary and how traffic, data, and load are affected by many configuration factors. For example, you might have two arrays each having 1,000 disks:

- Array 1: Has 1,000 SATA disks all 1 TB in size. All 1,000 disks are in one storage pool, and there are 1,000 LUNs, all presented (mapped and masked) to the same 32 nodes in an ESX cluster.
- Array 2: Has 400 2-TB data disks, 560 600-GB FC disks, and 40 SSD. There are 3 storage pools, but 320 of the FC disks are used in traditional RAID groups. The LUNs carved on the RAID groups use a traditional masking type (symmaskdb), while the thin provisioned, pool-based LUNs use a newer masking type (symaccess). There are 600 LUNs presented to 150 different hosts. There are 200 BCVs (full block replica volumes of 200 of the 600 LUNs). There are also 200 R2 volumes, remote replica volumes of volumes that exist on an array in a different site.

These arrays each have 1,000 disks and 1,000 logical volumes. They might be physically identical in the amount of rack space they consume in the data center, and they might even be running the same firmware, but the second array is much more complex in its configuration than the first array.

Virus scan software disablement

If antivirus software is active on your system, OnCommand Insight installation fails. You can prevent this problem by disabling the virus scan software before installation.

To prevent an installation failure due to active virus scan software, you must exclude the Insight path from access to antivirus scanning during the installation of the Insight components.

After all of the components, including the reporting Data Warehouse, are installed, you can safely reactivate the antivirus software; however, ensure you configure the scan to exclude everything in the Insight installation directory.

Insight Server requirements

The Insight Server requires a specific operating system, specific amounts of memory, CPU cores, and disk space. You must adhere to these requirements to successfully install Insight.

Tip: A dedicated server is recommended. Do not install Insight on a server that has any other applications installed. Both physical and virtual servers are supported, provided that the product requirements are met.

You must have local administrator permissions to install the OnCommand Insight Server software.

The dedicated server must meet your company's security standards and include these components:

- The SQL database that stores information about your SAN configuration
- The impact analysis and simulation engine
- The local acquisition unit

Important: Sizing for OnCommand Insight has multiple dependencies, such as data source type and data source size. Consequently, you should discuss and validate all sizing recommendations with a NetApp representative.

Component	Required
Operating system	A computer running a 64-bit Microsoft Windows Server 2008 R1, 2008 R2, 2012, or 2012 R2 with the latest service pack. A dedicated server is recommended.
Virtual machine (VM)	This component can also run on a virtual machine, provided that your environment allows for RAM reservations.
Memory and CPU	For environments with up to 100 storage arrays, 5000 Fibre Channel switch ports, and 5000 virtual machines, use an 8 core 32 GB memory server. This is a general guideline. **Note:** If your environment is larger than this, contact your Sales Engineer for guidance. Best Practice: It is strongly recommended to set the paging file size to “Windows managed”. Small, fixed-size paging files may interfere with the successful storage of Insight performance data.

Component	Required
Available disk space	The server needs 100 GB of free disk space.
Network	Ethernet connection and ports: • 100 Mbps or 1 Gbps Ethernet connection with dedicated (static) IP address and IP connectivity to all components in the SAN, including FC devices and remote acquisition units. • Port requirements for the OnCommand Insight Server process are 80, 443, 1090 through 1100, 3873, 8083, 4444 through 4446, 5445, 5455, 4712 through 4714, 5500, and 5501. • Port requirements for the acquisition process are 12123 and 5679. • Port requirement for MySQL is 3306. Ports 443 and 3306 require external access through any firewall that is present.
Permissions	Local administrator permissions are required on the OnCommand Insight Server.
Remote connectivity	Internet connectivity to allow WebEx access or a remote desktop connection to facilitate installation and postinstallation support.
Accessibility	HTTP, HTTPS, or FTP access to the Internet is highly recommended.
Virus scan	The entire OnCommand Insight directory should be excluded from any virus scan applications.
HTTP or HTTPS servers	Microsoft Internet Information Services (IIS) or other HTTP and HTTPS servers should not compete for the same ports (80 and 443) as the OnCommand Insight server, and should not start automatically. If they must listen to port 80 or 443, then you must configure the OnCommand Insight server to use other ports.

Data Warehouse and Reporting server requirements

You must run the Data Warehouse and the Reporting server on a computer that is compatible with established hardware and software requirements, ensuring that Apache web server or reporting software is not already installed on this machine. Data Warehouse is supported only on the Internet Explorer browser.

Component	Required
Operating system	Computer running a 64-bit Microsoft Windows Server 2008 R1, 2008 R2, 2012, or 2012 R2 with the latest service pack.

Component	Required
Virtual machine (VM)	This component can also run on a virtual machine, provided that your environment allows for RAM reservations.
CPU	8 CPU core
Memory	40 GB RAM Best Practice: It is strongly recommended to set the paging file size to "Windows managed". Small, fixed-size paging files may interfere with the successful storage of Insight performance data.
Available disk space	100 GB Installation requires 20 GB free on the C: drive.
Network	• 100 Mbps or 1 Gbps Ethernet connection • Static IP address • For the OnCommand Insight DWH server process, ports 80, 443, 1098, 1099, 3873, 8083, and 4444 through 4446 • For the reporting engine, ports 1527, 9362, 9300, and 9399 • For MySQL, port 3306 • Ensure that DNS is properly working by doing an `nslookup` against the host
Virus Scan	The entire OnCommand Insight directory should be excluded from any virus scan applications.

Remote Acquisition Unit server requirements

You must install a Remote Acquisition Unit (RAU) to acquire information from SAN devices that are behind a firewall, at a remote site, on a private network, or in different network segments. Before you install the RAU, you should ensure that your environment meets RAU operating system, CPU, memory, and disk space requirements.

Component	Requirement
Operating system	Computer running a 64-bit Microsoft Windows Server 2008 R1, 2008 R2, 2012, or 2012 R2 with the latest service pack
CPU	4 CPU cores
Memory	16 GB RAM
Available disk space	40 GB
Network	100 Mbps /1 Gbps Ethernet connection, static IP address, IP connectivity to all FC devices, and a required port to the OnCommand Insight server (80 or 443).
Permissions	Local Administrator permissions on the RAU server
Virus scan	Exclusion of the entire OnCommand Insight directory from any virus scan applications

Ethernet Monitoring Unit requirements

The Ethernet Monitoring Unit is a hardware server dedicated to monitoring NFS traffic in an OnCommand Insight environment. The minimum system requirements for Ethernet Monitoring Units and the supported NICs are listed below.

Server requirements

Component	Required
Hardware	Rack-mounted chassis with redundant power supplies
Operating system	Red Hat Enterprise Linux (RHEL) 7.2 operating system
CPU	Two 2.2 GHz 8-core hyper-threading CPUs
Memory	32 GB RAM
Available disk space	240 GB hard drive
Network	2 - 10GbE NICs for monitoring NFS traffic (from supported list)
	2 - Short Range 10GbE Gigabit Interface Converter (GBIC)
	1 - 1GbE interface for management with the OnCommand Insight server
Permissions	Sudo permissions on the Server.

Supported network interface cards

The Network Interface Cards (NICs) that are supported for monitoring NFS traffic are listed in the table below.

Manufacturer	Common Linux ethernet driver	Model designation
Cisco	Enic	UCS Virtual Interface Card
Intel	e1000	82540, 82545, 82546
Intel	e1000e	82571,82572, 82573,82574, 82583, ICH8, ICH9, ICH10, PCH1, PCH2, I217, I218
Intel	igb	82575, 82576, 82580, I210, I211, I350, I354, DH89xx
Intel	ixgbe	82598,82599, X540, X550
Intel	i40e	X710, XL710, X722
Intel	fm10k	FM10420
Qlogic	bnx2x	578xx

Anomaly detection requirements

The anomaly detection software requires a specific operating system, amounts of memory, CPU cores, and disk space. You must adhere to certain requirements to successfully install the anomaly detection software.

Component	Required
Operating system	A computer running a licensed version of Red Hat Enterprise Linux 7 that is running no other application-level software. A licensed version ensures that dependencies required for the installation are resolved automatically by the operating system. A dedicated server is recommended.
Virtual machine (VM)	Anomaly Detection can also run on a virtual machine, provided that your environment allows for RAM reservations.
Memory and CPU	An 8 core 32 GB memory server.
Available disk space	The server requires 200 GB of free disk space. 5 GB of free disk space must be available in the `/var/lib` partition and 25 GB of free disk space must be available in the `/opt` and `/var/log` partitions. It is a best practice to mount `/opt` and `/var` on separate disks from the root file system (`/`).
Permissions	Sudo permissions are required to install the anomaly detection software.
Network	The Insight server on which you want to install the anomaly detection software must reside on the same network, or at least in the same site or Data Center as the server that is running the anomaly detection engine. The anomaly detection software does not support configuration in a Wide-Area Network (WAN).
Prerequisites	You must be using OnCommand Insight 7.2 with a valid Perform license. You must have the IP address of the Insight server on which you want to install the anomaly detection software. You must have an alternate port number on the Insight server if you do not accept the default port. TCP ports 8080 and 9200 must be open on the VM. You must have a user name and password for an account with Administrator privileges on the VM. You must enter two backslashes (company\\user) for a user name containing a single backslash (company\user). A user name cannot contain a “t” following a backslash (company\\tom).

Important: You must discuss and validate all sizing recommendations with a NetApp representative.

Insight Java UI requirements

Because the OnCommand Insight Java UI Client operates in a Java run-time environment on your computer, it is important that you ensure that your environment meets specific operating system, CPU, and memory requirements.

To access the Java UI Client, you must install the Java run-time environment (JRE) on your computer.

Component	Requirement
Operating system	Any Java 8-enabled machine. The Java-based OnCommand Insight Client supports Windows, Macintosh, and Linux platforms.
CPU	1.8 GHz or faster is required.
Memory	2 GB or more is recommended. If you are monitoring the performance of complex data centers (over 50,000 switch ports), the server requires more memory. This is applicable only if the Perform license is installed.

Browsers supported by OnCommand Insight

The OnCommand Insight web UI is browser-based and can operate on several different browsers.

Insight supports the following browsers:

Insight component	Requirement
Insight web UI	Microsoft Internet Explorer 11 and later Mozilla Firefox 37 and later Google Chrome 41 and later Edge 25 and later
Reporting Connection (IBM Cognos)	Microsoft Internet Explorer 9 and later Mozilla Firefox ESR 38 and future fix packs Google Chrome 41 and future versions, releases, and fix packs

Insight installation instructions

Installation requires you to install several OnCommand Insight components, including Client, Data Warehouse and Reporting, and Anomaly Detection.

The installation includes the following major tasks:

- Downloading the OnCommand Insight installer
- Installing OnCommand Insight Server
- Installing licenses
- Optionally, installing DWH and Reporting (must be installed on a separate machine or virtual machine)
- Optionally, installing a remote acquisition unit (RAU), which acquires information from your device resources that reside behind a firewall, are located at a remote site, or are on a private network
- Optionally, installing the Anomaly Detection engine (must be installed on a separate machine or virtual machine running Linux.)
- For upgrades, upgrading OnCommand Insight reports.

After installation, you must configure Insight to acquire information about your environment. The tasks required are described in the *OnCommand Insight Configuration and Administration Guide*.

Downloading the OnCommand Insight installer

You can download the OnCommand Insight installer from the NetApp Support Site.

Before you begin

You must have a login to the NetApp Support Site at *mysupport.netapp.com*.

Steps

1. Log in to the server on which you want to install OnCommand Insight.
2. Download the installation file from the NetApp Support site.

Installing OnCommand Insight components

You install the OnCommand Insight software by running a wizard in which the installation is self-contained; however, two of the typical OnCommand Insight elements used to operate OnCommand Insight, the OnCommand Insight remote acquisition unit (RAU) and the OnCommand Insight Server must be installed separately. This installation includes both the web UI and Java UI.

You can install any number of additional RAUs to add remote data centers and private networks to the SAN devices that are managed by OnCommand Insight.

Installing the OnCommand Insight Server

You can easily install the OnCommand Insight Server by using the OnCommand Insight Setup wizard.

Before you begin

You must have completed all of the installation prerequisites.

Steps

1. Log in to the Insight server using an account with administrator privileges.
2. Open Windows Explorer and navigate to the directory where the installation files are located.
3. Double-click the `.MSI` file that you downloaded.
4. Click **Next** to continue.
5. Read the License Agreement, select **I accept the terms in the License Agreement** check box, and then click **Next**.
6. Enter the customer name and site name in the **Customer Information** window, and click **Next**.

   Best Practice: Use the customer name as a prefix for the site: for example, NetApp.
7. In the **Customer Information: Configure NetApp ASUP** window, do the following:

   a. Select the database containing the data that you want to upload to ASUP by selecting one of the following options:

   No database backup

   A backup is not sent to ASUP.

   Backup without Performance data

   A backup is made and sent to ASUP but does not include performance data.

   Backup with Performance data

   A backup is made that includes performance data, but this could generate a huge `*.gz` file.

   b. For automated support, select which send method you want to upload data to ASUP (FTP, HTTP, HTTPS, or email).

   Note: You must use HTTPS for delivery of AutoSupport (Phonehome) to provide the best security and to support the latest AutoSupport features. Although AutoSupport supports FTP and email for delivery of AutoSupport messages, HTTPS is recommended.

   Note: If you select email, you must configure the email server from the OnCommand Insight Administration web portal using the **Mail** option. To change to HTTP or HTTPS and a proxy, you can configure the ASUP settings in the OnCommand Insight Administration web portal.

   c. In **Logs**, select whether you want no logs, base logs, or extended logs, which contain a data source recording.

   d. Click **Next**.
8. In the **Configure Server** page, select or set the appropriate configuration parameters to configure the OnCommand Insight Server:

OnCommand Insight Portal Port (HTTP)

Ports used by the OnCommand Insight Server to support user Web services, including a portal to launch the client and to perform administration tasks. Use the default (80); however, if the default port is in use, change this to another port.

OnCommand Insight Portal Port (HTTPS)

Port used by remote acquisition units to send SAN change information to the OnCommand Insight Server through a secure channel. Use the default (443); however, if the default port is in use, change this to another port. You specify this same port number when configuring RAUs.

Internal Database Port (SQL)

Port used internally by the PC where the OnCommand Insight Server is running, to serve as an access point to the database. Use the default (3306); however, if the default port is in use, change this to another port.

9. Click **Next**.
10. Click **Install** to proceed.

    The installation should take approximately 20 minutes, depending on the applications installed.
11. Click **Finish**.

Related concepts

Virus scan software disablement on page 11

Related references

Installation prerequisites on page 9

Installing OnCommand Insight Data Warehouse and Reporting

The installation is self-contained and includes the elements required to run and operate OnCommand Insight Data Warehouse (DWH) and the Reporting utilities supplied by IBM.

Before you begin

You must have completed all of the installation prerequisites.

If you are upgrading, you should back up all of your OnCommand Insight reports.

About this task

To find details about the Reporting portal features, such as how to configure SMTP services, refer to the IBM Cognos documentation at *http://www-947.ibm.com/support/entry/portal/Documentation*.

Steps

1. Log in to the Data Warehouse server using an account with administrator privileges.
2. Open Windows Explorer; then open the directory where the installation files are located.
3. Double-click the `.MSI` file.
4. Click **Next**.
5. Select the **Accept License Agreement** check box.

6. Click **Next**.
7. In the **Customer Information** window, enter a customer name and a site name.

   Best Practice: Use the customer name as a prefix for the site name (for example, "NetAppSunnyvale").
8. If you want to install the software in a different location than the default (C:\program Files\), click **Browse** and select the location.
9. Click **Next**.
10. Follow the instructions on the windows.
11. Click **Install** to proceed with the installation of the OnCommand Insight Data Warehouse and Reporting.

    The installation should take approximately 40 minutes, depending on the selections made.
12. Click **Finish**.

Locating IBM Cognos documentation

For basic information such as how to start and stop the Reporting portal software, see the IBM Cognos documentation installed with the product. You can search with a web browser for information about any of the IBM Cognos reporting products, such as Query Studio, Report Studio, Business Insight, or Business Insight Advanced on the IBM website in the Information Centers for those software products.

Steps

1. To locate the IBM Cognos documentation installed with OnCommand Insight, navigate to this directory.

   `<install_dir>\cognos\c10_64\webcontent\documentation\help_docs.html`
2. You can also display topics describing individual IBM Cognos windows used in the OnCommand Insight Reporting Portal. Click the **?** icon on the window toolbar.

Verifying the Data Warehouse and Reporting installation

After a successful OnCommand Insight Data Warehouse installation, you should ensure that all of the DWH and Reporting services are available in your Microsoft Windows services.

Steps

1. From the Windows Start menu, select **Control Panel > Performance and Maintenance > Administrative Tools > Services**.
2. Ensure that the following entries appear in the list of services:

   - SANscreen Server
     The OnCommand Insight DWH server
   - MySQL
     The OnCommand Insight SQL database
   - IBM Cognos
   - IBM Cognos Content Database

Installing a Remote Acquisition Unit (RAU)

Install one or more RAUs in your OnCommand Insight environment.

Before you begin

You must have completed all of the installation prerequisites.

At least one port needs to be open and available between the RAU server and the OnCommand Insight Server in order to forward change information to the server. If you are unsure about this, validate it by opening a Web browser on the RAU computer and directing it to the OnCommand Insight server:

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

The acquisition port defaults to 443, but it may have been changed during the server installation. If the connection is successful, you see a OnCommand Insight response page indicating an open and available port between the RAU and the OnCommand Insight server.

Steps

1. Log in to the RAU server using an account with administrator privileges.
2. Open Windows Explorer and navigate to the directory where the RAU installation file is located.
3. Double-click `.MSI` file to start the installation.
4. Click **Next** to continue to the window that shows the License Agreement. Read this and accept the terms of the License Agreement and click **Next**.
5. Select to install the RAU on a local hard drive or the entire feature on a local hard drive. (You can check the Disk Usage link to ensure you have enough space - 116MB is required.) Click **Next**.
6. In the Configure window, set these parameters that are specific to your site:
   - **OnCommand Insight Server Name or Address** - hostname or IP address to identify the OnCommand Insight Server. The RAU uses this name/IP to open a communications link with the server. If you specify a hostname, make sure it can be resolved through DNS.
   - **Acquisition Unit Name** - unique name that identifies the RAU.
   - **OnCommand Insight Secured Remote Acquisition Port (HTTPS)** - Port used by Remote Acquisition Units to send environment change information to the OnCommand Insight server. This setting should match the value entered when installing the OnCommand Insight server and must be the same on all RAUs.
7. Review your selections. Click **Back** to go back and make changes. Click **Next**.
8. Click **Install** to start the installation.

   Wait for the installation to complete. This should take approximately 5 to 10 minutes.

After you finish

When the installation is complete, a final window appears. Click the **Start Remote Acquisition Service** box to start the RAU, and click **Finish** to end this operation.

Verifying the remote acquisition unit service

After a successful remote acquisition unit (RAU) installation, the OnCommand Insight RAU service should be available in the Microsoft Windows services environment.

Steps

1. To verify that the RAU was added to the Windows services, open the Windows Start menu and select the **Control Panel > Administrative Tools > Services**.
2. Locate the **OnCommand Insight Acq - OnCommand Insight's Remote Acquisition Unit (RAU)** in the list.

Validating the remote acquisition unit installation

To validate proper installation of the Remote Acquisition Unit, you can view the status of the Remote Acquisition Units connected to your server.

Steps

1. On the Insight toolbar, click **Admin**.
2. Click **Acquisition Units**.
3. Verify that the new Remote Acquisition Unit was registered correctly and that it has a Connected status.

   If it does not, you must contact technical support.

Installing the anomaly detection software

OnCommand Insight contains software that applies machine-learning anomaly detection to your Insight data. You can install this software separately from other OnCommand Insight components.

Before you begin

You must have completed all of the installation prerequisites.

Steps

1. Log in to the anomaly detection server using an account with sudo privileges.
2. Copy the `.zip` file that contains the anomaly detection software to the Linux server.
3. Extract the files to the `oci-prelert-<version>-linux-x86_64` directory.
4. Navigate to the directory where the installer is located:

   `cd oci-prelert-<version>-linux-x86_64`
5. Install the anomaly detection software:

   `sudo ./oci-prelert-install.sh`

   During the installation, you are prompted to enter the server name or IP address of the OnCommand Insight server, and the user name and password for an account with Administrator privileges.

   You can remove the anomaly detection software using the following command:

   `sudo /usr/bin/oci-prelert-uninstall.sh`

Result

The software is automatically registered with the instance of OnCommand Insight that is specified in the installation. The software can communicate only with the OnCommand Insight instance that it is registered with, and only one instance of the software can be registered with an OnCommand Insight server.

If you restart either the server that is running the anomaly detection software or the Insight server, the anomaly detection process restarts automatically.

Installing an Ethernet Monitoring Unit

You can install Ethernet Monitoring Units (EMU) to monitor network packets in your OnCommand Insight environment.

Before you begin

You must have completed all of the installation prerequisites.

Steps

1. Log in to the EMU server using an account with sudo privileges.
2. Navigate to the directory on the server where the installation files are located and type the following command:

   `unzip oci-ethernet-<version>-linux-x86_64.zip`

   Where `<version>` is the version number specified in the filename you downloaded.
3. You can view syntax, command arguments, and parameter usage for `oci-install.sh`:

   `sudo ./oci-ethernet-<version>-linux-x86_64/oci-install.sh --help`
4. Run the installation script:

   `sudo ./oci-ethernet-<version>-linux-x86_64/oci-install.sh`
5. Read the License Agreement and accept it.
6. Answer each of the prompts:

   - **OnCommand Insight Server Name or IP Address** - hostname or IP address to identify the OnCommand Insight Server. The EMU uses this name/IP to open a communications link with the server. If you specify a hostname, make sure it can be resolved through DNS.
   - **Acquisition Unit Name** - unique name that identifies the EMU.
   - **OnCommand Insight Secured Remote Acquisition Port (HTTPS)** - Port used by the EMU to send environment change information to the OnCommand Insight server. This setting should match the value entered when installing the OnCommand Insight server and must be the same on all EMUs.
   - **Ethernet PAS output directory** - Enter the folder for PAS output.
   - **Ethernet PAS interfaces to monitor** - Enter the interfaces whose traffic you wish to monitor.
   - **Enable jumbo packets** - Choose whether to enable jumbo packets.

   After you answer all the prompts, the installation begins and should take approximately 10 minutes, depending on the applications installed.

Checking the installation

You can open Insight in a supported browser to check the installation. You might also want to check the Insight log files.

When you first open Insight, the license setup page opens. After you enter the license information, you must set up the data sources. See the *OnCommand Insight Configuration and Administration Guide* for information about entering data source definitions and setting up Insight users and notifications.

If you have experienced installation problems, contact technical support and provide the requested information.

Verifying new Insight services

After a successful installation, you should verify that the services for the Insight components are operating on your server.

Steps

1. To display a list of services that are currently operating:
   a. Click the **Start** button.
   b. Click **Run**.
   c. Type the following:
      ```
      cmd
      ```
   d. Press Enter.
   e. Type the following in the **Command Prompt** window:
      ```
      net start
      ```
2. Check for these Insight services in the list:
   - **SANscreen Server**
   - **SANscreen Acq** (the acquisition process)
   - **MySql** (Insight SQL database)
   - **Cassandra** (Insight Performance database included with the Perform license)

   If these services do not display in the list, contact technical support.

Insight logs

Insight supplies many log files to assist you with research and troubleshooting. The available logs are listed in the log directory. You might want to use a log monitoring tool, such as BareTail, to display all of the logs at one time.

The log files are located in the <install directory>\SANscreen\jboss\server\onaro\log directory.

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 client (web UI).

Steps

1. Do one of the following:

   - Open Insight on the Insight server:

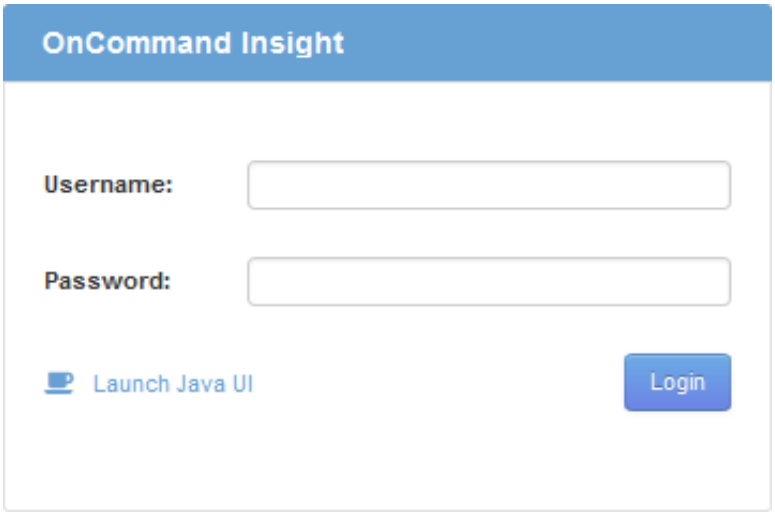
     `https://fqdn`

   - 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**.

   The following table shows the default user name and password. Change these defaults as soon as possible after installation:

Data	Value
Default user name	`admin`
Default password	`admin123`

   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**.

After you finish

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

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

See the Insight Help or the *OnCommand Insight Configuration and Administration Guide* for instructions.

OnCommand Insight licenses

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

Discover

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

Assure

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

Perform

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

Plan

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

Host Utilization pack

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

Report Authoring

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

OnCommand Insight modules are licensed for annual term or perpetual:

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

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

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

Discover

Acquire and manage inventory (Foundation)

Monitor changes and manage inventory policies

Assure

View and manage SAN path policies and violations

View and manage vulnerabilities

View and manage tasks and migrations

Plan

View and manage requests

View and manage pending tasks

View and manage reservation violations

View and manage port balance violations

Perform

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

View and manage performance policies and violations

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

Feature (admin)	With Perform license	Without Perform license
Application	Yes	No performance data or charts; no anomaly detection-related widgets
Virtual machine	Yes	No performance data or charts
Hypervisor	Yes	No performance data or charts
Host	Yes	No performance data or charts
Datastore	Yes	No performance data or charts
VMDK	Yes	No performance data or charts
Internal volume	Yes	No performance data or charts
Volume	Yes	No performance data or charts

Feature (admin)	With Perform license	Without Perform license
Storage pool	Yes	No performance data or charts
Disk	Yes	No performance data or charts
Storage	Yes	No performance data or charts
Storage node	Yes	No performance data or charts
Fabric	Yes	No performance data or charts
Switch port	Yes	No performance data or charts; “Port Errors” shows “N/A”
Storage port	Yes	Yes
NPV port	Yes	No performance data or charts
Switch	Yes	No performance data or charts
NPV switch	Yes	No performance data or charts
Search	Yes	Yes
Admin	Yes	Yes
Dashboard	Yes	Yes
Widgets	Yes	Partially available (only asset, query, and admin widgets are available)
Violations dashboard	Yes	Hidden
Assets dashboard	Yes	Partially available (storage IOPS and VM IOPS widgets are hidden)
Manage performance policies	Yes	Hidden
Manage annotations	Yes	Yes
Manage annotation rules	Yes	Yes
Manage applications	Yes	Yes
Queries	Yes	Yes
Manage business entities	Yes	Yes

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

Feature	User - with Perform license	Guest - with Perform license	User - without Perform license	Guest - without Perform license
Manage annotations	Yes	Hidden	Yes	Hidden
Manage applications	Yes	Hidden	Yes	Hidden
Manage business entities	Yes	Hidden	Yes	Hidden
Queries	Yes	View and edit only (no save option)	Yes	View and edit only (no save option)

Troubleshooting installations

OnCommand Insight installations are generally managed through the installation wizards. However, customers might experience problems during upgrades or with conflicts due to computer environments.

You should also be certain that you install all of the necessary OnCommand Insight licenses for installing the software.

Missing licenses

Different licenses are required for different OnCommand Insight functionality. What you see displayed in OnCommand Insight is controlled by your installed licenses. Refer to the OnCommand Insight licenses section for information on functionality controlled by each license.

Refer to the OnCommand Insight licenses section for information on functionality controlled by each license.

Disabling User Account Control (UAC) in Windows 2008

The UAC might cause the installation on Microsoft Windows 2008 to fail. Disabling it resolves the issue.

About this task

If you do not disable it, the OnCommand Insight installation in Windows 2008 can fail and show the following message: "There is a problem with this Windows Installer package. A program run as part of the setup did not finish as expected."

Note: This problem might relate to the installation of the OnCommand Insight Scrub utilities into your environment. See the "Scrubbing data for transfer to support" for more information about this feature.

Steps

1. Navigate to the Microsoft Windows **Control Panel > User Accounts**.
2. Turn "User Account Control" off.
3. Uncheck "Use user account control (UAC) to help protect your computer."
4. Reboot your computer.
5. Install OnCommand Insight.

6. After the installation is complete, enable UAC again.

Submitting an online technical support request

If you have problems with the Insight installation, as a registered support customer, you can submit an online technical support request.

Before you begin

Using your corporate email address, you must register as a support customer to obtain online support services. Registration is performed through the support site (http://support.netapp.com).

About this task

To assist customer support in solving the installation problem, you should gather as much information as possible, including these items:

- Insight serial number
- Description of the problem
- All Insight log files
- Screen capture of any error messages

Steps

1. Create a `.zip` file of the information you gathered to create a troubleshooting package.
2. Log in to the support site at *mysupport.netapp.com* and select **Technical Assistance**.
3. Click **Open a Case**.
4. Follow the instructions to your package of data.

After you finish

You can use **Check Case Status** on the Technical Assistance page to follow your request.

Upgrading OnCommand Insight

Upgrading Insight to a current release requires planning, preparation, the upgrade itself, and some post-upgrade procedures. It involves upgrading the Insight client, Data Warehouse, and Remote Acquisition Unit(s), if you have any in your environment; you must upgrade each component independently and all components must be running the same version of Insight.

Unless otherwise indicated, the requirements and procedures apply to upgrading from Insight 6.4.x to 7.2.x. If you are upgrading from a version prior to 6.4, contact your account representative.

Note: For Data Warehouse and remote acquisition units to operate with an Insight client, they must be all running the same version of Insight.

Overview of the OnCommand Insight upgrade process

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

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

- Downloading the installation packages
- Backing up the Data Warehouse database
  To avoid the possibility of misreporting data, you must back up the Data Warehouse database before you back up the Insight client database.
- Backing up the Insight client database
  The database is automatically backed up when you perform the in-place upgrade. It is a best practice to back up the database before the upgrade, and place the backup in a location other than on the Insight server. During the upgrade process, Insight does not collect new data. To minimize the amount of data that is not collected, you must start the database backup within an hour or two of your planned upgrade time.
- Backing up any custom Data Warehouse reports
  When you back up the Data Warehouse database, custom reports are included. The backup file is created on the Data Warehouse server. It is a recommended best practice to back up the custom reports to a location other than the Data Warehouse server.
- Uninstalling the Data Warehouse and the Remote Acquisition Unit software, if applicable
  The Insight client has an in-place upgrade; you do not have to uninstall the software. The in-place upgrade backs up the database, uninstalls the software, installs the new version, and then restores the database.
- Upgrading the software on the Insight client, Data Warehouse, and Remote Acquisition Unit(s)
  All previously applied licenses remain in the registry; you do not have to reapply these licenses.
- Completing the post-upgrade tasks

OnCommand Insight upgrade checklist

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

Checklist for preparing for the upgrade (required)

Condition	Complete?
If your version of Insight is 6.4.x, 7.0, 7.0.1, or 7.0.2, you must upgrade to 7.0.3 or to 7.1 before you can upgrade to 7.2. You can obtain 7.0.3 or 7.1 from the support Downloads page.	
Ensure that you have Windows local administrator permissions, which are required to perform the upgrade process, on all Insight servers.	
If your Insight, Data Warehouse, or Remote Acquisition Unit servers reside on 32-bit platforms, you must upgrade your servers to 64-bit platforms. As of Insight 7.x, upgrades are only available for 64-bit platforms.	
Ensure that you have the necessary permissions to modify or disable the antivirus software on all the servers in your environment. To prevent an upgrade failure due to active virus scan software, you must exclude the Insight installation directory (*`disk drive`*`:\`*`install directory`*`\sanscreen` from access to antivirus scanning during the upgrade. After you upgrade all of the components, you can safely reactivate the antivirus software; however, ensure that you configure the scan to still exclude everything in the Insight installation directory.	

Checklist for preparing for the upgrade (best practice)

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

Condition	Complete?
Ensure that you have access to Firefox® or the Chrome™ browser when you back up the Insight and Data Warehouse databases. Internet Explorer is not recommended, because it experiences some issues when uploading and downloading files larger than 4 GB.	
Delete the `.tmp` files on the Insight server, which you can find in the following location: *`disk drive`*`:\`*`install directory`*`\SANscreen\jboss\server\onaro\tmp`.	
Remove duplicate data sources and decommissioned data sources from the Insight client. Removing decommissioned or duplicate data sources decreases the amount of time required to perform the upgrade and mitigates the opportunity for data corruption.	
If you have modified any of the default reports shipped with Insight, you should save the reports with a different name and then save them to the Customer Reports folder (7.0.x) or My Folders (6.4.x) folder so that you do not lose your modified report when you upgrade or restore the system.	
If you have any custom or modified Data Warehouse reports created by you or professional services, create a backup of them by exporting them to XML and then moving them to the Customer Reports (7.0.x) or My Folders (6.4.x) folder. Ensure that the backup is not located on the Data Warehouse server. If you do not move your reports to the recommended folders, these reports might not be backed up by the upgrade process. For earlier versions of Insight, failure to locate reports in the appropriate folders may result in the loss of custom and modified reports.	
Record all settings in the IBM Cognos Configuration utility, because these are not included in the Data Warehouse backup; you have to reconfigure these settings after the upgrade. The utility is located in the *`disk drive`*`:\`*`install directory`*`\SANscreen\cognos\c10_64\bin64` directory on the Data Warehouse server and you run it using the `cogconfigw` command. Alternatively, you can perform a complete backup of Cognos and then import all of your settings. Refer to the IBM Cognos documentation for more information.	
If you are upgrading from 7.0.2, ensure that you apply the latest patches for the release prior to upgrading. Running your systems with these patches for 7 days ensures that your switch port performance is not lost. Obtain the patch files from technical support.	

Checklist for preparing for the upgrade (if applicable)

Condition	Complete?
If you have replaced the self-signed certificates that the Insight installation created due to browser security warnings with certificates signed by your internal certificate authority, back up your keystore file, which is in the following location: *`disk drive`*`:\`*`install directory`*`\jboss\server\onaro\cert` and restore it after the upgrade. This replaces the self-signed certificates that Insight creates with your signed certificates.	

Condition	Complete?
If any of your data sources were modified for your environment and you are unsure if these modifications are available in the Insight version to which you are upgrading, make a copy of the following directory, which will help you troubleshoot if there are recovery issues: *disk drive*:*install directory*\sanscreen\jboss\server\onaro\deploy\datasources.war.	
Back up all custom database tables and views using the `mysqldump` command line tool. Restoring custom database tables requires privileged database access. Contact technical support for assistance with restoring these tables.	
Ensure that no custom integration scripts, third-party components required for Insight data sources, backups, or any other required data is stored in the *disk drive*:*install directory*\sanscreen directory, because the contents of this directory is deleted by the upgrade process. Ensure that you move any of these things from the `\sanscreen` directory to another location. For example, if your environment contains custom integration scripts, ensure that you copy the following file to a directory other than the `\sanscreen` directory: `\install_dir\sanscreen \jboss\server\onaro\deploy \datasources.war\new_disk_models.txt`.	

Related references

Insight Server requirements on page 11
Remote Acquisition Unit server requirements on page 13
Data Warehouse and Reporting server requirements on page 12

Downloading the OnCommand Insight installation packages

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

About this task

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

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

Steps

1. Open the Insight client by opening a web browser and entering one of the following:
   - On the Insight server:

     `https://localhost`
   - From any location:

     `https://IP Address:port or fqdn:port`

     The port number is either 443 or the port that was configured when the Insight client was installed. The port number defaults to 443 if you do not specify the port number in the URL.
2. Log in to the Insight client.

3. Click on the Help icon and select **Check for updates**.
4. If a newer version is detected, follow the instructions in the message box.

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

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

   Incomplete file transfers can cause issues with the upgrade process.

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

Backing up the databases

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

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

Backing up the Data Warehouse database

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

Steps

1. Log in to the Data Warehouse Portal at `https://fqdn/dwh`.
2. From the navigation pane on the left, select **Backup/Restore**.
3. Select **All Datamarts Including Performance Datamart**.
4. Click **Backup**.

   This operation can take 30 minutes or more.

   Data Warehouse creates a backup file and displays its name.
5. Right-click the backup file and save it to a location you want.

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

   The Data Warehouse backup file includes the DWH instance's MySQL; custom schemas (MySQL DBs) and tables; LDAP configuration; the data sources that connect Cognos to the MySQL database (not the data sources that connect the Insight client to devices to acquire data); import

and export tasks that imported or exported reports; reporting security roles, groups, and namespaces; user accounts; any modified Reporting Connection reports; and any custom reports, regardless of where they are stored, even in the My Folders directory. Cognos system configuration parameters, such as SMTP server setting, and Cognos custom memory settings are not backed up.

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

dwh_capacity	dwh_capacity_efficiency	dwh_capacity_staging	dwh_dimensions
dwh_fs_util	dwh_inventory	dwh_inventory_staging	dwh_inventory_transient
dwh_management	dwh_performance	dwh_performance_staging	dwh_ports
dwh_reports	dwh_sa	dwh_sa_staging	

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

information_schema	acquisition	cloud_model	host_data
innodb	inventory	inventory_private	inventory_time
logs	management	mysql	nas
performance	performance_schema	performance_views	sanscreen
scrub	serviceassurance	test	tmp
workbench			

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

- A daily backup `.zip` file, which contains Cognos report definitions
- A reports backup `.zip` file, which contains all the reports in Cognos, including those in the My Folders directory
- A Data Warehouse database backup file

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

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

Backing up the OnCommand Insight client database (7.0.x)

Back up the Insight client database to ensure that you have a recent backup if an issue occurs after the upgrade. During the backup and restore phase, data will be lost; thus, the backup should occur as close as possible to the upgrade time.

Steps

1. Open Insight in your browser.

2. Click **Admin** > **Troubleshooting**.
3. On the **Troubleshooting** page, click **Backup**.

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

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

Backing up the Insight client database (6.4.x)

Back up the Insight client database to ensure that you have a recent backup if an issue occurs after the upgrade. During the backup and restore phase, data will be lost; thus, the backup should occur as close as possible to the upgrade time.

Steps

1. Log in to the OnCommand Insight Portal as administrator at `https://fqdn/legacy`.
2. From the navigation pane on the left, click **Backup/Restore**.
3. In the **Manual** section, select **Assure and Perform** from the **Database** list.
4. Select **All** from the **Insight data** list.
5. Click **Backup Database to File**.
6. When prompted, save the file to a server other than the Insight server.

   During the backup process, do not perform any other OnCommand Insight tasks. The time to back up the database might vary depending on your available resources (architecture, CPU, and memory), the size of your database, and the number of objects monitored in your environment.

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

Backing up custom Data Warehouse reports

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

Steps

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

Performing the software upgrade

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

Upgrading the Insight client

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

Before you begin

The Insight installation package must be located on the server.

Steps

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

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

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

After you finish

To verify if the upgrade is successful or if errors are generated, check the upgrade log in the following location: *`disk drive`*`:\`*`install directory`*`\SANscreen\jboss\server\onaro\log`.

Upgrading Data Warehouse

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

Steps

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

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

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

After you finish

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

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

Preserving custom Cognos settings during a Data Warehouse upgrade

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

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

Upgrading remote acquisition unit servers

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

Before you begin

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

Steps

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

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

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

After you finish

- To verify if the upgrade is successful or if errors are generated, check the upgrade log in the following location: *`disk drive`*`:\`*`install directory`*`\SANscreen\jboss\server\onaro\log`.
- Clear your browser's cache and history to ensure that you are receiving the latest data from the server.

Upgrading the anomaly detection engine

Newer releases of OnCommand Insight may contain a new release of the anomaly detection engine. In order to preserve anomaly detection configuration data and anomaly score data following an upgrade of the software, you must follow these instructions. Refer to the release notes to determine whether your Anomaly detection needs to be upgraded.

Before you begin

- The system must be running OnCommand Insight 7.2 or later.
- The system must be running version 1.4.x or later of the anomaly detection engine.

About this task

Attention: Failure to execute the steps of this task in sequential order might result in the loss of the anomaly detection configuration data and anomaly score data stored on the Insight server.

Steps

1. Back up the existing version of OnCommand Insight to preserve the anomaly detection registrations, application monitoring, anomaly history, and so on.
2. Shut down the OnCommand Insight server.

   Attention: Failure to shut down the OnCommand Insight server before uninstalling the anomaly detection software results in the loss of the anomaly detection configuration data and anomaly score data stored on the Insight server.

3. Uninstall the anomaly detection software:

   ```
   sudo /usr/bin/oci-prelert-uninstall.sh
   ```

   The system displays a “failure to unregister” message. You can ignore this message.

4. Install the newer version of OnCommand Insight by using the upgrade process.

   See the OnCommand Insight Installation Guide for instructions.

5. Restart the OnCommand Insight server.

   The system reports that applications are “failing to monitor”. You can ignore these failures.

6. Install the new version of the anomaly detection software on a system that has the same IP address as the previous machine that was running the anomaly detection software:

   ```
   sudo /usr/bin/oci-prelert-install.sh
   ```

   The anomaly detection software is successfully registered with the OnCommand Insight server.

Completing post-upgrade tasks

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

Installing data source patches

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

Before you begin

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

Steps

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

   All data sources of the same type are updated with this patch. Insight automatically forces acquisition to restart when you add a data source. Discovery includes the detection of changes in network topology including the addition or deletion of nodes or interfaces.
8. To force the discovery process manually, click **Data Sources** and click **Poll Again** next to the data source to force it to collect data immediately.

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

Replacing a certificate after upgrading OnCommand Insight

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

Before you begin

The minimum encryption bit level is 1024 bits.

About this task

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

Steps

1. List the contents of the keystore:

   `C:\Program Files\SANscreen\java\bin>keytool.exe -list -v -keystore "c:\Program Files\SANscreen\jboss\server\onaro\cert\server.keystore"`

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

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

2. Delete the `ssl certificate`:

   `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles \SANscreen\jboss\server\onaro\cert\server.keystore`

3. Generate a new key:

   `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\jboss\server\onaro\cert \server.keystore"`

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

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

   - Country: two-letter ISO abbreviation for your country (for example, US)
   - State or Province: name of the state or province where your organization's head office is located (for example, Massachusetts)
   - Locality: name of the city where your organization's head office is located (for example, Waltham)
   - Organizational name: name of the organization that owns the domain name (for example, NetApp)
   - Organizational unit name: name of the department or group that will use the certificate (for example, Support)
   - Domain Name/ Common Name: the FQDN that is used for DNS lookups of your server (for example, www.example.com)

   The system responds with information similar to the following:
   `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`

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

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

4. Generate a certificate request file:

   `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen \jboss\server\onaro\cert\server.keystore" -file c:\localhost.csr`

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

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

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

6. Import the approved certificate:

   `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\jboss\server\onaro\cert\server.keystore"`

   a. When prompted for a password, enter the keystore password.

   The system displays the following message:
   `Certificate reply was installed in keystore`

7. Restart the SANscreen Server service.

Result

The web browser no longer reports certificate warnings.

Increasing Cognos memory

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

Steps

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

   cogconfigw

   The IBM Cognos Configuration window displays.

   Note: The IBM Cognos Configuration shortcut application points to *disk drive*:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat. If Insight is installed in the Program Files (space between) directory, which is the default, instead of ProgramFiles (no space), the .bat file will not work. If this occurs, right click the application shortcut and change cognosconfigw.bat to cognosconfig.exe to fix the shortcut.
4. From the navigation pane on the left, expand **Environment**, expand **IBM Cognos services**, and then click **IBM Cognos**.
5. Select **Maximum memory for Tomcat in MB** and change 768 MB to 2048 MB.
6. On the IBM Cognos Configuration toolbar, click  (Save).

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

Restoring the Data Warehouse database

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

About this task

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

Steps

1. Log in to the Data Warehouse Portal at https://*fqdn*/dwh.
2. From the navigation pane on the left, click **Backup/Restore**.
3. In the **Restore Database and Reports** section, click **Browse** and locate the .zip file that holds the Data Warehouse backup.

4. It is a best practice to leave both of the following options selected:
   - **Restore database**
     Includes Data Warehouse settings, data marts, connections, and user account information.
   - **Restore reports**
     Includes custom reports, predesigned reports, changes to predesigned reports that you made, and reporting settings you made in the Reporting Connection.
5. Click **Restore**.

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

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

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

After you finish

Restoring custom Data Warehouse reports

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

Steps

1. Open your report with a text editor, and then select and copy its contents.
2. Log in to the Reporting portal at `https://`*`fqdn`*`/reporting`.
3. On the Data Warehouse toolbar, click  to open the Insight Reporting portal.
4. From the Launch menu, select **Report Studio**.
5. Select any package.

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

   The **Open Report from Clipboard** dialog box displays.
9. From the File menu, select **Save As** and save the report to the Custom Reports folder.
10. Open the report to verify that it was imported.

    Repeat this task for each report.

    Note: You may see an "Expression parsing error" when you load a report. This means that the query contains a reference to at least one object that does not exist, which means there is no

package selected in the Source window to validate the report against. In this case, right-click on a data mart dimension in the Source window, select Report Package, and then select the package associated with the report (for example, the inventory package if it is an inventory report or one of the performance packages if it's a performance report) so Report Studio can validate it and then you can save it.

Verifying that Data Warehouse has historical data

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

Steps

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

Testing the connectors

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

Steps

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

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

   If it does not succeed, check the connection configuration and ensure the client does not have any issues.
7. Click **Test**.

   Data Warehouse tests the connection.

Verifying the Extract, Transform, and Load scheduling

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

Steps

1. Log in to the Data Warehouse portal at `https://fqdn/dwh`.
2. From the navigation pane on the left, click **Schedule**.
3. Click **Edit schedule**.
4. Verify that **Daily** is selected from the **Type** list.

   The best practice is to schedule ETL to run once a day.
5. Verify that the time selected is the time at which you want the job to run.

   This ensures that the build job runs automatically.
6. Click **Save**.

Updating disk models

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

Before you begin

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

Steps

1. Stop the SANscreen Acq service.
2. Navigate to the following directory: *`disk drive`*`:\`*`install directory`*`\SANscreen\jboss\server\onaro\deploy\datasources.war`.
3. Move the current `diskmodels.jar` file to a different location.
4. Copy the new `diskmodels.jar` file into the `datasources.war` directory.
5. Start the SANscreen Acq service.

Verifying that business intelligence tools are running

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

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

Troubleshooting an upgrade

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

Unable to start Cognos from the Windows Start menu

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

"Not a valid win32 application" error message

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

Annotations are not present

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

Differences in values displayed in reports

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

Data does not display in reports

In 7.0.1, several model names were changed (for example, Symmetrix was changed to Symmetrix VMAX). As a result, if a report contains a filter for "Symmetrix", you will not see any data when you run the report. To change the report, you must open the report with Query Explorer in Report Studio, search for the model name, replace it with the new model name, and save the report.

Uninstalling the software

You must uninstall the old versions the Data Warehouse and Remote Acquisition software to install the new versions. You should do this before you attempt to upgrade any of these components. The client software on the Insight server is uninstalled during the in-place upgrade.

Uninstalling the OnCommand Insight Server

You can uninstall the OnCommand Insight server if needed.

Before you begin

Best practice: before uninstalling Insight, back up the OnCommand Insight database.

Steps

1. Log in to the OnCommand Insight server using an account with administrator privileges.
2. Ensure that all of the Insight windows on the server are closed.
3. Open the **Uninstall a Program** feature from the control panel and select the OnCommand Insight application for removal.
4. Click **Uninstall** and follow the prompts.

Uninstalling the Data Warehouse software

You must uninstall the Data Warehouse software before you can upgrade.

Before you begin

If you made changes to reports you want to keep, it is critical that you create a backup before you uninstall Data Warehouse. Uninstalling Data Warehouse permanently deletes all previously collected data and removes all reports, including any newly created or edited reports.

Steps

1. Log in to the Data Warehouse server.
2. Ensure that all of the Insight windows on the server are closed.
3. Open the **Uninstall a Program** feature from the control panel and select the OnCommand Insight application for removal.
4. Click **Uninstall** and follow the prompts.

   Important: When the uninstall operation is complete, reboot the Data Warehouse server.

Uninstalling the remote acquisition unit software

You must uninstall the existing version of the remote acquisition unit software before you can upgrade to a new version. You should perform this task on all remote acquisition unit servers in your environment.

Steps

1. Log in to the remote acquisition unit server.
2. Ensure that all of the OnCommand Insight windows on the server are closed.
3. Click  , select **Control Panel**, and then click **Programs and Features**.
4. Select the OnCommand Insight Remote Acquisition Unit program, and then click **Uninstall**.

   This takes approximately 5 minutes to finish.

Copyright information

Trademark information

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., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

E

F

H

I

J

L

M

N

O

V

W