HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

Getting Started Guide: Device Configuration Supplement

FASTFIND LINKS

Hitachi Data Systems

MK-90IOS006-12

Contents

Preface

This guide is a supplement to the Hitachi IT Operations Analyzer Getting Started Guide: It will assist you with the pre-installation setup tasks for the network components that your site intends to monitor.

This preface includes the following information:

- Intended audience
- Product version
- Document revision level
- Related documents
- Document conventions
- Getting help
- Comments

Intended audience

This document is intended for system administrators and other users who are responsible for configuring and operating Hitachi IT Operations Analyzer.

Product version

This document revision applies to IT Operations Analyzer version 3.3.1.

Document revision level

This section provides a history of the revisions to this document.

Revision	Date	Description
MK-90IOS006-00	March 2010	Initial Release
MK-90IOS006-01	October 2010	Revision 1, supersedes and replaces MK-90IOS006-00
MK-90IOS006-02	October 2010	Revision 2, supersedes and replaces MK-90IOS006-01
MK-90IOS006-03	January 2011	Revision 3, supersedes and replaces MK-90IOS006-02
MK-90IOS006-04	April 2011	Revision 4, supersedes and replaces MK-90IOS006-03
MK-90IOS006-05	October 2011	Revision 5, supersedes and replaces MK-90IOS006-04
MK-90IOS006-06	February 2012	Revision 6, supersedes and replaces MK-90IOS006-05
MK-90IOS006-07	June 2012	Revision 7, supersedes and replaces MK-90IOS006-06
MK-90IOS006-08	November 2012	Revision 8, supersedes and replaces MK-90IOS006-07
MK-90IOS006-09	November 2012	Revision 9, supersedes and replaces MK-90IOS006-08
MK-90IOS006-10	March 2013	Revision 10, supersedes and replaces MK-90IOS006-09
MK-90IOS006-11	June 2013	Revision 11, supersedes and replaces MK-90IOS006-10
MK-90IOS006-12	July 2013	Revision 12, supersedes and replaces MK-90IOS006-11

Related documents

- *Hitachi IT Operations Analyzer Getting Started Guide: Device Configuration Supplement*, MK-90IOS006
- Hitachi IT Operations Analyzer Help
- Release Notes, RN-99IOS004

Document conventions

The following symbols are used to alert you to important information.

Symbol	Meaning	Description
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Note	Notes emphasize or supplement important points of the main text.

The following typographic conventions are used in this document.

Convention	Description
Bold	Indicates text in a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. In the case of version information, the italic x represents all subsequent versions. Examples: • Copy *source-file target-file*. • Kernel version 2.6.*x*. **Note**: Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or is entered by the user. Example: `# pairdisplay -g oradb`
angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` **Note**: Italic font is also used to indicate variables.

Product references

In this manual, there are references to VMware® products. Those references are handled as follows:

- Reference to the product when the type/version is specific; for example: VMware ESX 3, VMware ESX 3i, VMware ESX 4.0, etc.
- Reference to the product server when the server type/version is non-specific: ESX Server

Getting help

If you purchased this product and have a current product support agreement, then please collect the following information:

- The product name and version number
- The operating system name and revision or service pack number
- The serial number of the license for which you are requesting help
- The content of any error message(s) that are displayed
- The circumstances surrounding the error or failure
- A description of the problem and what has been done to try to solve it

After you collect this data, contact the Hitachi Data Systems Support Center.

Following is a link to the Hitachi Data Systems Web site, where you can obtain current telephone numbers and other contact information for the Hitachi Data Systems Support Center:

https://portal.hds.com

NOTE: If you are working with a trial version of the product, then please refer to the self-service materials that are located on the IT Operations Software Portal: http://www.itoperations.com

Comments

Please send us your comments about this document: doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

1

Overview

Before installing IT Operations Analyzer or using the Discovery Wizard, it is important to check and prepare your environment. This involves verifying the settings that are used in your environment, and collecting information that will be necessary later on, during the setup procedures.

Preparing your environment

Table 1-1 describes the tasks that are required, and those that are either recommended or optional, based on your environment and monitoring objectives.

For each task, there is a reference to the chapter that contains details.

Table 1-1: Environment Preparations

Required Tasks	
Task	**Details**
At the management server (the machine on which IT Operations Analyzer is installed), check DCOM settings for WMI.	Prevent WMI remote connection errors from occurring because remote execution of DCOM is not permitted. See Chapter 2, Preparing WMI for Windows servers.
If your site uses any of the following monitoring targets, then you must set them up:	Monitoring targets are the servers, storage, and switches that your site intends to monitor.
• IP Switches	IT Operations Analyzer uses SNMP to monitor IP switches. • Enable SNMP • Obtain the SNMP community string • Obtain the IP address See Chapter 5, Preparing SNMP for IP switches.
• Hitachi 9500V	IT Operations Analyzer monitors Hitachi 9500V through Device Manager's SMI-S agent. Performance is not monitored. Install Device Manager 5.9 or later and enable SMI-S. See Chapter 6, Preparing Hitachi storage.
• Hitachi USP VM	IT Operations Analyzer monitors Hitachi USP VM through Device Manager's SMI-S agent. Install Device Manager 6.2 or later and enable SMI-S. See Chapter 6, Preparing Hitachi storage.

• Other storage, FC switches	IT Operations Analyzer uses SMI-S to discover and monitor other storage and FC switches. Install the SMI-S agent, then obtain the following:
	• IP address
	  • SMI-S agent (proxy): Use an IP address of the SMI-S server for the switch.
	  • SMI-S agent (embedded): Use the same IP address for the FC switch.
	• User ID and Password
	• Port number
	• Namespace
	Also, check the SSL status.
	See Chapter 7, Reviewing the SMI-S preparations.
	When specifying credentials for NetApp FAS series or when managing Linux versions using an SMI-S agent, we recommend specifying **http** for the **SSL**, in the **Add Credential** dialog.

Table 1-1: Environment Preparations

Recommended Tasks	
Task	**Details**
Check monitoring targets: • Windows servers	IT Operations Analyzer uses WMI to monitor Windows servers. For remote access to WMI, DCOM must be enabled at the Windows server and at the management server. If DCOM is not enabled, then the software may be unable to discover or monitor Windows servers. Also, install the Integration Service on a virtual machine if your site will monitor a Hyper-V virtual machine. See Chapter 2, Preparing WMI for Windows servers.
• Linux/Solaris servers	IT Operations Analyzer uses SSH to discover Linux and Solaris servers. It also uses password authentication (not certificate authentication), to monitor them. Verify that: • SSH service is installed and running. • SSH2 connection is enabled. • Password authentication is permitted. See Chapter 3, Preparing SSH for Linux/Solaris servers.
• VMware ESX Servers	IT Operations Analyzer cannot correctly monitor Windows or Linux servers on virtual machines unless VMware tools are installed. Verify the supported version: • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4 • VMware ESX 4i • VMware ESX 4.1 • VMware ESX 4.1i • VMware ESX 5 • VMware ESX 5i • VMware ESX 5.1 • VMware ESX 5.1i Also, install VMware Tools on virtual machines. See Chapter 4, Preparing VMware ESX servers.
• Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series	Check whether account authentication or password protection is enabled. If account authentication or password protection is enabled, then IT Operations Analyzer needs the User ID and Password. See Chapter 6, Preparing Hitachi storage.

Table 1-1: Environment Preparations

Recommended Tasks	
Task	**Details**
• Dell servers	By using the built-in Dell Chassis plug-in, Dell server-specific information can be acquired. "Dell Chassis (Windows)" is installed as a plug-in for Windows and "Dell Chassis (Linux)" is installed as a plug-in for Linux. Following are the system requirements for Dell servers that are monitored by IT Operations Analyzer: • Dell OpenManage Server Administrator (OMSA) Versions 6.1.0 or 6.2.0 must be running on the monitored Dell server(s). • SNMP agent is installed and running on the monitored Dell server(s). • "Dell Chassis (Windows)" requires that the DSM SA Data Manager service is running on Microsoft Windows Server. • "Dell Chassis (Linux)" requires that the dsm_sa_datamgrd or dsm_sa_datamgr32d process is running on Red Hat Enterprise Linux Server. For operating system requirements for Linux-based and Windows-based Dell servers, refer to the Linux servers and Microsoft Windows servers setup tasks.
Optional Tasks	
Task	**Details**
Check monitoring targets: • Windows servers	IT Operations Analyzer uses WMI to monitor Windows servers. Windows 2003 must have FCInfo installed to provide FC HBA data through WMI. If your Windows servers use an FC HBA, then install FCInfo. See Chapter 2, Preparing WMI for Windows servers.
• IP Switches	Enable sending of SNMP traps. IT Operations Analyzer can receive SNMP traps from IP switches. This task is optional because IT Operations Analyzer can monitor IP switches without traps, by using polling. See Chapter 5, Preparing SNMP for IP switches.

2

Preparing Hyper-V and WMI for Windows servers

IT Operations Analyzer uses WMI to monitor Windows servers. For remote access to WMI, DCOM must be enabled at the Windows server and at the management server. If DCOM is not enabled, then the software may be unable to discover or monitor Windows servers. This chapter describes the Hyper-V and WMI environment preparations.

Preparing Hyper-V

If your site plans to monitor a Windows or Linux server that is installed on a Hyper-V virtual machine, then you need to install the "Integration Service" on the virtual machine's OS. Otherwise, if the Integration Service is not installed, neither the state of the virtual machine, nor the relationship between the host machine and guest OS are correctly displayed within IT Operations Analyzer.

NOTE: The Hyper-V host machine setup is similar to the preparations for the Windows server. For reference, see the next section, below.
Also, if KB2264080 is not applied to Windows Server 2008 R2 for the host OS of the management target, then it may not be possible to connect to the guest OS of the management target Hyper-V when:
-there are a lot of sessions on the VM of the Hyper-V.
-transmitting a large amount of data to the VM of the Hyper-V.

Preparing WMI for Windows servers

IT Operations Analyzer discovers and monitors Windows servers through Windows Management Instrumentation (WMI). The following sections describe the tasks that are associated with enabling remote access to WMI, and configuring Windows 2003/2003 R2 servers that use FC Host Bus Adaptors (HBAs).

NOTE:

- For Microsoft Hyper-V nodes and Windows Server nodes, you can acquire performance information about the hard disk by FC connection, iSCSI connection, and local connection. Performance information about the CD-ROM or USB memory cannot be acquired. When performance information cannot be acquired, then in the **Performance** tab of the **Monitoring** module, the icon for the performance metric indicates Unknown.
- For Windows Server 2003, please apply KB953955. Otherwise, incorrect values may be reported for the CPU name.

Preparing the Management server

To monitor Windows computers or storage servers, DCOM must be enabled on the Management server. See Permitting remote execution of DCOM on page 2-4.

Preparing the Windows computers and Windows storage server

Table 2-1 lists the information that is necessary for monitoring.

Table 2-1: Information for Connecting to Windows Servers

Item	Details
IP address	The IP address of the Windows server to be monitored.
User name	A user account with Administrator privileges for the Windows server to be monitored.
Domain name	The user's domain name (if the user account described above is a domain user).
Password	The password that is associated with the User name.

To monitor Windows servers, DCOM must be validated, and any WMI exceptions must be added to the Windows firewall. If you plan to acquire FC HBA information using Windows Server 2003 or 2003 Windows Server R2, then install the Fibre Channel Information tool (fcinfo).

Installing the Fibre Channel Information Tool (fcinfo)

The fcinfo tool is required when using a host bus adapter (HBA) to connect fibre channel SAN disk devices to the server you want to monitor. It supports the fibre channel's HBA API in Windows, and it provides WMI-compliant functions. Refer to the Microsoft Download Center Web site: http://www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

Adding a WMI exception to the Windows firewall

You can change permissions from either the Windows command prompt or by using the Group Policy editor. The following instructions apply to Windows Server 2003. For Windows Server 2008 or Windows Server 2012 details, see Applying Windows Server 2008 or Windows Server 2012 configuration settings on page 2-5.

Using the Windows command prompt:

1. After logging on to the server, click **Start**, then **Run**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** and **Run** commands are different.

2. At the prompt, type **cmd**, then click **OK**.
3. At the command prompt, type the following, then press **Enter**:
   `netsh firewall set service RemoteAdmin enable`

Using a Group Policy editor:

1. After logging on to the server, click **Start**, then **Run**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** and **Run** commands are different.

2. To launch the **Group Policy** editor, type **gpedit.msc**, then click **OK**.
3. Under **Local Computer Policy**, expand the **Administrative Templates** folder.
4. Expand the folders: **Network**, **Network Connections**, and **Windows Firewall**, then select **Domain Profile**.
5. In the settings list, right-click on **Windows Firewall: Allow remote administration exception**, then click **Properties**.
6. Click **Enabled**, then **OK**.

NOTE: Refer to the Microsoft Developer Center Web site for details: http://msdn2.microsoft.com/en-us/library/aa389286(VS.85).aspx

Permitting remote execution of DCOM

By executing dcomcnfg.exe from the Windows command prompt, you can launch the Component Services panel, and confirm the DCOM status.

1. After logging on to the server, click **Start**, then **Run**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** and **Run** commands are different.

2. To launch **Component Services**, type **dcomcnfg.exe**, then click **OK**.
3. From **Component Services**, select **Computers**, then **My Computer**.
4. Right-click on **My Computer** and select **Properties**.
5. Click the **Default Properties** tab.
6. Check the box, **Enable Distributed COM on this computer**, then click the **COM security** tab.
7. To display the **Launch Permission** dialog, click **Edit Limits** for **Launch and Activation Permissions**. If a user name or group is not displayed in the **Group or user names** box, then do the following:
   a. Click **Add**.
   b. In the **Select Users, Computers, or Groups** dialog, add the user name and group to the **Enter the object names to select** box. Click **OK**.
   c. In the **Launch Permission** dialog, click the user and group in the **Group or user names** area. In the **Permissions for User** area, for **Remote Launch**, check the box in the **Allow** column. Click **OK**.

Applying Windows Server 2008 or Windows Server 2012 configuration settings

If you are using a Windows Server 2008 or Windows Server 2012, then in addition to the Windows server settings described in the previous sections, any one of the following is required:

- Use the built-in administrator account
- Use a domain user account
- Enable WMI remote connection by using a local administrator account

Enabling local administrator accounts for WMI remote connection

You can change the User Account Control (UAC) setting from either the Control Panel of the monitoring target computer, or by applying setting methods from the registry.

To change the UAC from the Control Panel:

1. From the **Start** menu, click **Control Panel**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** menu is different.

2. Select **User Accounts** and choose **Change User Account Control settings**.
3. Set the UAC level to **Never notify**.
4. Restart the computer.

As another method for monitoring a target computer, register the **LocalAccountTokenFilterPolicy** key in the Registry, and set it up as **1**, on the monitoring target computer. Afterward, disable **Filtering by UAC**, which prevents local administrator privileges during WMI remote connection.

By using a local administrator account, you can manage both Windows server 2003 and Windows Server 2008 or Windows Server 2012. If you edit the Registry, then a critical error might occur, which can seriously affect the entire system. We recommend that you back up the Registry before editing it.

For details, refer to the following URL, which provides a description of UAC and remote restrictions in Windows Vista:
http://support.microsoft.com/kb/951016/en-us

When configuring the Registry, either use the:

- Registry Editor, or the
- “reg” command

Using the Registry Editor:

1. Click **Start**, then **Run**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** and **Run** commands are different.

2. At the prompt, type **regedit**, then click **OK**.

   The **Registry Editor** displays.

3. Locate the following Registry sub key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
4. If the **LocalAccountTokenFilterPolicy** key does not exist, then add it:
   a. From the **Edit** menu, select **New** then **DWORD**.
   b. Type **LocalAccountTokenFilterPolicy**, then press **Enter**.
5. If the value of **LocalAccountTokenFilterPolicy** is not **1**, then change it to **1**:
   a. Right-click on **LocalAccountTokenFilterPolicy**, and select **Modify**.
   b. Type **1** in the input dialog, then click **OK**.
6. Close the **Registry Editor**.

Using the reg Command:

1. Click **Start**, then **Run**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** and **Run** commands are different.

2. At the prompt, type the following:
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
3. Click **OK**.

Checking if duplicate network adapter names exist in the Device Manager tree of the node

If duplicate Network Adapter names exist in the Device Manager tree of the node, IT Operations Analyzer will not be able to correctly display the following performance information:

- network average packet reception amount [packet/second]
- network average packet send amount [packet/second].

To check if duplicate Network Adapter names exit in the Device Manager:

1. Click **Start** > **My Computer** > **View system information**. The **Systems Properties** pop-up menu displays.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** menu is different.

2. Click the **Hardware** tab.
3. Click **Device Manager**.
4. Check the **Device Manager** tree to see if duplicate names appear in the **Network adapters** section.

NOTE: If duplicate Network adapter names are listed, you will not be able to view the accurate network average packet send amount [packet/second] performance information. There will be a difference between the actual value and the displayed performance information. It is recommended that you check with your IT services group to rename the Network adapter devices to avoid any duplication.

3

Preparing SSH for Linux/ Solaris servers

IT Operations Analyzer uses SSH to discover Linux and Solaris servers. It also uses password authentication (not certificate authentication), to monitor them. This chapter describes how to configure your Linux and Solaris servers.

- Installing the required packages
- Obtaining connection settings based on the login method
- Applying SSH server security settings

Installing the required packages

For CentOS, prerequisite and required packages must be installed.

Table 3-1: Example packages to add for CentOS

Package	Commands included in the package that IT Operations Analyzer executes
smartmontools	/usr/sbin/smartctl
nfs-utils	/usr/sbin/exportfs
pciutils	/sbin/lspci
iscsi-initiator-utils	/sbin/iscsid

For SUSE Linux 11 SP1 and SP2, prerequisite and required packages must be installed.

Table 3-2: Example package to add for SUSE Linux 11 SP1 and SP2

Package	Commands included in the package that IT Operations Analyzer executes
nfs-kernel-server	/usr/sbin/exportfs

Obtaining connection settings based on the login method

There are different login methods, using SSH, by which information can be obtained from the Linux or Solaris server:

- As **root user**, you can log in directly using SSH
- As a **normal user**, after logging in using SSH, run the:
  - su command for root privileges.
  - sudo/pfexec command for root privileges.

For each login method, certain connection settings are necessary. Those settings are described in the following sections.

NOTE: For Linux/Solaris nodes, performance information about the mount point can be acquired with read/write permissions. Performance information about the Windows partition and CD-ROM drive cannot be acquired with read permissions. When performance information cannot be acquired, then in the **Performance** tab of the **Monitoring** module, the icon for the performance metric indicates Unknown.

Settings for the root User connection method

The following configuration is required:

- Enable connection using SSH2
- Permit SSH password authentication
- Permit root login using SSH

Table 3-3: Linux/Solaris Server Connection Settings (root Users)

Setting	Details
IP address	Specify the IP address of the Linux/Solaris server to be monitored.
Port Number	Specify the SSH port number of the Linux/Solaris server to be monitored.
User Name	Specify `root`.
Password	Specify the root password.
root password	Specify blank.

Settings for the Normal User connection method (su command)

The following configuration is required:

- Enable connection using SSH2
- Permit SSH password authentication

Table 3-4: Linux/Solaris Server Connection Settings (su Command)

Setting	Details
IP address	Specify the IP address of the Linux/Solaris server to be monitored.
Port Number	Specify the SSH port number of the Linux/Solaris server to be monitored.
User Name	Specify the User ID that was used for the login.
Password	Specify the password that is associated with the User ID.
root password	Specify the root password.

Settings for the Normal User connection method (sudo command)

The following configuration is required:

- Enable connection using SSH2
- Permit SSH password authentication
- Add definitions of the sudo/pfexec settings. For information, see Adding the sudo settings definition (Linux) on page 3-7.
- Add the definitions for the Profile, for Solaris. For information, see Adding the profile for pfexec (Solaris) on page 3-9.

Table 3-5: Linux/Solaris Server Connection Settings (sudo Command)

Setting	Details
IP address	Specify the IP address of the Linux/Solaris server to be monitored.
Port Number	Specify the SSH port number of the Linux/Solaris server to be monitored.
User Name	Specify the User ID that was used for the login.
Password	Specify the password that is associated with the User ID.
root password	Specify blank.

NOTE: Following are some security items to consider when using SSH:

- Permitting root login is the simplest way to configure; however, just leaking the root password to the public might cause the falsification of server settings. This method should be permitted only if the environment can prevent unauthorized access.
- Letting a normal user execute `su root` with root login prohibited is more secure than permitting root login, except if a normal user's ID and password are leaked to the public.
- The SSH1 protocol has more risk of sniffing than the SSH2 protocol, which is why the SSH2 protocol is recommended.
- When password authentication is permitted, there is more vulnerability than permitting only the public key authentication. Because IT Operations Analyzer cannot handle the public key authentication, using ports other than port 22 provides more security with password authentication.

Applying SSH server security settings

This section provides instructions for:

- Enabling the SSH2 connection
- Permitting SSH password authentication
- Permitting root login using SSH
- Adding the sudo Settings Definition (Linux)
- Adding the profile for pfexec (Solaris)

Before you begin

- Verify that SSH service (sshd daemon) is installed and running.
- If you use other SSH software, then refer to the software manual, and configure the equivalent settings. Linux contains OpenSSH.
- Prepare the environment where you can log in to the monitoring-target server and operate the system shell.
- Log in from the server console, or log in remotely using SSH or telnet. We recommend logging in from a local console, to prevent reconnection failures (if mistakes exist in the configuration settings).
- Prepare the root password (root privilege is required).
- After logging in as a root user or as a normal user, acquire the root privilege by using the `su root` command.

Enabling the SSH2 connection

1. Open **/etc/ssh/sshd_config** using an editor.
2. In **sshd_config**, search the file using the **Protocol** keyword.
   - If there is no description or if **Protocol** has been commented out, then SSH1 and SSH2 are enabled. No changes are necessary.
   - If **Protocol 1** is located, then only SSH1 is enabled. Change **Protocol 1** to **Protocol 1, 2**.
   - If **Protocol 2** is located, then only SSH2 is enabled. No changes are necessary.
   - If **Protocol 1, 2**, or **Protocol 2, 1** is located, then both SSH1 and SSH2 are enabled. No changes are necessary.
3. Save the file, and close the editor. To check for any errors with your settings, run the command, as appropriate:

   Linux: `/usr/sbin/sshd -t`

   Solaris: `/usr/lib/ssh/sshd -t`

   - Nothing is displayed if there are no errors in syntax or range.
   - An error message displays if there are errors in syntax or range.

Example of an incorrect Protocol (Protocol 2, 3) setting:

```
[root@linuxhost ssh]# /usr/sbin/sshd -t
ignoring bad proto spec: '3'.
```

4. Restart the SSH service, by executing the appropriate command:
   - Linux: `service sshd restart`
   - Solaris 9: `/etc/init.d/sshd restart`
   - Solaris 10: `svcadm restart ssh`
5. If **OK** is displayed for **Stopping / Starting**, the service is running normally; for example: `Stopping sshd: [ OK ]`

Permitting SSH password authentication

NOTE: For information about editing **/etc/ssh/sshd_config** and restarting the SSH service, refer to the previous section, Enabling the SSH2 connection.

In **/etc/ssh/sshd_config**, search the file by the keyword, **PasswordAuthentication**.

- If there is no description or if **PasswordAuthentication** has been commented out, then password authentication is enabled. No changes are necessary.
- If **PasswordAuthentication no** is located, then password authentication is prohibited (Only Public Key Authentication is enabled). Change it to **PasswordAuthentication yes**.
- If **PasswordAuthentication yes** is located, then password authentication is allowed. No changes are necessary.

Permitting root login using SSH

NOTE: For information about editing **/etc/ssh/sshd_config** and restarting the SSH service, refer to the previous section, Enabling the SSH2 connection.

In **/etc/ssh/sshd_config**, search the file by the keyword, **PermitRootLogin**.

- If there is no description or if **PermitRootLogin** has been commented out, then root login is enabled, by default. No changes are necessary.
- If **PermitRootLogin no** is located, then root login is prohibited (only normal users are permitted). Change it to **PermitRootLogin yes**.
- If **PermitRootLogin yes** is located, then root login is permitted. No changes are necessary.

Adding the sudo settings definition (Linux)

The **sudo** settings are described in the **/etc/sudoers** file. Only edit the file using the **visudo** command, because it provides exclusion control and syntax check.

1. Run the **visudo** command. If it starts normally, an editor opens.

NOTE: If **visudo** is executed simultaneously in different places, then an error message is displayed, and the editor will not be started:

```
[root@linuxhost ssh]# visudo
visudo: sudoers file busy, try again later
```

If the error message displays but the command was not run simultaneously, then at the command's previous execution, the connection may have been terminated, but the process is still running. In this case, kill the **visudo** process.

2. Add lines to enable users to run the commands without a password.

RedHat Linux 5.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
```

RedHat Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

SUSE Linux 10:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/usr/sbin/ethtool
```

SUSE Linux 11:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
```

SUSE Linux 11 SP1 and SP2:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
/usr/sbin/exportfs
```

CentOS and Oracle Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

For example, if a user name that is used for the connection is **sshconn** and the applicable server name is **linuxhost**, then specify the following script to /etc/sudoers of SUSE Linux 11:

```
sshconn linuxhost=NOPASSWD: /usr/sbin/dmidecode
sshconn linuxhost=NOPASSWD: /usr/sbin/smartctl
sshconn linuxhost=NOPASSWD: /bin/cat
sshconn linuxhost=NOPASSWD: /sbin/ethtool
```

3. Save the file, and close the editor.

   If there is a syntax error, an error message displays and the save is deferred.

   - When entering **e**, the editor will be started again. Modify it and save the change.
   - When entering **x**, the change is abandoned, and you can revert to the status before running visudo.
   - When entering **Q**, forcibly save the change even if it is incorrect. For example, if you make a mistake when typing NOPASSWD, the following error message is displayed:

     ```
     Warning: undeclared Cmnd_Alias `NOOPASSWD' referenced
     near line 92
     >>> sudoers file: syntax error? line 91 <<<
     What now?
     ```

NOTE: Use caution when forcibly saving changes for which you may be unfamiliar with the outcome. If you are unsure of the result, do not forcibly apply the change.

Adding the profile for pfexec (Solaris)

To give a root authority by using pfexec, add the profile to **/etc/security/prof_attr** and **/etc/security/exec_attr**, then assign the profile to the user.

1. Run `vi /etc/security/prof_attr`.
   - If it starts correctly, the editor opens.
   - If an error message is displayed, but a command is not executed at the same time, then the connection might have been curtailed when the command was previously run, causing the process to remain. In this case, kill the **vi** process.
2. Register the profile. For example, if the profile name is set to HITOA, it will be indicated as follows: **HITOA::::**
3. Save the file, and exit the editor.
4. Run `vi /etc/security/exec_attr`. If it starts correctly, the editor opens.
5. Add the following four lines to run the commands without a password:

   ```
   /sbin/ifconfig
   /usr/sbin/prtvtoc
   /usr/sbin/luxadm
   /usr/sbin/iscsiadm
   ```

   For example, if the profile name has been set to **HITOA**, the description will be as follows:

   ```
   HITOA:suser:cmd:::/sbin/ifconfig:euid=0
   HITOA:suser:cmd:::/usr/sbin/prtvtoc:euid=0
   HITOA:suser:cmd:::/usr/sbin/luxadm:euid=0
   HITOA:suser:cmd:::/usr/sbin/iscsiadm:euid=0
   ```
6. Save the file and exit the editor.
7. Allocate the profile to the user. For example, if the user name has been set to **sshconn**, the following command should be used:
   `usermod –P HITOA sshconn`

4

Preparing VMware ESX servers

IT Operations Analyzer cannot correctly monitor Windows or Linux servers on virtual machines unless VMware tools are installed. This chapter describes how to prepare your ESX Servers.

- Obtaining ESX server connection information
- Installing VMware Tools on virtual machines

Obtaining ESX server connection information

The following table describes the information that is necessary when connecting to an ESX Server. Note that for the discovery process, no additional credentials are required (only the user name and password information, as described in Table 4-1).

Table 4-1: Information for Connecting to VMware ESX Servers

Item	Details
IP address	Use the IP address of the ESX Server.
Port number	Specify the port number that is used by the ESX Server.
Protocol	Depending on the configuration of the ESX Server, use either http or https.
User name	Use the administrator user name for the ESX Server.
Password	Use the password for the ESX Server.

Installing VMware Tools on virtual machines

If you are planning to monitor Windows server or Linux server virtual machines, then you must install VMware Tools on each Guest OS of the virtual machine, in order to obtain information from the ESX Server.

When VMware Tools is not installed, neither the state of a virtual machine, nor the relationship between the host machine and the guest OS are correctly displayed.

Note that the Guest OS is managed as an individual node.

For information about the installation of these tools, please refer to the ESX Server product manual, *Basic System Administration*, which is available at the following Web site:

http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_admin_guide.pdf

When a free version of ESX is targeted for management, it may not be possible for IT Operations Analyzer to accurately acquire the state of the disk.

NOTE: IT Operations Analyzer does not support monitoring of a VMware ESX server that serves as an enabled distributed virtual switch. However, when IT Operations Analyzer recollects or updates the configuration information of an enabled distributed virtual switch per schedule, any change event information of the VM kernel NIC belonging to the distributed virtual switch and the service console NIC will be reported.

5

Preparing SNMP for IP switches

IT Operations Analyzer can receive SNMP traps from IP switches. This chapter describes how to configure your IP switches.

Overview

IT Operations Analyzer can monitor the IP switches in your environment provided that they are set up as follows:

- SNMP version 1 is installed and running.
- MIB-II is Readable by using your community name.
- Bridge MIB is Readable by using your community name.

To monitor IP switches, the information that is outlined in Table 5-1 and Table 5-2 is necessary.

Table 5-1: Information for Connecting to IP Switches: SNMP version 1 or 2c

Item	Details
IP address	The address of the SNMP IP switch node.
Port number	The port where the SNMP IP switch waits for the communication (port 161).
Community name	The Community name used for SNMP IP switches.

Table 5-2: Information for Connecting to IP Switches: SNMP version 3

Item	Details
IP address	The address of the SNMP IP switch node.
Port number	The port where the SNMP IP switch waits for the communication (port 161).
User name	The user name used for the SNMP IP switch.
Security level	The security level used for communication in SNMPv3. Options: noAuthNoPriv, authNoPriv, authPriv
Authentication method	The authentication method used for communication in SNMPv3. Options: MD5, SHA
Authentication password	The authentication Password used for communication in SNMPv3.
Ciphering method	The ciphering method used for communication in SNMPv3. Options: DES, AES128
Ciphering password	The ciphering password used for communication in SNMPv3.

These optional settings help ensure the accuracy of the collected data:

- Virtual Bridge MIB is Readable by using your community name.
- Cisco VTP MIB is Readable by using your community name.
- Extreme FDB MIB is Readable by using the community name.
- SNMP version 1, 2c or version 3 is installed, and running.
- The Interfaces Group MIB is Readable by using the community name.

NOTE: The IP switch to be monitored must meet both of the following conditions:
-RFC1213: SNMP v1 MIB-II is supported.
-RFC1493: SNMP v1 Bridge MIB is supported.
To ensure that the RCA and the Topology view function properly, verify that either RFC2674 (Virtual Bridge MIB) (or RFC4363 (Virtual Bridge MIB)), or Cisco VTP MIB are supported. When you monitor IP switches of the Extreme Networks®, use ExtremeXOS® (version 12.1.2 or later).

Example configuration procedure for a Cisco IP switch (IOS)

For SNMPv1 or v2c:

1. Use telnet to connect to the IP switch.
   a. Type `enable`. If you are prompted to do so, enter your password.
   b. Type `configure terminal`.
   c. Type `snmp-server community public RO`. (Where `public` is the community name and can be changed.)
   d. Type `end`.
   e. Type `show running-config`, then confirm the settings.
2. Disconnect telnet.

For SNMPv3:

1. Use telnet to connect to the IP switch.
   a. Type `enable`. If you are prompted to do so, enter your password.
   b. Type `configure terminal`.
   c. Type `snmp-server view allView`. (Where `allView` is the View name and can be changed.)
   d. Create a View.
   e. Type `snmp-server group privGroup v3 priv read allView notify allView`. (Where `privGroup` is the Group name and can be changed, and `allView` is the View name that you specified at step c.)
   f. Create a Group.
   g. Type `snmp-server user Md5DesUser privGroup v3 auth md5 password1 priv des password2` (Where:
   `Md5DesUser` is a user name and can be changed.
   `privGroup` is the group name that you specified at step e.
   `md5` is an authentication method and can be changed.
   `password1` is the authentication password and can be changed.
   `des` is the ciphering method and can be changed.
   `password2` is the ciphering password and can be changed.)
   Set the password and authentication method/encryption/password according to the security level.
   h. Create a User.
   i. Type `end`.
2. Disconnect telnet.

Example configuration procedure for a Cisco (Catalyst) IP switch (IOS)

For SNMP v3:

1. Use telnet to connect to the IP switch.
   a. Type `enable`. If you are prompted to do so, enter your password.
   b. Type `configure terminal`.
   c. Type `snmp-server view allView iso included`. (Where `allView` is the View name and can be changed.)
   d. Create a View.
   e. Type `snmp-server group authGroup v3 auth read allView notify allView`. (Where `authGroup` is the Group name and can be changed, and `allView` is the View name that you specified at step c.)
   f. Create a Group.
   g. Type `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` (Where:
      `Md5NoneUser` is a user name and can be changed.
      `authGroup` is the group name that you specified at step e.
      `md5` is an authentication method and can be changed.
      `password1` is the authentication password and can be changed.
      `des` is the ciphering method and can be changed.)
      Set the password and authentication method/encryption/password according to the security level.
   h. Create a User.
   i. Type `show vlan` and confirm the vlan list. In that case, type `refrains from the one of enet(ethernet)`.
   j. Type `snmp-server group authGroup v3 auth context vlan-1 read allView notify allView` and set it to permit the context. Note that an authority error might occur if the setting is not applied to all VLAN.
      `authGroup` is a Group name and can be changed.
      `vlan-1` is the VLAN name. Set it to all refrained VLAN.
      `allView` is the View name that you specified at step c.
   k. Type `end`.
2. Disconnect telnet.

Example configuration procedure for an HP IP switch

For SNMPv1 or v2c:

1. Use telnet to connect to the IP switch.
   a. Type `configure terminal`.
   b. Type `snmp-server community public manager restricted`. (Where:
   `public` is a community name and can be changed.)
   c. Type `show snmp-server`, then confirm the settings.
2. Disconnect telnet.

For SNMPv3:

1. Use telnet to connect to the IP switch.
   a. Type `configure terminal`.
   b. Type `snmpv3 user Md5DesUser auth md5 password1 priv password2`. (Where:
   `Md5DesUser` is a User name and can be changed.
   `md5` is an authentication method and can be changed.
   `password1` is an authentication password and can be changed.
   `password2` is a ciphering password and can be changed.)
   Set the password and authentication method/encryption/password according to the security level.
   c. Create a User.
   d. Type `snmpv3 group managerpriv user Md5DesUser sec-model ver3` (Where `managerpriv` is a Group name and can be changed and `Md5DesUser` is the User name that you specified at step b.)
   e. Connect the Group with the User.
2. Disconnect telnet.

Example configuration procedure for a Juniper IP switch

For SNMPv1 or v2c:

1. Use the Web browser to access the Juniper Web Device Manager.
   a. Log in.
   b. From the navigation pane, select **System**, **Management**, **SNMP**, then **Community Config**.
   c. In the **Community Config** panel, add or update the SNMP community to be accessed by the IT Operations Analyzer management server.
2. Close the Web browser.

For SNMPv3:

1. Use telnet to connect to the IP switch.
   a. Type `cli` then change to cli mode.
   b. Type `configure`.
   c. Type `set snmp view allView oid .1 include`, (where `allView` is a View name and can be changed.)

d. Create View.

e. Type `set snmp v3 vacm access group privGroup default-context-prefix security-model usm security-level privacy read-view allView notify-view allView` (where `privGroup` is a Group name and can be changed and `allView` is a the View name you specified at step c.)

f. Create a Group.

g. Type `set snmp v3 usm local-engine user Md5DesUser authentication-md5 authentication-password password1` (where:
`Md5DesUser` is a User name and can be changed.
`authentication-md5` is an authentication method and can be changed.
`password1` is an authentication password and can be changed.)
Set the authentication system/password according to the security level.

h. Create a User.

i. Type `set snmp v3 usm local-engine user Md5DesUser privacy-des privacy-password password2` (where:
`Md5DesUser` is the User name you specified at step g.
`privacy-des` is a ciphering method and can be changed.
`password2` is a ciphering password and can be changed.)
Set the ciphering method/ciphering password according to the security level.

j. Type `set snmp v3 vacm security-to-group security-model usm security-name Md5DesUser group privGroup` (where "Md5DesUser" is the User name you specified at step g.
"privGroup" is the Group name you specified at step e.)
The User and Group are related.

k. Type `commit`.

2. Disconnect telnet.

Example configuration procedure for an Enterasys IP switch

For SNMPv1 or v2c:

1. Use telnet to connect to the IP switch. Log in with an administrator mode and run the following commands:

   a. `set snmp community public`.

   b. `set snmp group groupRW user public security-model v1` (where `groupRW` and `public` are names that can be changed).

   c. `show snmp access groupRW`, then confirm the settings.

2. Disconnect telnet.

Example configuration procedure for an Extreme IP switch

For SNMPv1 or v2c:

1. Use the Web browser to access the ExtremeXOS ScreenPlay.
   a. Log in.
   b. From the navigation pane, select **System**, **Management**, **SNMP**, then **Community Config**.
   c. In the **Community Config** panel, add or update the SNMP community to be accessed by the IT Operations Analyzer management server.
2. Close the Web browser.

For SNMPv3:

1. Use telnet to connect to the IP switch.
   a. Type `configure snmpv3 add mib-view allView subtree 1 type included` (where `allView` is a View name and can be changed as needed.)
   b. Create a View.
   c. Type `configure snmpv3 add access authGroup sec-model usm sec-level authnopriv read-view allView notify-view allView` (where `authGroup` is a Group name and can be changed and `allView` is the View name you specified at step a.)
   d. Create a Group.
   e. Type `configure snmpv3 add user Md5NoneUser authentication md5 password1` (where:
   `Md5NoneUser` is a User name and can be changed.
   `md5` is an authentication method and can be changed.
   `password1` is an authentication password and can be changed.)
   Set the authentication method/password according to the security level.
   f. Create a User.
   g. Type `configure snmpv3 add group authGroup user Md5NoneUser sec-model usm` (where `authGroup` is the Group name you specified at step c and `Md5NoneUser` is the User name you specified at step e.)
   h. Make the connection between the User and Group.
2. Disconnect telnet.

Example configuration procedure for a NETGEAR switch

For SNMPv1 or v2c:

1. Use the Web browser to access the NETGEAR switch:
   a. Log in.
   b. From the navigation pane, select **System**, **Management**, **SNMP**, then **Community Config**.
   c. In the **Community Config** panel, add or update an SNMP community to be accessed by the IT Operations Analyzer management server.

2. Close the Web browser.

Example configuration procedure for a DELL IP switch

For SNMPv1 or v2c:

1. Use the Web browser to access the DELL OpenManage Switch
1. Administrator:
   a. Log in.
   b. From the navigation pane, select **System**, **SNMP**, then **Global Parameters**.
   c. In the **Global Parameters** panel, set **SNMP Notifications** to **Enable**.
   d. From the navigation pane, select **Communities**.
   e. In the **Communities** panel, add or update an SNMP community to be accessed by the IT Operations Analyzer management server.

2. Close the Web browser.

For SNMPv3

1. Use telnet to connect to the IP switch.
   a. Type `configure`.
   b. Type `snmp engineid local default`, and configure the Engine ID.
   c. Type `snmp view allView 1 included` (where `allView` is a View name and can be changed.)
   d. Create a View.
   e. Type `snmp group authGroup v3 auth read allView notify allView` (where `authGroup` is a Group name and can be changed and `allView` is the View name you specified at step c.)
   f. Create a Group.
   g. Type `snmp user Md5NoneUser authGroup auth-md5 password1` (where:
   `Md5NoneUser` is a User name and can be changed.
   `authGroup` is the Group name you specified at step e.
   `auth-md5` is an authentication method and can be changed.
   `password1` is a authentication password and can be changed.)
   Set the authentication method/password according to the security level.
   h. Create a User.
2. Disconnect telnet.

Example configuration procedure for an Allied-Telesis (AT-9424T) switch

For SNMPv3

1. Use telnet to connect to the IP switch.
   a. Type `enable snmp` and enable the SNMP.
   b. Type `create snmpv3 view allView Subtree=1 Type=Included` (where `allView` is a View name and can be changed.)
   c. Create a View.
   d. Type `create snmpv3 access authGroup SecurityModel=V3 SecurityLevel=Authentication ReadView=allView NotifyView=allView` (where `authGroup` is a Group name and can be changed and `allView` is the View name you specified at step b.)
   e. Create a Group.
   f. Type `add snmpv3 user Md5NoneUser Authentication=Md5 AuthPassword=password1` (where:
   `Md5NoneUser` is a User name and can be changed.
   `Md5` is a authentic method and can be changed.
   `password1` is an authentication password and can be changed.)
   Set the authentication method/password according to the security level.
   g. Create a User.
   h. Type `create snmpv3 group UserName=Md5NoneUser SecurityModel=V3 GroupName=authGroup` (where `Md5NoneUser` is the User name you specified at step f and `authGroup` is the Group name you specified at step d.)
2. Disconnect telnet.

Example configuration procedure for an ALAXALA (AX3600) switch

For SNMPv3

1. Use telnet to connect to the IP switch.
   a. Type `configure terminal`.
   b. type `snmp-server view allView 1 included` (where `allView` is a View name and can be changed.)
   c. Create a View.
   d. Type `snmp-server group authGroup v3 auth read allView notify allView` (where `authGroup` is a Group name and can be changed and `allView` is the View name you specified at step b.)
   e. Create a Group.
   f. Type `snmp-server user Md5NoneUser authGroup v3 auth md5 password1` (where:
   `Md5NoneUser` is a User name and can be changed.
   `authGroup` is the Group name. you specified at step d.
   `md5` is a authentic method and can be changed.
   `password1` is a authentic password and can be changed.)
   Set authentication method/password according to the security level.

g. Create a User.

h. Type `write`.

2. Disconnect telnet.

Enabling SNMP traps

IT Operations Analyzer can receive an SNMP trap whenever the IP switch communication link goes up or down. To optionally set up these trap receptions, apply the following settings:

- Enable **Send trap** (the version must be SNMP v1).
- Set up **Send Trap Destination Address** as the IT Operations Analyzer management server IP address, and set up **Send Trap Destination Port** as the IT Operations Analyzer management server's **Trapping Port** (the port number is 162).

NOTE: For information about the default port numbers that are used by IT Operations Analyzer, refer to Chapter 2 of the *Hitachi IT Operations Analyzer Getting Started Guide*.

Example configuration procedure for a Cisco IP switch (IOS)

1. Use telnet to connect to the IP switch. Type the following:
   a. `enable`. If you are prompted to do so, enter your password.
   b. `configure terminal`.
   c. `snmp-server enable traps`.
   d. `snmp-server host 192.168.1.1 version 1 public` (Where `192.168.1.1` is the destination for sending traps, and `public` is the community name. Both can be changed as needed.).
   e. `end`.
   f. `show running-config`, then confirm the settings.
2. Disconnect telnet.

Example configuration procedure for an HP IP switch

1. Use telnet to connect to the IP switch.
   a. Type `configure`.
   b. Type `snmp-server host 192.168.1.1 public all`. (Where `192.168.1.1` is the destination for sending traps, and `public` is the community name. Both can be changed as needed.)
   c. Type `show snmp-server`, then confirm the settings.
2. Disconnect telnet.

Example configuration procedure for a Juniper IP switch (EX series)

1. Use the Web browser to access the Juniper Web Device Manager:
   a. Log in.
   b. Click **Configure**.
   c. Click **Service** then select **SNMP**.
   d. Click **Add** within **Trap Groups**.
   e. Specify a **Trap Group Name**.
   f. From the **Categories** area, select **Link** or **none**.
   g. Add the IP address of the management server to **Targets**.
   h. Click **OK**.
2. Close the Web browser.

Example configuration procedure for an Enterasys IP switch

1. Use telnet to connect to the IP switch. Log in with an administrator mode and run the following commands:
   a. `set snmp targetparams testParams user public security-model v1 message-processing v1`.

      Note that **testParams** is a name that can be changed as needed.
   b. `set snmp notify testNotify tag testTag trap`.

      Note that **testNotify** and **testTag** are names that can be changed as needed.
   c. `set snmp targetaddr testTargetAddr 192.168.55.11 param testParams udpport 162 mask 255.255.255.0 taglist testTag`.

      Note that **testTargetAddr** is a voluntarily name, **192.168.55.11** is the IP address of the trap destination, **162** is the port number of the trap destination, and **255.255.255.0** is a subnet mask of the trap destination. You can change this information, if needed.
   d. `show running-config`, then confirm the settings.
2. Disconnect telnet.

Example configuration procedure for an Extreme IP switch

1. Use telnet to connect to the IP switch. Log in with an administrator mode and run the following commands:
   a. `configure snmpv3 add target-params testTargetParam user v1v2c_ro mp-model snmpv1 sec-model snmpv1 sec-level noauth`.

      Note that **testTargetParam** is an arbitrary name and **v1v2c_ro** is a security name. Either name can be changed as needed. You can confirm the security name by using `show snmpv3 community`.

   b. `configure snmpv3 add target-addr 192.168.55.11 param testTargetParam ipaddress 192.168.55.11/FFFFFF00 transport-port 162 from 192.168.55.7`.

      Note that **191.168.55.11** is the IP address of the trap destination, **FFFFFF00** is a subnet mask of the trap destination, **162** is the port number of the trap destination, and **192.168.55.7** is an IP address of the trap source. You can change this information, if needed.

   c. `show running-config`, then confirm the settings.

2. Disconnect telnet.

Example configuration procedure for a NETGEAR IP switch

1. Use the Web browser to access the NETGEAR switch:
   a. Log in.
   b. From the navigation pane, select **System**, **Management**, **SNMP**, then **Trap Config**.
   c. In the **Trap Config** panel, add or update a trap configuration for sending an SNMP trap to the IT Operations Analyzer management server. For the **SNMP Version**, specify **SNMP V1**.
   d. From the navigation pane, select **Trap Flags**.
   e. From the **Trap Flags** pane, set **Link Up/Down** to **Enable**.

2. Close the Web browser.

Example configuration procedure for a DELL IP switch

1. Use the Web browser to access the DELL **OpenManage Switch Administrator**:
   a. Log in.
   b. From the navigation pane, select **System**, **SNMP**, then **Global Parameters**.
   c. In the **Global Parameters** panel, set **SNMP Notifications** to **Enable**.
   d. From the navigation pane, select **Notification Recipients**.
   e. In the **Notification Recipients** panel, add or update a trap configuration for sending an SNMP Trap to the IT Operations Analyzer management server. For the configuration, select **SNMPv1.2**.

2. Close the Web browser.

6

Preparing Hitachi storage

IT Operations Analyzer can monitor Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series. It can also monitor Hitachi 9500V and Hitachi USP VM through Device Manager's SMI-S agent. However, it will not monitor the performance of Hitachi 9500V.

This chapter describes the information that must be collected for connecting to the Hitachi AMS/WMS/SMS storage nodes, Hitachi Unified Storage, Hitachi 9500V and Hitachi USP VM. It also describes preparation tasks for acquiring performance information for Hitachi AMS/WMS/SMS series, Hitachi Unified Storage series and Hitachi USP VM.

- Preparations for connecting to Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series
- Preparations for acquiring performance information for Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series
- Preparations for connecting to Hitachi 9500V and Hitachi USP VM
- Preparations for acquiring performance information for Hitachi USP VM

Preparations for connecting to Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series

IT Operations Analyzer can monitor Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series. When you connect to Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series, the information that is listed in Table 6-1 is necessary.

Table 6-1: Information for Connecting to Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series

Item	Details
IP Address	The IP address that is used to connect to the storage.
User ID	If either **Account Authentication** or **Password Protection** is enabled, specify the ID of the user who can log on to the storage.
Password	The password that is associated with the User ID. It is required if either **Account Authentication** or **Password Protection** is enabled.

NOTE: When **Password Protection** is used, errors might occur. For example, when multiple management servers are attempting simultaneous access to the Hitachi storage where **Password Protection** is configured. To prevent errors, we recommend disabling **Password Protection**.

About modifying the port number

When the management port number for Hitachi storage is changed, register the changed port number in the services file. The services file is located in the following Windows directory:

<*Windows Directory*>\system32\drivers\etc\services

- Service name of the **normal port** number: df-damp-snm
- Service name of **secure port** number: df-damp-snm-ssl

In the following example, the **normal port** is set to 2300 and the **secure port** is set to 25000:

df-damp-snm 2300/tcp #normal port

df-damp-snm-ssl 25000/tcp #secure port - SSL

NOTE: The port number of the Hitachi storage that is monitored by IT Operations Analyzer should match. When the services file is changed, the change affects products that use HSNM2-API, such as Hitachi Storage Navigator Modular 2, HiCommand series, etc.

Preparations for acquiring performance information for Hitachi AMS/WMS/SMS series and Hitachi Unified Storage series

Complete the following steps to acquire performance information.

1. Open the **Performance Statistics** panel of the storage device whose performance is to be monitored from Hitachi Storage Navigator Modular 2.
2. Complete tasks based on whether the management dialog displays in a new window:
   - **When the management dialog displays in a new window**

   a. Log in to Hitachi Storage Navigator Modular 2.

   b. Click target array name and open the management dialog.

   c. From the menu, click **Tool**, **Performance**, then **Setting**.

   - **When the management dialog displays in the same window**

   a. Log in to Hitachi Storage Navigator Modular 2.

   b. Click target array name and open the management screen.

   c. From the tree view, open **Performance** then click **Monitoring**.

   d. Click **Acquisition item change**.
3. Confirm that the following are selected: **RAID Group/Logical Unit Information**, **Cache information**, **Processor information**, and **Drive activation information**, then click **OK**.

Preparations for connecting to Hitachi 9500V and Hitachi USP VM

IT Operations Analyzer can monitor:

- Hitachi 9500V through Hitachi Device Manager's SMI-S agent. Install Device Manager 5.9 or later and enable the use of the SMI-S provider.
- Hitachi USP VM through Device Manager's SMI-S agent. Install Device Manager 6.2 or later and enable the use of the SMI-S provider.

Following is a general procedure outline for acquiring connection information for Hitachi 9500V and the Hitachi USP VM. For specific details, refer to the applicable manuals:

- Hitachi Device Manager, Provisioning Manager and Tiered Storage Manager Software Installation Guide
- Hitachi Device Manager and Provisioning Manager Software System Configuration Guide
- Hitachi Device Manager Software Web Client User Guide

1. Install **Device Manager** on an arbitrary server. Because you can select the existence of an SMI-S agent during the installation, enable it.
2. Log in to **Device Manager**, and click **Subsystems**, then **Add Subsystem**, and register storage devices.

   When registering devices, use the IP addresses, User IDs, and passwords of the storage controllers. Table 6-2 lists the information that is necessary when connecting to Hitachi storage.
3. When you use an SMI-S agent, as described in this manual, you need to increase the memory heap size of the Device Manager server. Following is an example procedure when working with Microsoft Windows:
   a. Calculate the memory heap size.
   b. Open the **Server.ini** file using a text editor:

      <*Device Manager server install location*>\HiCommandServer\Server.ini
   c. Based on the calculations at step a, change the value of **JVM_XOPT_HEAP_MAX**. For example:

      JVM_XOPT_HEAP_MAX=Xmx<*Setting value*>m
   d. Restart the Device Manager server.

Table 6-2: Information for Connecting to Hitachi 9500V and Hitachi USP VM

Item	Details
IP address	Use the IP address of the server where Device Manager is installed.
Namespace	For Device Manager 5.9 or later, specify: root/smis/smis12 For Device Manager 6.2 or later, specify: root/smis/smis13 For Device Manager 7.0 or later, specify: root/smis/smis14
Existence of an SSL	Use the settings that were applied during the installation of Device Manager.
Port Number	Use the settings that were applied during the installation of Device Manager. By default: • Non-SSL communication: 5988 • SSL communication: 5989

Table 6-2: Information for Connecting to Hitachi 9500V and Hitachi USP VM

Item	Details
User ID	Use the User ID for Device Manager.
Password	Use the password that is associated with the User ID.

NOTE: When your site monitors Hitachi storage using Hitachi Device Manager, the following components will always be reported as operating normally, within the **Monitoring** module:
-Storage Controller
-Storage FC Port
-Storage Disk Drive
-Storage Volume
-LUN
Consequently, any error conditions will not be detected.

Preparations for acquiring performance information for Hitachi USP VM

Following is a general outline for acquiring Hitachi USP VM performance information. For details, please refer to the Hitachi Device Manager manuals.

1. Prepare the storage subsystem.

   Prepare the command device in each storage subsystem from which you want to acquire performance data. (The command device is a control device that issues the control command to the large-scale disk array unit.) Then, allocate a path to the host that collects performance data, and configure the host to recognize the command device.

2. Prepare the host that collects performance data.

   Install the Device Manager agent, and configure the command device.

3. Prepare the Device Manager server.

   Set the host name of the host that collects performance data, in the property file of the Device Manager server.

7

Preparing SMI-S for FC switches and storage

IT Operations Analyzer uses SMI-S to discover and monitor other storage and FC switches. This chapter describes SMI-S and the tasks that are required to setup your FC switches and storage.

- Reviewing the SMI-S preparations
- Preparing SMI-S for Fibre Channel (FC) switches
- Preparing SMI-S for storage

Reviewing the SMI-S preparations

SMI-S is the Storage Networking Industry Association (SNIA) standard that provides an open management application programming interface (API). It supports the interoperable management of storage networks and storage devices, which include virtual storage, switches, and hosts.

If your environment uses third-party storage (that is, storage other than Hitachi storage or FC switches), IT Operations Analyzer can discover and monitor it through the use of an SMI-S agent.

In an environment that uses third-party storage with an SMI-S agent, there may be one of two models in use: An embedded model or a proxy model.

- In an **embedded model**, the SMI-S agent is running on a device. We refer to this as SMI-S agent (embedded).
- In a **proxy model**, the SMI-S agent is installed on a server. We refer to this as SMI-S agent (proxy).

Figure 7-1 provides an example of an SMI-S environment, which is comprised of a server (referred to as the SMI-S server) and client. IT Operations Analyzer operates as the client, and in this example, is collecting information about Fibre Channel (FC) switches. Note that the blue shaded area, encompassing the embedded and proxy models, needs to be prepared before you start the initial discovery.

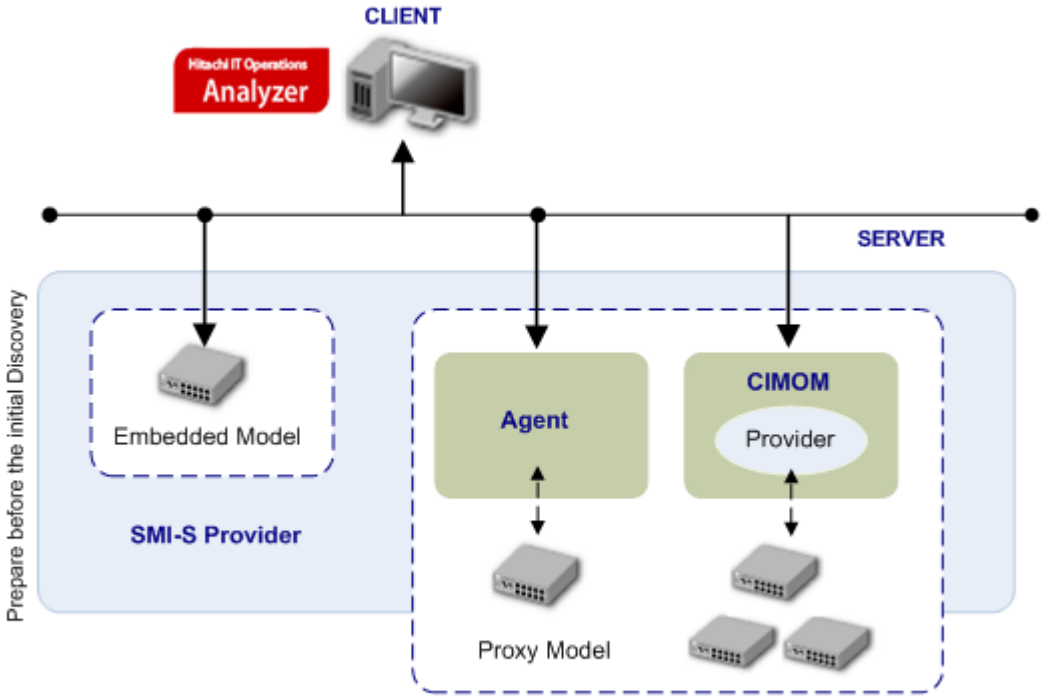

Figure 7-1: Example of an SMI-S Environment

The following sections describe the necessary preparations for the FC switches and storage in your environment.

Preparing SMI-S for Fibre Channel (FC) switches

To specify devices as the monitoring targets, they must support SMI-S version 1.0 - 1.3, and the service that manages those devices must be running. This section describes the SMI-S agent settings for the following:

- Brocade® FC Switches
- Brocade Sphereon series FC switches
- QLogic® FC switches
- Cisco® FC switches

Configuring Brocade FC switches (except the Sphereon series)

Configure SMI-S agent settings according to the following guidelines. For details, please refer to the Brocade SMI Agent documentation, located at the following Web site:
http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

You can confirm installation requirements, installation procedures, post-installation settings and updates contained in release notes, as follows:

- Installation requirements

  Brocade SMI Agent v120.6.0a Installation Guide, Chapter 1 "Installation Requirements"

- Installation procedures

  Brocade SMI Agent v120.6.0a Installation Guide, Chapter 2 "Installing the SMI Agent"

- Post-installation settings

  Brocade SMI Agent v120.6.0a User's Guide

- Release Notes

  Brocade SMI Agent v120.6.0a Release Notes v1.1

Pre-installation requirements

- Brocade SMI-S Agent version: Brocade SMI Agent v120.6.0a
- Operating system: Microsoft Windows Server 2003 (32 bit)

When a previous version of the Brocade SMI-S Agent is installed, complete the following installation tasks.

To install a Brocade SMI Agent:

1. Download the Brocade SMI-S Agent v120.6.0a from the following Web site, then run the **install.exe**:
   http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

2. Complete each prompt of the installation wizard. For certain prompts, check the following guidelines:
   a. **HTTP Port Configuration**. The default port number is 5988. Note that the port number you specify is used to connect to IT Operations Analyzer.
   b. **HTTPS Port Configuration**. The default port number is 5988. Note that the port number you specify is used to connect to IT Operations Analyzer.
   c. **Proxy Connections Configuration**. Specify the following:

      Proxy IP: IP Address of the FC switch

      User name: User name of the FC switch

      Password: Password of the FC switch

      Specify other settings based on your environment.
3. To save your changes at the end of the Brocade Agent installation, click **Done**.

   Now, you are ready to register the FC switch.

To register the FC switch:

1. Launch the **Brocade SMI Agent Configuration Tool**:
   a. From the **Start** menu, select **All Programs**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** menu is different.

   b. Select **SMIAgent120.6.0a** then **Brocade SMI Agent Configuration Tool**.
2. Click **Add** to launch the **Proxy Configuration** dialog.
3. Enter the requested information, then click **OK** to save your settings and close the **Proxy Configuration** dialog.
4. Within the **Brocade SMI Agent Configuration Tool**, change the proxy status from **Not Connected** to **Connected** by clicking **Apply**.

Table 7-1 lists the information that is necessary when connecting to a Brocade FC switch.

Table 7-1: Information for Connecting to a Brocade FC Switch

Item	Details
IP address	Specify the IP address of the server where Brocade SMI Agent is installed.
Namespace	Specify `root/brocade1`.
Existence of an SSL	Apply the Brocade SMI Agent settings that were configured during the installation.
Port Number	Apply the Brocade SMI Agent settings that were configured during the installation. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID of the Brocade SMI Agent.
Password	Enter a password for the User ID.

NOTE: When an FC-FC Routing port status is "link-down", the status of the phantom switch changes to "unreachable". The unreachable status for the switch will not change, even if the port status becomes normal again.

To change the status of the switch from unreachable to normal, IT Operations Analyzer needs to rediscover the switch. This is required because the SMI-S provider of the phantom switch will not answer or respond, when the port status is link-down. Even if the port status becomes normal again, the SMI-S provider will report the switch status as unreachable.

See the online Help for information on discovering switches, nodes, and other devices.

Configuring Brocade Sphereon FC switches

Configure SMI-S agent settings according to the following guidelines. For details, please refer to the Brocade SMI Agent for EOS documentation, located at the following Web site: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

You can confirm installation requirements, installation procedures, post-installation settings and updates contained in release notes, as follows:

- Installation requirements

  Brocade SMI Agent for EOS Products User Guide 2.0, Chapter 1"System Requirements"

- Installation procedures

  Brocade SMI Agent for EOS Products User Guide 2.0, Chapter 2 "Installing Brocade SMI Agent for EOS products"

- Post-installation settings

  Brocade SMI Agent for EOS Products User Guide 2.0, Chapter 3 "Using the SMI Agent for EOS products Server Configuration Program", and Chapter 4 "Server Setup for Client Operations"

- Release Notes

  Brocade SMI Agent for EOS Products 2.0 Release Notes

Pre-installation requirements

- Brocade SMI-S Agent version: Brocade SMI Agent for EOS products 2.0 for Windows
- Operating system: Microsoft Windows Server 2003 (32 bit)

To install a Brocade SMI Agent:

1. Download the Brocade SMI Agent for EOS for Windows from the following Web site, then run the **install.exe**: http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. Complete each prompt of the installation wizard.

3. To save your changes at the end of the Brocade Agent installation, click **Done**.

   Now, you are ready to register the FC switch.

To register the FC switch:

1. Open the **Switch.properties** file which is located in the following path: <*Installation directory*>\agent\server\jserver\bin
2. Specify the following parameters:
   - **cimserver**

     The URL of the server, for example: https://localhost/root/mcdata
   - **cimserverusername**

     The user name for logging in to the CIM Server, for example: Administrator
   - **cimserverpassword**

     The password for logging in to the CIM Server, for example: Password
   - **switchip**

     The IP Address of the switch, for example: 172.26.24.180
   - **switchtype**

     The switch product type code. Refer to the note, below.
   - **switchusername**

     The user name for logging on to the switch.
   - **switchpassword**

     The password for logging on to the switch.

NOTE: Following are the FC switch product type codes:

Sphereon 3016: Code 2

Sphereon 3032: Code 3

Sphereon 3216: Code 4

Sphereon 3232: Code 5

Sphereon 4300: Code 6

Sphereon 4400: Code 12

Sphereon 4500: Code 7

Sphereon 4700: Code 13

3. Move information to the following path, from the command prompt: <*Installation directory*>\agent\server\jserver\bin
4. Run the following command: ManageSwitch Add

Table 7-2 lists the information that is necessary when connecting to a Brocade Sphereon series FC switch.

Table 7-2: Information for Connecting to a Brocade FC Switch

Item	Details
IP address	Specify the IP address of the server where Brocade SMI Agent for EOS is installed.
Namespace	Specify `root/mcdata`.
Existence of an SSL	Apply the Brocade SMI Agent settings that were configured during the installation.
Port Number	Apply the Brocade SMI Agent for EOS settings that were configured during the installation.
User ID	Use the User ID of the Brocade SMI Agent for EOS.
Password	Enter a password for the User ID.

Configuring QLogic FC switches

The SMI-S provider is embedded in the QLogic FC switch. The procedure in this section describes how to connect to the management port of the QLogic FC switch using a Web browser.

For details about configuring the SMI-S provider settings using the command line interface (CLI), refer to the documentation for the QLogic FC switch. The documentation is available from the following Web site:

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/NewDefault.aspx

To configure QLogic FC switches:

1. From your Web browser, connect to the QLogic FC switch management port (for example, http://10.208.113.46). The **Switch Manager** window displays.
2. From the **Switch Manage**r menu bar, select **Switch**, then **Services**. The **System Services** dialog displays.
3. Verify whether the SMI-S provider service is enabled:
   - If the **CIM service** is selected, the SMI-S provider service is enabled. Click **Close**.
   - If the **CIM service** is not selected, then select it and click **OK**.
4. If an option for specifying the **SSL service** exists in the **System Services** dialog, then you can use SSL port **5989**.

Table 7-3 lists the information that is necessary when connecting to a QLogic FC switch.

Table 7-3: Information for Connecting to a QLogic FC Switch

Item	Details
IP address	The IP address of the QLogic FC switch.
Namespace	Specify `root/switch`.
Existence of an SSL	Apply the QLogic FC switch settings.
Port Number	Apply the QLogic FC switch settings that were configured during the installation. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID of the QLogic FC switch.
Password	Enter a password for the User ID.

Configuring Cisco MDS 9000 Family FC switches

The SMI-S provider is embedded in the Cisco FC switch. The procedure in this section describes how to enable the server and connect to it by using the HTTP protocol (port 5988). If your site chooses to use the HTTPS protocol (port 5989), apply Secure Socket Layer (SSL) authentication to encrypt the login information, and then enable the HTTPS and SMI-S agent (proxy). Details of the procedure are provided in the link that is referenced in Table 7-4.

For additional details, refer to the Cisco MDS 9000 Family SMI-S Programming Reference. The document is available from the following Web site:

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html

To configure Cisco MDS 9000 family FC switches:

An example of the command execution that is described in the following procedure is listed after step 8.

1. Access the FC switch by telnet, then log in.
2. Enter `show cimserver`, and verify that cimserver Http is enabled.
3. Enter `config terminal`, then start the configuration mode.
4. By default, HTTP is enabled. If this is not the case, then enable it by entering `cimserver enableHttp`.
5. Enter `cimserver enable`, to enable the CIM server.
6. Enter end to end the configuration mode.
7. Enter `show cimserver`, and verify the settings:
   - cimserver is enabled
   - cimserver Http is enabled
8. Enter `exit` to disconnect telnet.

Command example

```
FCGS03 login: ********

Password:

FCGS03# show cimserver

 cimserver is not enabled

 cimserver Http is enabled

 cimserver Https is not enabled

 cimserver certificate file is not installed

FCGS03# config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

FCGS03(config)# cimserver enable
```

```
FCGS03(config)# end

FCGS03# show cimserver

 cimserver is enabled

 cimserver Http is enabled

 cimserver Https is not enabled

 cimserver certificate file is not installed

 Current value for the property logLevel in CIMServer is
'WARNING'.

FCGS03# exit
```

Table 7-4: Information for Connecting to a Cisco FC Switch

Item	Details
IP address	The IP address of the Cisco FC switch.
Namespace	Specify `root/cimv2`.
Existence of an SSL	Apply the Cisco FC switch settings. For details, see the Cisco MDS 9000 Family SMI-S Programming Reference: http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html
Port Number	Apply the Cisco FC switch settings that were configured during the installation. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID of the Cisco FC switch.
Password	Enter a password for the User ID.

Preparing SMI-S for storage

To specify storage as the monitoring target, it must support SMI-S version 1.0 - 1.3, and the service that manages the storage must be running. This section describes the SMI-S settings for the following:

- EMC storage
- HP EVA series storage
- HP MSA series storage
- Engenio OEM Sun storage and IBM storage
- NetApp Storage

NOTE: For information about configuring Hitachi storage and acquiring Hitachi storage (USP VM) performance, see Chapter 6, Preparing Hitachi storage.

Notes about the maximum monitoring volume for one storage device

The maximum number of volumes (logical devices) that can be monitored for one storage device is 2000. When the number of storage volumes exceeds 2000, the Storage Volume (Component Type), which is displayed in the **Components** tab of the **Monitoring** module, reflects the following information, and the volume cannot be monitored:

- Component Name: Volumes (Number of Volumes)
- Component Status: The volume cannot be monitored because the number of volumes exceeds 2000.

Additionally, the following information related to the volume is not acquired. Information displayed in the **Monitoring** module is as follows:

- **Components** tab. For the following component types, nothing is displayed: "LUN", "Storage Exported FileShare", "Storage FileShare Port", "Storage Volume"
- **Performance** tab. For the Write Cache Hit Ratio, the state is Unknown, and the performance is not acquired.

Configuring EMC storage

Configure the SMI-S agent settings using the following guidelines. For details, refer to the following EMC SMI-S agent documentation:

- EMC SMI-S Provider Release Notes

  Overview: Installation method and Setting method after the installation

  http://Powerlink.EMC.com

  Support > **Technical Documentation and Advisories** > **Software ~ S ~ Documentation** > **SMI-S Provider** > **Release Notes**

- EMC Support Matrix

  Overview: Support target of the EMC SMI-S provider

  http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

Pre-installation requirements

- EMC SMI-S Provider Version: V3.2.3, V3.3.1
- Operating system: Microsoft Windows 2003 [x86] R2, SP1
- Storage Array: CLARiiON

Refer to the following link for the EMC support matrix for the storage operating environment requirements:

http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

NOTE: The value of the performance metric, **WriteHitIOs**, is not acquired in EMC CLARiiON.

To install the EMC SMI-S provider:

Please note that when the EMC SMI-S provider of the previous version or if the Solutions Enabler is installed, those are uninstalled.

1. Download the EMC SMI-S provider from the following Web site:

   http://Powerlink.EMC.com
2. Navigate to the following site location: **Support** > **Software Downloads and Licensing** > **Downloads S** > **SMI-S Provider**
3. Close all applications before starting the installation
4. Download **se6430-WINDOWS-x86-SMI.msi** or **se65132-WINDOWS-x86-SMI.msi**.
5. Run the installation executable file to launch the **EMC Solutions Enabler with SMI** wizard.
6. Complete all prompts in the wizard. When you are finished, click **Finish**.

   Now, you are ready to register storage information.

To register storage information:

The following procedure will ensure that you can manage storage using the EMC SMI-S provider.

1. When the EMC storage volume is not applied to a server on which EMC SMI-S provider is installed, then complete the following Out-of-Band steps. An example of the command execution that is described in the following procedure is listed after step j:
   a. Run the **TestSmiProvider.exe** file, which is located in the following path: <*Installation folder*>\SYMCLI\storbin\TestSmiProvider.exe
   b. For all Hosts, Connection Type, Logfile path, Port, Username, and Password click Enter to keep the default information.
   c. Type **addsys** then click **Enter**.
   d. Type **y** then click **Enter**.
   e. Select the type of storage array. For CLARiiON, type **1** then click **Enter**.
   f. Specify the IP Address of **Processor A** then click **Enter**. Also, specify the IP Address of **Processor B** then click **Enter**, twice.

g. Choose the type of the address specified at step f. Type **2**, then click **Enter**.

h. Specify the user ID and password that is associated with administrator authority, for the storage you are registering.

i. When the registration is successful, **OUTPUT : 0** is displayed. Write down the serial number that is referenced in the applicable area of the command, for example, CK200080001000.

j. Type **dv**, then click **Enter**. Check if the serial number that you noted at step **i** is indicated in the **Firmware version information**.

Command example

```
Host [localhost]:
Connection Type (ssl,no_ssl) [no_ssl]:
Logfile path [Testsmiprovider.log]:
Port [5988]:
Username []:
Password []:
Connecting to localhost: 5988
(localhost:5988) ? addsys
Add System {y|n} [n]: y
ArrayType (1=Clar, 2=Symm) [1]: 1
One or more IP address or Hostname or Array ID
Elements for Addresses
IP address or hostname or array id 0 (blank to quit):
192.168.10.31
IP address or hostname or array id 1 (blank to quit):
192.168.10.32
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]: 2
Address Type (1) [default=2]: 2
User [null]: analyzer
Password [null]: analyzerpass
++++ EMCAddSystem ++++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout,
4=Failed
       5=Invalid Parameter
       4096=Job Queued, 4097=Size Not Supported
```

```
System: //kaede/root/
emc:Clar_StorageSystem.CreationClassName="Clar_StorageSys
tem",Name="CLARiiON+CK200080001000"

(localhost:5988) ? dv

++++ Display version information ++++

CIM ObjectManager Name: PG:5B48A8C4-682F-4FCB-AE98-
F0687C31225F

CIMOM Version: Pegasus CIM Server Version 2.6.1

SMI-S spec version: 1.3.0

SMI-S Provider version: V3.3.1.0

Solutions Enabler version: V6.5-883 1.32

Firmware version information:

CLARiiON Array CK200080001000 (Rack Mounted CX3_10_C) :
3.26.10.5.019
```

2. When the EMC storage volume is applied to a server on which EMC SMI-S provider is installed, then complete the following In-Band steps. An example of the command execution that is described in the following procedure is listed after step f:
   a. Confirm that at least one CLARiiON LUN is registered. Run the following command from the server on which the EMC SMI-S provider is installed:

      <*Installation folder*>\SYMCLI\bin> symiq -cids

   b. Confirm that value for the following setting is set to **true**:
      OslProv/com.emc.se.osls.osl.StorApi.database.discover
      This setting is located in configuration file of **emcprovider.conf**:
      <*Installation folder*>\SYMCLI\storbin

      If the value is **false**, change it to **true**.

   c. Run the following command to suspend the EMC SMI-S provider service:

      <*Installation folder*>\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider

   d. Run the following command to register authentication information:

      <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host <*Storage IP address*> -Username <Storage User ID> -Password <*Storage Password*>

      As an example, the following commands would be run when the IT Operations Analyzer password is **analyzerpass**, the IP address of **Processor A** is **192.168.10.31**, and the IP address of **Processor B** for CLARiiON is **192.168.10.32**. Processor A is registered first:

      <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host

      192.168.10.31 -username analyzer -password analyzerpass

      <*Installation folder*>\SYMCLI\bin>symcfg authorization add -host

      192.168.10.32 -username analyzer -password analyzerpass

e. Run the following command to start the EMC SMI-S provider service. Afterward, it will take some time before you can search from IT Operations Analyzer:

   <*Installation folder*>\SYMCLI\strobin> cimserver -start EMC_SMI_Provider

f. Run the following command to confirm the registration information:

   <*Installation folder*>\SYMCLI\bin> symcfg list auth

Command example

```
C:\Program Files\EMC\SYMCLI\bin>syminq -cids
Device                Clariion               Device
------------------------ -------------------- ---------
Name               Type   ID Rev  Ser Num      Cap (KB)
------------------------ -------------------- ---------
\\.\PHYSICALDRIVE2      CK200080001000  0326 070000B5
1048576

C:\Program Files\EMC\SYMCLI\storbin>cimserver -stop
EMC_SMI_Provider

Pegasus stopped as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.31 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.32 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\storbin>cimserver -start
EMC_SMI_Provider

Pegasus started as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg list auth

Hostname            Username          Namespace     Port

192.168.10.31         analyzer

192.168.10.32         analyzer
```

Acquiring EMC storage performance

Use the following procedure to acquire EMC storage performance data.

1. Use the EMC storage management software to acquire performance data. As an example, following are the instructions for the **EMC Navisphere Management Suite**:
   a. Open the **Data Logging** window from the **EMC Navisphere Management Suite** menu bar: From the **Tools** menu, select **Analyzer** then **Data Logging....**
   b. In the **Target** area, select the storage from which you want to obtain performance, and confirm the **Status** field for **Logging**:

      If **Status** is **Stopped**, then click **Start**.

If **Status** is **Running. Started on date time**, then click **Cancel**. It is not necessary to restart the SMI-S agent.

2. Restart the SMI-S provider. If you use the CLI, run the `cimserver` command, then stop and start the SMI-S provider:

   ```
   <Installation folder>\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider
   Pegasus stopped as a Windows service
   <Installation folder>\SYMCLI\strobin> cimserver -start EMC_SMI_Provider
   Pegasus started as a Windows service
   ```

Table 7-5: Information for Connecting to EMC Storage

Item	Details
IP address	Use the IP address of the server where the EMC SMI-S provider is installed.
Namespace	Specify `root/emc`.
Existence of an SSL	Use the EMC provider settings.
Port Number	Use the EMC SMI-S provider settings. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID for EMC provider. Default is empty.
Password	Use the password that is associated with the User ID. Default is empty.

Configuring HP EVA series storage

Configure the SMI-S provider settings according to the following guidelines. For details, please refer to the Command View EVA manuals.

NOTE: The HP EVA series SMI-S agent does not support the feature to collect performance information.

Pre-installation requirements

- Supported version: HP StorageWorks Command View EVA 8.0
- Operating system: Microsoft Windows Server 2003
- Storage: HP StorageWorks 4400 Enterprise Virtual Array

To install HP StorageWorks Command View EVA 8.0:

1. Run the executable file, HP StorageWorks Command View EVA Software Suite.exe.
2. Click **OK** to start the installation wizard.
3. At the installation panel, **Choose Install Set**, verify that **SMI-S CIMOM** is selected.

   The HP SMI-S EVA uses default port number 5988 or 5989.

   If it is not possible to use the default ports, a message displays, indicating which ports are not available. If you receive such a message, specify an available port number (from 60000 through 65536). Then, continue with the installation.
4. The last panel of the installation wizard displays **Install Complete**. To finish, click **Done**.

   Now, you are ready to apply HP Command View EVA settings.

To apply HP Command View EVA settings:

1. Configure the CIMOM server:
   a. Modify the following file to change the port number and HTTP/HTTPS that is used for the CIMOM server:

      <*Installation directory*>\SMI-S\CXWSCimom\config\cxws.properties

   b. Following are the default values:

      enableHttp: true

      enableHttps: true

      cxws.http.port: 5988

      cxws.https.port: 5989

      Specify **False** when you invalidate enableHttp (Https) and specify the port number to be used.

   c. After you change the settings, restart the HP StorageWorks CIM Object Manager Service:

From the **Start** menu, select: **Setting**, **Control panel**, **Management tool**, then **Service**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** menu is different.

2. Register your storage:
   a. Launch your browser and specify the following URL:

      https://host_name:2372

      Specify the **Server name** or **IP Address** for the **host_name**.

   b. Log in at the **HP Command View EVA prompt**.

      When logging in, use the user account information of the server on which you installed the HP Command View EVA. Ensure that the user account belongs to the **HP Storage Admin group**.

   c. After you log in, confirm that your storage is displayed within the **Storage System** panel. If it is not displayed, click **Discover** to register your storage.

NOTE: In order for the storage to be registered, the server on which the HP Command View EVA is installed must be directly connected to the FS switch.

Table 7-6: Information for Connecting to HP EVA Storage

Item	Details
IP address	Use the IP address of the server where Command View EVA is installed.
Namespace	Specify `root/eva`.
Existence of an SSL	Use the Command View EVA settings.
Port Number	Use the Command View EVA settings. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID for Command View EVA.
Password	Use the password that is associated with the User ID.

Configuring HP MSA series storage

Configure SMI-S agent settings according to the following procedure. For details, please refer to the MSA SMI-S agent documents.

NOTE: The HP MSA series SMI-S agent does not support the feature to collect performance information.

1. Download **MSA SMI-S Provider** from the following Web site:

   http://h18006.www1.hp.com/storage/smis.html

2. Install **MSA SMI-S Provider** on an arbitrary server.

Table 7-7: Information for Connecting to HP MSA Storage

Item	Details
IP address	Use the IP address of the server where MSA SMI-S Provider is installed.
Namespace	Specify `root/hpmsa`.
Existence of an SSL	Use the MSA SMI-S Provider settings.
Port Number	Use the MSA SMI-S Provider settings.
User ID	Use the User ID for MSA SMI-S Provider.
Password	Use the password that is associated with the User ID.

Configuring Engenio OEM Sun storage and IBM storage

Configure SMI-S Provider settings according to the following procedure. For details, please refer to the Engenio SMI-S Provider documents. In order to download the documents, a login account to NetApp's Web site is required:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Pre-installation requirements

- Supported version: Engenio SMI Provider 09.19.G0.07
- Operating system: Microsoft Windows Server 2003 (32 bit)

To install the Engenio SMI-S Provider:

1. Run the executable file to install the Engenio SMI Provider 09.19.G0.07.
2. Complete all prompts within the installation wizard.
3. When you have completed the installation, click **Done**.

To register the storage device:

The following procedure registers the storage device that you want to manage using the Engenio SMI Provider.

1. Launch the command prompt.
2. Switch to the following directory:

   <*Installation directory*>\SMI_SProvider\bin
3. Run the `ProviderUtil` command, and input the following information:
   - **Input CIMOM Username**

     Optionally specify the CIMOM user name, for example: any
   - **Input CIMOM Password**

     Optionally specify the CIMOM password, for example: any
   - **Input Port [5988]**

     Optionally specify a port number. The default value is 5988.
   - **Input Operation**

     1) add Device

     2) remove Device

     3) Add credentials for an array

Please Input 1, 2, or 3

Specify **1** to register a storage device.

- **Input device DNS-resolvable hostname or IP address**

  Specify the IP address or the host name for the storage device.

- **Input Array Password** (default is blank)

  Specify the password of the storage device.

The storage device is successfully registered when **The extrinsic call succeeded** message displays.

Table 7-8 lists the information that is necessary when connecting to the storage node that you want to monitor.

Table 7-8: Information for Connecting to Sun Storage and IBM Storage

Item	Details
IP address	Use the IP address of the server where Engenio SMI-S Provider is installed.
Namespace	Specify `root/lsissi11`.
Existence of an SSL	Use the Engenio SMI-S Provider settings.
Port Number	Use the Engenio SMI-S Provider settings. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID for Engenio SMI-S Provider.
Password	Use the password that is associated with the User ID.

Configuring NetApp storage

Configure SMI-S provider settings for NetApp storage according to the following procedure. For details, please refer to the NetApp SMI-S provider documentation. In order to download the documents, a login account to NetApp's Web site is required:

http://support.netapp.com/NOW/apbu/oemcp/protcd/

Pre-installation requirements

- Supported version of NetApp Data ONTAP SMI-S Agent: Data ONTAP SMI-S Agent 3.0
- Operating system: Microsoft Windows Server 2003 (32 bit)

JDK 1.5.0 or later, and JRE 1.5.0 are required to use NetApp Data ONTAP SMI-S Agent. Confirm whether the information is installed on the Windows server on which you will install the SMI-S Agent.

To install the Data ONTAP SMI-S Agent 3.0:

1. Download the Data ONTAP SMI-S Agent installation file.
2. Select **Windows** from **Select Platform** of **Data ONTAP SMI-S Agent**, then click **Go**.
3. Click **View & Download**.
4. Click **CONTINUE** of the **Software download Instructions** page.

5. Click **Accept** to continue. Download the SMI-S Agent and corresponding manuals.
6. Run the executable file to install the Data ONTAP SMI-S Agent 3.0.
7. Based on your preference, indicate which installation type, **Typical** or **Custom**, you would like to follow.
8. Complete all prompts within the installation wizard.
9. When you have completed the installation, click **Finish**.

To configure the SMI-S provider settings:

1. In the **Edit System Variable** dialog, specify **JAVA_HOME** as the system environment variable or the user environment variable. If you specify a path that contains a blank space, enclose the path with double quotation marks (").
2. To connect to the SMI-S Provider, use port number **5989** and the **https** protocol. To change the port number or to enable the connection using http protocol, edit the **WEBSconfig.ini** file contained in the following directory: **C:\Program Files\ws\server\cserver\bin**. Following are the default settings that are listed in the **WEBSconfig.ini** file. If you change them, then set **enableOverride** to **True**.

   enableOverride=False (Must be set to **True** if you modify any of the subsequent settings.)

   HTTPPort=5988

   HTTPSPort=5989

   enableSSL=True

   enableHTTP=False

To register the storage device:

1. From the command prompt, switch to the following path:

   C:\Program Files\ws\server\cserver\bin
2. Specify **C:\Program Files\ws\bin**
3. To register the storage device, run the following command:

   `smis.bat <User ID> <Password> add <Storage IP address> <Storage User ID> <Storage Password> [-p http]*`

   *Only specify if you use the http protocol.

   < UserID > and < Password > use the Windows management authority account of the server on SMI-S is installed. The IP address of the device the < Storage_UserID > and the < Storage_Password > specify the authentication information of the storage for < StorageIP >.
4. To check that information was registered, run the **smis.bat** file:

   `smis.bat <User ID> <Password> list`
5. Run the natest script that is located in the in **ws\bin** directory to check whether the SMI-S Provider could obtain the storage information. The following example outputs disc information of the storage:

   `natest.bat <User ID> <Password> disks`

Table 7-9 lists the information that is necessary when connecting to NetApp storage.

Table 7-9: Information for Connecting to NetApp Storage

Item	Details
IP address	Specify the IP address of the server where the Data ONTAP SMI-S Agent is installed.
Namespace	Specify `root/ontap`.
Existence of an SSL	Use the Data ONTAP SMI-S Agent settings.
Port Number	Use the Data ONTAP SMI-S Agent settings. By default: • Non-SSL communication: 5988 • SSL communication: 5989
User ID	Use the User ID of the server where the Data ONTAP SMI-S Agent is installed.
Password	Use the password that is associated with the User ID.

NOTE: In the **Monitoring** module, when you select a NetApp storage node, an icon displays when IT Operations Analyzer processes status information or when it gathers information for the component. Additionally, the following error message may display within 15 minutes:

KAZZ20087-E The update to the configuration was unsuccessful. The node name in which the failure occurred: <Device Name>

This error message displays when all of the following conditions exist:

1. The NetApp storage is being monitored.
2. The NetApp storage is managed on a Linux server using a Linux version SMI-S agent.
3. An HTTPS connection exists between the IT Operations Analyzer management server and the Linux version SMI-S agent that is being monitored.

Complete one of the following tasks:

- Register the IP address and Host name of the Linux version SMI-S agent into the host file of the server on which IT Operations Analyzer is installed: the management server.
- Change the current HTTPS connection method that exists between the IT Operations Analyzer management server and the Linux version SMI-S agent, to HTTP.
- Change the Linux version SMI-S agent to the Windows version SMI-S agent.

8

Preparing Dell servers

This chapter describes the tasks that are required to setup your Dell servers.

Overview

Two of each of the following must be set up:

- WMI/SNMP for Windows-based Dell server (Credential information).
- SSH/SNMP for Linux-based Dell server (Credential information).

Table 8-1 lists the information that is necessary when connecting to a Dell server.

Table 8-1: Information for Connecting to a Dell Server

Item	Details
IP address	Specify the IP address of the Dell server.
Port Number	The SNMP port where the Dell Server waits for the communication (port 161).
Community name	The Community name used for SNMP Dell Server.

Enabling SNMP service and trap communication

The SNMP agent on each monitored Dell server must be configured to send SNMP traps to the Hitachi IT Operations Analyzer management server.

When a Dell OMSA trap is received from the server, IT Operations Analyzer updates the status of the Dell OMSA Trap Component based on the severity of the received trap.

Configuring an SNMP Agent in a Microsoft Windows environment

To configure the Dell server's SNMP Agent in a Microsoft Windows environment:

1. From your **Desktop's Start** menu, select **Control Panel**.

NOTE: On Windows Server 2012, the steps to navigate to the **Start** menu is different.

2. Open **Administrative Tools**.
3. Open **Services**.
4. Right-click **SNMP Service** and select **Properties**.
5. Click the **Security** tab to open the **Security** dialog box.
6. Select **Accept SNMP packets from any host**, or select **Accept SNMP packets from these hosts** then click **Add**.

   The **SNMP Service Configuration** box displays.
7. Type the host name or IP address of the IT Operations Analyzer management server, then click **Add**.
8. Click the **Traps** tab to open the **Traps** dialog box.
9. Select the appropriate SNMP community name from the **Community Name** drop-down list, then click **Add** beneath the **Trap Destinations** list box.

   The **SNMP Service Configuration** box displays.

10. Type the host name or IP address of the IT Operations Analyzer management server, then click **Add**.
11. Click **OK** to close the dialog.

Configuring an SNMP Agent in a Linux environment

To configure the Dell server's SNMP Agent in a Red Hat Enterprise Linux environment:

1. Add the following line to the **/etc/snmp/snmpd.conf** configuration file:

   trapsink IP_address community_name

   The value of the **IP_address** variable is the IP address of the IT Operations Analyzer management server. The value of the **community_name** variable is the SNMP community name.

2. Restart the SNMP agent using the following command:

   /sbin/service snmpd restart

Index

V

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90IOS006-12