

Dell™ Smart Plug-in Version
1.0 For HP Operations
Manager Version 8.10 For
Microsoft® Windows®
User's Guide



Notes, Cautions, and Warnings



NOTE: A NOTE indicates important information that helps you make better use of your computer.



CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

Information in this document is subject to change without notice.

© 2010 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell*, the *DELL* logo, *OpenManage*, *PowerEdge*, and *PowerVault* are trademarks of Dell Inc.; *Microsoft*, and *Windows*, are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

January 2010

Contents

1	Introduction	5
	Accessing the Dell Smart Plug-in Installer	5
	Key Features and Benefits of the Dell Smart Plug-in	5
	Understanding the Dell Smart Plug-in	6
	Supported Dell Devices	8
	Supported Operating Systems	8
	Other Documents You May Need	8
	Obtaining Technical Support	9
2	Installing and Uninstalling the Dell Smart Plug-in (SPI)	11
	Configuring the Management Server for Dell SPI	11
	Configuring the Managed Systems	12
	Installing the Dell SPI	12
	Verifying the Installation of Dell SPI	13
	Uninstalling the Dell SPI	14
	Using the Repair Option in the Installer.	15

3	Using Dell Smart Plug-in (SPI)	17
	Features	17
	Deploying the Policies Automatically.	17
	Deploying the Policies Manually	18
	Auto-grouping Policy	18
	SNMP Interceptor Policy	19
	Understanding Dell SPI Trap Message	
	Severity	20
	SNMP Trap Based Severity Propagation.	20
	Monitoring the Health of Dell Devices	21
	Launching Dell OpenManage Server	
	Administrator.	21
	Launching OMSA from Tools	22
	Launching OMSA from the Node Group	22
	Launching OMSA from the Service Map	22
	Launching OMSA from the Alert Message.	23
4	Troubleshooting the Dell Smart Plug-in (SPI)	25
	Installer takes time to Launch	25
	SNMP Trap Messages Are Not Created	25
	SNMP Traps Received At Wrong Nodes	26
	Global Health Status Not Fetched for Dell Systems	26

Introduction

△ CAUTION: The procedures in this document should be performed only by personnel with knowledge and experience in using HPOM in order to avoid data corruption and/or data loss.

This guide is intended for system administrators who use Dell™ Smart Plug-in (SPI) on HP Operations Manager (HPOM) for Microsoft® Windows® version 8.10 to monitor Dell systems.

With the integration of Dell SPI into HPOM, you can use the HPOM console to monitor the availability of your Dell devices that are discovered in HPOM.

The readme file packaged with the Dell SPI contains the latest information about software and management station requirements, as well as information about known issues. The readme file is available on the Systems Management documentation page on the Dell Support website at support.dell.com/manuals. The readme file is also packaged in the self-extracting executable `Dell_Smart_Plugin_v1.0_A00.exe` file.

Accessing the Dell Smart Plug-in Installer

The Dell Smart Plug-in (`Dell_Smart_Plugin_1.0.msi`), readme file, and this user's guide are packaged in a self-extracting executable `Dell_Smart_Plugin_v1.0_A00.exe` file. You can download the installer from the Dell Support website at support.dell.com.

Key Features and Benefits of the Dell Smart Plug-in

The Dell SPI consists of different policies and tools that you can deploy on the management server. The Dell SPI enables you to:

- Group all the Dell systems present under the managed or unmanaged nodes with the supported Windows operating systems, under the **Dell Managed Systems** group in the HPOM console.

- Process Simple Network Management Protocol (SNMP) traps generated by Dell OpenManage™ Server Administrator (OMSA) and OpenManage Storage Systems (OMSS) running on Dell systems.
- Periodically monitor the global system health of Dell systems grouped under the **Dell Managed Systems** group.
- Launch OMSA web console as a tool from the HPOM console for troubleshooting the alerts.

Understanding the Dell Smart Plug-in

The Dell SPI consists of three policy files. After you install the Dell SPI, the HPOM console displays:

- The **SPI for Dell Devices** policy group under **Policy Management** → **Policy Groups**.
- The **Dell Hardware Service** in the **Service Map** view.
- The **Server Administrator** tool under **Tools**.

For more information on installing the Dell SPI, see "Installing and Uninstalling the Dell Smart Plug-in (SPI)."

Table 1.1 lists the policy files included in the Dell SPI.

Table 1-1. Dell SPI Policy Files

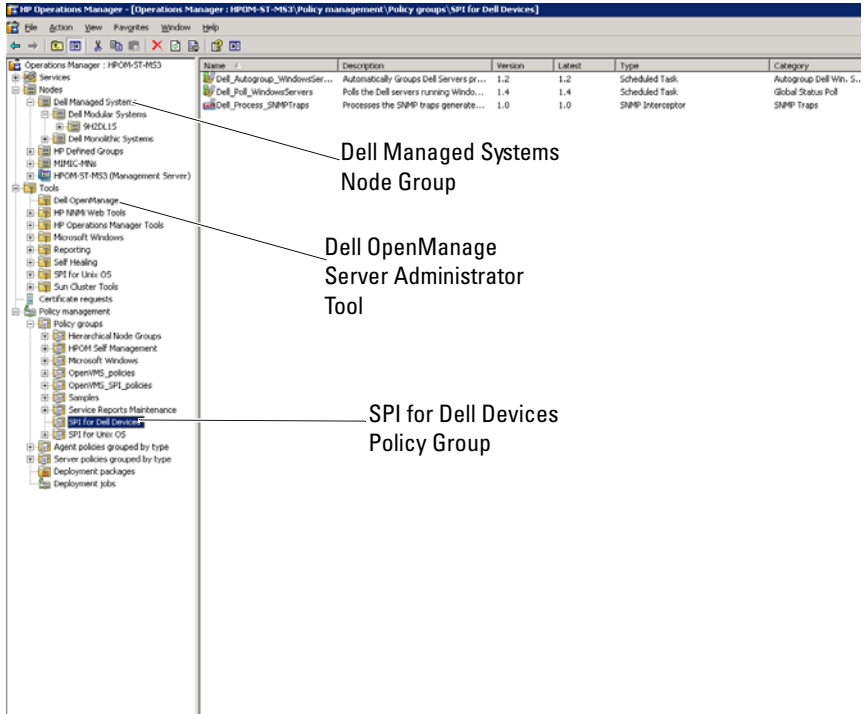
Policy File	Description
Dell_Autogroup_WindowsServers	<p>This policy scans across all managed nodes and external nodes, identifies the Dell systems configured under Nodes group, and groups them under Dell Managed Systems on the HPOM console.</p> <p>This policy groups only those Dell systems where you have installed the supported versions of OMSA and Windows operating system, and have enabled SNMP on the systems. This policy is scheduled to run at 23:00 hours everyday.</p>

Table 1-1. Dell SPI Policy Files

Policy File	Description
Dell_Process_SNMPTraps	This policy processes OMSA and OMSS SNMP traps from the Dell systems and sends appropriate messages to the HPOM console. The policy retrieves the global health status of the Dell system for every trap received from the system.
Dell_Poll_WindowsServers	This policy periodically polls the Dell systems grouped under Dell Managed Systems and retrieves the system health status information. The default schedule is 1 hour.

Figure 1-1 displays the HPOM console after you install the Dell SPI.

Figure 1-1. Dell SPI Deployed On HPOM Console



Supported Dell Devices

The following Dell devices are supported by the Dell SPI for HPOM:

- Dell PowerEdge systems - complete support for systems ranging from x8xx to xx1x (both inclusive) that have OMSA versions 5.3 to 6.2 installed on them.
- Dell PowerVault systems - support for systems ranging from x8xx to xx1x (both inclusive) that have OMSA versions 5.3 to 6.2 and above installed on them.

Supported Operating Systems

For the latest information on operating system support for the Dell SPI, see the readme file.

You can access the readme file from the Systems Management documentation page on the Dell Support website at support.dell.com/manuals or from the location where you have extracted the contents of `Dell_Smart_Plugin_v1.0_A00.exe` file.

Other Documents You May Need

Besides this *User's Guide*, you may need to refer to the following guides available on the Dell Support website at support.dell.com:

- The *Dell OpenManage Installation and Security User's Guide* provides detailed installation procedures and step-by-step instructions for installing, upgrading, and uninstalling Server Administrator for each supported operating system.
- The *Dell OpenManage Server Administrator Compatibility Guide* provides compatibility information about Server Administrator installation and operation on various hardware platforms (or systems) running supported operating systems.
- The *Dell OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in your Server Administrator home page Alert log or on the event viewer of your operating system. This guide explains the text, severity, and cause of each service alert message that the Server Administrator issues.

- The *Dell OpenManage Server Administrator Command Line Interface User's Guide* documents the complete command line interface for Server Administrator, including an explanation of the command line interface (CLI) commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.

For information on SNMP Trap correlation, see the *SNMP Trap Correlation Guide* on the Dell Support website at support.dell.com/manuals.

For information on terms used in this document, see the *Glossary* on the Dell Support website at support.dell.com/manuals.

Obtaining Technical Support

For assistance and information about Dell SPI, see the Dell Support website at support.dell.com.

Installing and Uninstalling the Dell Smart Plug-in (SPI)

You must install the pre-requisite software on your management server and managed systems before installing the Dell™ SPI.

A complete list of software requirements is provided in the Dell Smart Plug-in readme. The readme is available with the Dell SPI installer and on the Systems Management documentation page on the Dell Support website at support.dell.com/manuals.

Configuring the Management Server for Dell SPI

This section lists the steps to configure the management server to install the Dell SPI.



NOTE: You must have domain administrator privileges on the HPOM management server where you install the Dell SPI

- 1 Install HP Operations Manager (HPOM) for Microsoft® Windows® version 8.10 with the latest patches on the management server.

For more information on installing HPOM, refer to *HP Operations Manager Installation Guide*.

- 2 Install and enable the SNMP service to establish communication between the management server and the managed node.

Configuring the Managed Systems

This section lists the steps to configure the managed systems.

- 1 Install the supported Windows operating system on the managed systems.
- 2 Install and enable the SNMP service on the managed system and ensure that the management server is able to communicate with it. Configure the SNMP agent to change the community name, enable Get operations, and send traps to the HPOM management server. For information on configuring the SNMP agent, see the *OpenManage Server Administrator User Guide* available on the Dell Support website at support.dell.com/manuals.
- 3 Install Dell OpenManage™ Server Administrator (OMSA). The supported versions of OMSA are versions 5.3 to 6.2.

You can download OMSA from the Dell Support website at support.dell.com.

Installing the Dell SPI

This section provides the instructions to install the Dell SPI.



NOTE: You must close the HPOM console before you install or uninstall the Dell SPI.

To install the Dell SPI on the HPOM management server:

- 1 Download the Dell SPI from the Dell Support website at support.dell.com. The `Dell_Smart_Plugin_v1.0_A00.exe` is a self-extracting.exe file.
- 2 Login to the HPOM management server as the user with domain administrator privileges.
- 3 Ensure that HPOM version 8.10 for Windows is installed correctly and running on the management server.
- 4 Run the `Dell_Smart_Plugin_v1.0_A00.exe` on the management server. Extract the contents under any folder on the system.
- 5 Run the `Dell Smart Plug-In 1.0.msi` from the folder where you extracted the contents of the self extracting package.
- 6 Follow the wizard to install the Dell SPI.

During the installation process, you can choose to auto-deploy the policy files. If you do not choose to auto-deploy the policy files during installation, then you must deploy them manually on the management server. For more information, see "Deploying the Policies Automatically" and "Deploying the Policies Manually".

When the installation process completes, you can verify the installation.

Verifying the Installation of Dell SPI

To verify the installation of the Dell SPI:

- 1** Launch the HPOM console and verify that the **SPI for Dell Devices** policy group is created under **Policy Management** → **Policy Groups**.
- 2** Verify that the following policies are present under the **SPI for Dell Devices** policy group:
 - **Dell_Autogroup_WindowsServers**
 - **Dell_Process_SNMPTraps**
 - **Dell_Poll_WindowsServers**
- 3** Verify that the HPOM console displays the **Dell Hardware** node under **Service** → **System Infrastructure** and displays the service map for all Dell devices.
- 4** Verify that the HPOM console displays the **Server Administrator** tool under **Tools**.
- 5** If you have chosen to auto-deploy the policy files during installation:
 - Select the management server under **Nodes**.
 - Right click and select **View** → **Policy Inventory**. The Dell SPI policies are displayed on the right pane.

Uninstalling the Dell SPI

You can uninstall the Dell SPI from the Windows[®] Control Panel. Before you uninstall the Dell SPI, ensure the following:

- The Dell policies are not running on the management server.
- Users of the Dell SPI policies have logged out of the system.



NOTE: You must always uninstall the Dell SPI first before you uninstall HPOM. If you uninstall HPOM first and then attempt to uninstall the Dell SPI, the uninstallation process displays several errors and fails.



NOTE: When you uninstall the Dell SPI, the following error may be displayed: "One or more Dell SPI processes in progress. Cannot proceed with uninstallation." To resolve this, disable the policies, or wait till the policies complete execution, and then retry the uninstallation.

To remove the Dell SPI from the HPOM management server:

- 1 From the Start menu select **Settings** → **Control Panel** and open **Add/Remove Programs/Programs and Features**.
- 2 Select **Dell Smart Plug-in 1.0** and click **Remove**.

The uninstallation process removes the Dell SPI from the HPOM management server.


To verify that the Dell SPI is completely uninstalled from the management server:

- 1 Launch the HPOM console and ensure that the **SPI for Dell Devices** policy group under **Policy Management**—**Policy Group** is removed.
- 2 Click **Nodes** and ensure that the **Dell Managed Systems Group** is removed.
- 3 Click **Service** → **System Infrastructure** and ensure that the **Dell Hardware** node and the service map for all Dell deviceez is removed.
- 4 Click **Tools** and ensure that the **Server Administrator** tool is removed.

Using the Repair Option in the Installer

If you delete any of the policies from the **SPI for Dell Devices** policy group, or from the Policy Inventory of the management server, use the **Repair** option in the Dell SPI installer to re-install the policies.

The **Repair** option installs the missing Dell SPI policies, and automatically deploys all the policies on the management server.

 **NOTE:** If you modify any of the policies and then delete them, the Repair option installs only the original version of the policies. You must modify them again as per your requirements.

Additionally, if the **Dell Server Helper.dll** file is missing or corrupted, the **Repair** option replaces the file.

Using Dell Smart Plug-in (SPI)

This chapter discusses the various operations that you can perform after you install the Dell™ SPI on the HP Operations Manager (HPOM) management server.

Features

After you deploy the policies on the management server you can:

- Group all the Dell systems present under the managed or unmanaged nodes with the supported Windows operating systems, under the **Dell Managed Systems** group in the HPOM console.
- Process Simple Network Management Protocol (SNMP) traps generated by Dell OpenManage™ Server Administrator (OMSA) and OpenManage Storage Systems (OMSS) running on Dell systems.
- Periodically monitor the global system health of Dell systems grouped under the **Dell Managed Systems** group.
- Launch Dell OpenManage™ Server Administrator (OMSA) web console as a tool from the HPOM console for troubleshooting the alerts.

After you install the Dell SPI on the HPOM management server, you can see the policy files under **Policy Management → Policy Groups → SPI for Dell Devices** on the HPOM console.

Deploying the Policies Automatically

You can choose to deploy the Dell SPI policies on the management server when you install the Dell SPI.

If you automatically deploy the policies, the policies run as per the default schedule.

Deploying the Policies Manually

You can deploy the policies manually after you complete installing the Dell SPI.

To deploy the policies manually:

- 1 Launch the HPOM console and navigate to **Policy Management** → **Policy Groups** → **SPI for Dell Devices**.
- 2 Select the policy that you want to deploy.
- 3 Right click and select **All Tasks** → **Deploy on**. The **Deploy policies on** screen is displayed.
- 4 Select the management server and click **OK**. The policy is deployed on the management server and runs as per the default schedule.



NOTE: Ensure that you deploy the policies only on the management server and not on the managed nodes.

Auto-grouping Policy

The auto-grouping policy **Dell_Autogroup_WindowsServers** is a **Scheduled Task**. The policy is scheduled to run at 23:00 hours every day.

The auto-grouping policy:

- Identifies Dell systems running the supported Microsoft® Windows® operating systems, have OMSA installed on them, and have SNMP enabled.
- Groups Dell PowerEdge™ and PowerVault™ systems running supported Microsoft Windows operating systems under the **Dell Managed Systems** node group on the HPOM console.
- Groups the PowerEdge and PowerVault systems under two broad categories — **Dell Monolithic Systems** and **Dell Modular Systems**.
 - **Dell Modular Systems**. Creates a group with the Chassis Service tag as the name of the group. All the blade servers belonging to the same chassis are grouped under the **Chassis Service tag** group.
 - **Dell Monolithic Systems**. Groups all the monolithic servers.
- Creates three services corresponding to each node under **Dell Managed Systems** in **HPOM Service Map** view.

To view the Dell systems in the HPOM Service Map view:

- a** Select **Systems Infrastructure** under **Services** in the HPOM console. The Service Map view is displayed on the right pane.
- b** Click **Dell Hardware** and click **Dell Windows Servers**. The **Service Map** view displays all the Dell systems that are grouped under **Dell Modular Systems** and **Dell Monolithic Systems**.
- c** Every system in the Service Map view has two components — **Dell SNMP Traps** and **Dell Server Health**. The two components display the severity status of the system based on SNMP traps and Server Health Poll. For more information see, "SNMP Trap Based Severity Propagation".



NOTE: To know the actual health of the Dell system, you must view the status in the **Dell Server Global Health** service.

SNMP Interceptor Policy

The SNMP interceptor policy **Dell_Process_SNMPTraps** processes all SNMP traps sent from the Dell systems to the management server, generates formatted messages, and sends them to the HPOM console. The SNMP Interceptor policy has pre-defined rules for processing all the OMSA/OMSS traps sent by the Dell devices.

For every trap received from the Dell systems, the SNMP interceptor policy processes the traps in the following manner:

- 1** Sends a message to the active message browser of the node, which sends the trap.
- 2** Reflects the severity of the message in the **Dell SNMP Traps** service in the **Service Map** view.
- 3** Retrieves the global health status of the node and sends a message with the global health status to the active message browser of the node. You can also view the global health status in the global health service of the node.

- 4 Auto-acknowledges the trap once it receives a **Clear Event** trap. For more information on the trap correlation, see the *Dell SPI Trap Correlation Guide* available on the Dell Support website at support.dell.com/manuals.



NOTE: If there is any message corresponding to an SNMP trap present in an active message browser for a particular Dell system, and the SNMP interceptor policy receives the same trap again, then it is counted as a duplicate of the existing trap.



NOTE: If a node is not DNS resolvable, the Dell SPI may not update the global health status for that node.

Understanding Dell SPI Trap Message Severity

Traps often contain information about values recorded by probes or sensors. Probes and sensors monitor critical components for values such as amperage, voltage, and temperature. When an event occurs on the Dell system, it sends a trap having one of the following severities:

- **Normal** — An event that describes the successful operation of a unit, such as a power supply turning on, or a sensor reading returning to normal.
- **Warning** — An event that is not necessarily significant, but may indicate a possible future problem, such as crossing a warning threshold.
- **Critical** — A significant event that indicates actual or imminent loss of data or loss of function, such as crossing a failure threshold or a hardware failure.

SNMP Trap Based Severity Propagation

The severity propagation for the managed nodes is different for both the **Nodes** view and the **Service Map** view.

The following table describes the severity propagation based on SNMP traps.

Table 3-2. Severity Propagation Behavior

View	Description
Nodes View	The node status displays the highest severity of all the active messages. This status is propagated to the parent node groups. To know the actual health of the node, view the status in the Dell Server Global Health service.

Table 3-2. Severity Propagation Behavior

View	Description
Service Map View	The Dell SNMP Traps service displays the highest severity of all the active trap messages of the corresponding node. This is not propagated to the parent services. The Dell Server Global Health service displays the present health status of the corresponding node, and this is propagated to the parent object.

Monitoring the Health of Dell Devices

The global status update policy **Dell_Poll_WindowsServers** is a scheduled policy that updates the global status of the Dell systems periodically. The default schedule for this policy is 1 hour.

The global status update policy polls each of the Dell systems that are grouped under the **Dell Managed Systems** node group to get the global system status and sends corresponding severity messages to the active message browsers of the nodes.

The global health is the overall health of the system. However, the health of the individual components of the system may differ. To view the health of the individual components, launch the **Server Administrator** tool.

The policy also updates the status of the systems under the **Dell Server Global Health** component in the **Service Map** view.



NOTE: Until the **Dell_Autogroup_WindowsServers** policy runs for the first time, and the Dell systems are grouped under the **Dell Managed Systems** group, the global health status of the systems is not displayed on the HPOM console.

Launching Dell OpenManage Server Administrator

The Dell SPI enables you to launch the OMSA web console from the HPOM console. You can launch the OMSA web console to get more information about the Dell system you are monitoring. After you install the Dell SPI, you can see the **Dell OpenManage** folder under **Tools** on the HPOM console.

You can launch OMSA using any of the options given below.

Launching OMSA from Tools

To launch the OMSA web console from the **Tools** folder on the HPOM console:

- 1 Select **Tools** → **Dell OpenManage** on the HPOM console.
- 2 Select **Server Administrator** on the right pane and right click.
- 3 Select **All Tasks** → **Launch Tool** from the pop-up menu. The **Edit Parameters** window is displayed.
- 4 Select any Dell system under **Dell Managed Systems**.

You can select only a single system under the parent nodes. If you select any of the parent nodes such as **Dell Managed Systems**, **Dell Modular Systems**, **Dell Monolithic Systems**, or the chassis group under **Dell Modular Systems** the following message is displayed "Tool cannot be launched on multiple nodes".

- 5 Click **Launch** on the **Edit Parameters** window. The OMSA web console is launched on the default browser on your system.



NOTE: The HPOM enables you to select even non-Dell systems. However, if you select such a system, the OMSA web console does not launch.

Launching OMSA from the Node Group

To launch the OMSA web console from the **Dell Managed Systems** node group:

- 1 Select any Dell system under any of the parent nodes such as **Dell Monolithic Systems**, or the chassis group under **Dell Modular Systems**.
- 2 Right click and select the **All Tasks** → **Launch Tool** option from the pop-up menu. The **Select the Tool to Execute** window is displayed.
- 3 Select **Server Administrator** under **Tools** → **Dell OpenManage** and click **Launch**. The OMSA web console is launched on the default browser on your system.

Launching OMSA from the Service Map

To launch the OMSA web console from the **Dell Hardware** → **Dell Servers** service map object:

- 1 Select any Dell system under **Dell Servers** on the **Service Map** view.

- 2 Right click and select the **Launch Tool** option from the pop-up menu. The **Select the Tool to Execute** window is displayed.
- 3 Select **Server Administrator** under **Tools** → **Dell OpenManage** and click **Launch**. The OMSA web console is launched on the default browser on your system.

Launching OMSA from the Alert Message

To launch the OMSA web console from the alert messages associated with a Dell system:

- 1 Select any Dell system under any of the parent nodes such as **Dell Monolithic Systems**, or the chassis group under **Dell Modular Systems**.
- 2 Select any alert message associated with the system on the right pane.
- 3 Right-click and select **Launch Tool** → **Message**, **Launch Tool** → **Nodes**, or **Launch Tools** → **Service** from the pop-up menu. The **Select the Tool to Execute** window is displayed.
- 4 Select **Server Administrator** under **Tools** → **Dell OpenManage** and click **Launch**. The OMSA web console is launched on the default browser on your system.

Troubleshooting the Dell Smart Plug-in (SPI)

This section lists the problems that you may encounter while using the Dell™ SPI.

Installer takes time to Launch

When the Dell SPI installer is run for first time on the management server, there is a delay of 40-45 seconds to launch the installer if the system does not have access to the internet.

This problem occurs because a .NET Framework 2.0 managed assembly that has an Authenticode signature takes longer than usual to load. The signature is always verified when the .NET Framework 2.0 managed assembly that has an Authenticode signature is loaded.

To resolve this, ensure that the management server is connected to the internet when you run the installer.

SNMP Trap Messages Are Not Created

The SNMP Interceptor policy may not display the SNMP trap messages in the active message browser of the node from which it receives the traps.

To resolve this, ensure that the trap destinations and the community strings on the Dell managed nodes are configured correctly and communication is established between the managed node and the management server.

SNMP Traps Received At Wrong Nodes

After you start monitoring the Dell systems grouped under **Dell Managed Systems** group, if you interchange the IP addresses of the nodes, then the SNMP traps are received on the wrong nodes. For example, if you have two nodes A and B under **Dell Managed Systems** → **Dell Monolithic Servers** group and you interchange the IP addresses of the two nodes, then the traps from A are displayed as messages in the active message browser of B and vice versa.

To resolve this:

- 1 Launch the Server Configuration Editor on the HP Operations Manager (HPOM) console.
- 2 Under the **Node Cache Settings** option, set the **DNS cache** value to **False** to disable the DNS caching.

The nodes now display the traps correctly.

Global Health Status Not Fetched for Dell Systems

The global status update policy **Dell_Poll_WindowsServers** does not fetch the global health of discovered Dell systems till the systems are grouped under the **Dell Managed Systems** group.

If you choose to auto-deploy the policy files during installation of the Dell SPI, the policies start running as per the default schedule. The global status update policy runs every 1 hour and starts polling systems for global health status. However, the auto grouping policy is scheduled to run only at 23:00 hours every day. Therefore, until the **Dell_Autogroup_WindowsServer** policy runs and the Dell systems are grouped under the **Dell Managed Systems** group, the global health status of the systems is not displayed on the HPOM console.