Integrating Dell PowerEdge Servers into HP Systems Insight Manager 7.1

This paper explains how to integrate Dell PowerEdge servers into an environment managed by HP Systems Insight Manager 7.1.

Niven Brooks

Onsite Systems Engineer

Dell Enterprise Solutions

August 2012| Rev 2.0

Contents

Figures

Executive summary

This paper details the specific steps needed to add a Dell™ PowerEdge™ server running the Microsoft® Windows Server® 2008 R2 operating system to an environment currently being managed by Hewlett-Packard® Systems Insight Manager (HPSIM) version 7.1. To add a Dell server running VMware® or Linux®, the HPSIM and Dell OpenManage™ Server Administrator (OMSA)[1] configuration is similar, substituting Linux or VMWare instructions for the Windows instructions provided below.

At a high level, the steps for integrating Dell PowerEdge servers into an environment managed by HP Systems Insight Manager are:

1. Load and configure OpenManage Server Administrator on the Dell server in order to forward events to HPSIM.
2. Load the Dell management information bases (MIBs) into HPSIM so it can properly interpret information from OMSA.
3. Configure HPSIM to recognize Dell servers.
4. Generate test events.

Introduction

In response to the need for increased productivity of system administrators, server vendors have developed systems management tools. Dell's systems management tools are provided via the Dell OpenManage suite of products. While these products cover software deployment, hardware configuration, asset management, remote support, and system health monitoring, this paper focuses on system health monitoring.[2]

To monitor the health of Dell servers using Dell's OpenManage tools, OMSA instrumentation is installed on supported[3] Dell PowerEdge servers. One instance of OpenManage Essentials is installed and configured for monitoring the instrumented PowerEdge servers. Errors detected by Server Administrator are then forwarded via SNMP to OpenManage Essentials, where they are logged and can generate email or other notifications.

Since the HPSIM environment uses the same architecture, it is possible to integrate instrumented Dell PowerEdge servers into HPSIM by taking advantage of the industry-standard interfaces of SNMP and Hypertext Transport Protocol – Secure (HTTPS) in Server Administrator. These interfaces allow administrators to continue to use their existing HPSIM-based notification processes while fully benefitting from the use of Server Administrator on supported Dell servers.

HPSIM 7.1 has some built-in third-party device support, including some Dell PowerEdge servers. In some cases the Dell server can be detected and managed from the default HPSIM installation without any further customization. However, the built-in third-party device support may not be comprehensive, especially for newer Dell PowerEdge models, and it is recommended that the Dell-provided MIBs are used to monitor Dell servers.

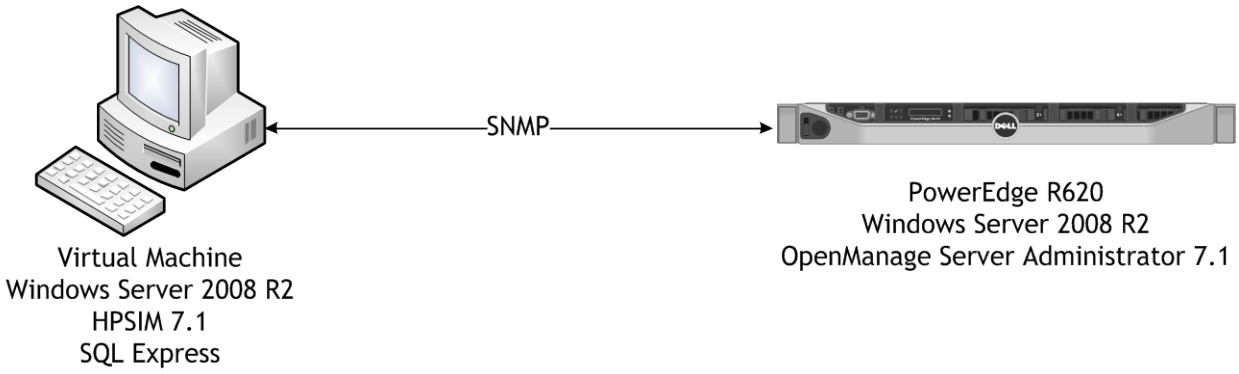
---

[1] In this paper, OpenManage Server Administrator is referenced as either OMSA or Server Administrator.
[2] For information on how to monitor Dell servers without the use of OMSA, see the article, *Agent-Free Monitoring of Dell PowerEdge 12th Generation Servers Using iDRAC7 in HP Systems Insight Manager*.
[3] Supported versions of OpenManage Server Administrator are available on Support.Dell.com for each Dell PowerEdge product.

Architecture of the test environment

To provide an example of how to integrate Dell PowerEdge servers into an environment managed by HP Systems Insight Manager 7.1, one Dell PowerEdge server was configured to report to one instance of HPSIM. Windows Server 2008 R2 was installed on a Dell PowerEdge R620 that acted as the managed node, and Windows Server 2008 R2 was installed in a virtual machine on a second host in which HPSIM was loaded. On the PowerEdge R620 server, the operating system was loaded using the Lifecycle Controller with defaults selected. HP Systems Insight Manager 7.1 was installed in the virtual machine along with HPSIM's default installation of Microsoft SQL Server® Express.

Figure 1. Architecture of the test environment



SNMP configuration

The SNMP community name is like a password both HPSIM and Server Administrator use to communicate. To enhance security, access can be read-only to the Dell servers. This prohibits using SNMP to make changes to the server, such as changing threshold settings or shutting it down, but allows Server Administrator to send alerts to a console when status changes. A Dell PowerEdge server can function in a read-only SNMP environment, but it is possible that other devices need SNMP set to read-write.

Because OpenManage Server Administrator leverages the operating system's SNMP service for SNMP communication, the managed system's SNMP service must be configured correctly before Server Administrator can communicate with HPSIM.

For this paper, the community name of *Dell* with read-only rights was used with a single trap destination: the virtual machine running HPSIM. SNMP settings need to be configured on each Dell server added to the environment.

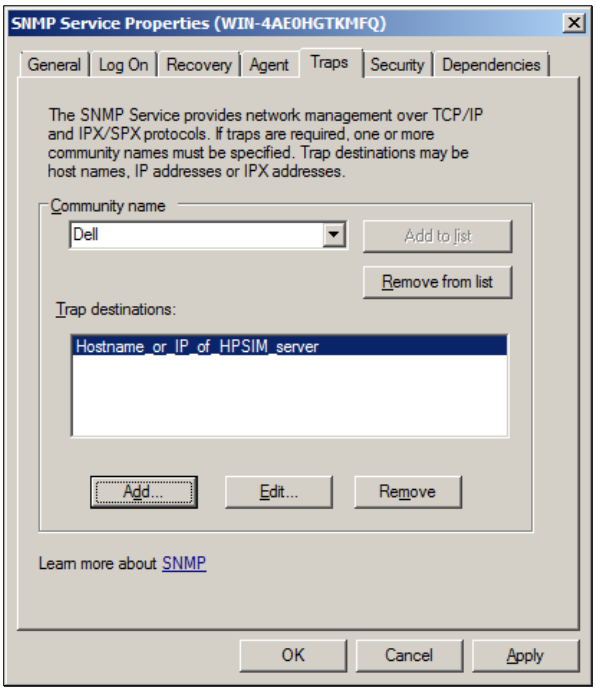
NOTE: The default installation of Windows Server 2008 R2 does not install the SNMP feature. To install the SNMP feature, follow these steps:

1. Click **Start > Administrative Tools > Server Manager.**
2. Click **Features** in the left-hand pane of the **Server Manager** window.
3. Click **Add Features.**
4. Check the **SNMP Services** checkbox, and then click **Next.**
5. Click **Install** to install the SNMP Services feature, and then click **Close**.

After installing the SNMP Services feature, set the parameters in the **SNMP Service Properties** dialog box:

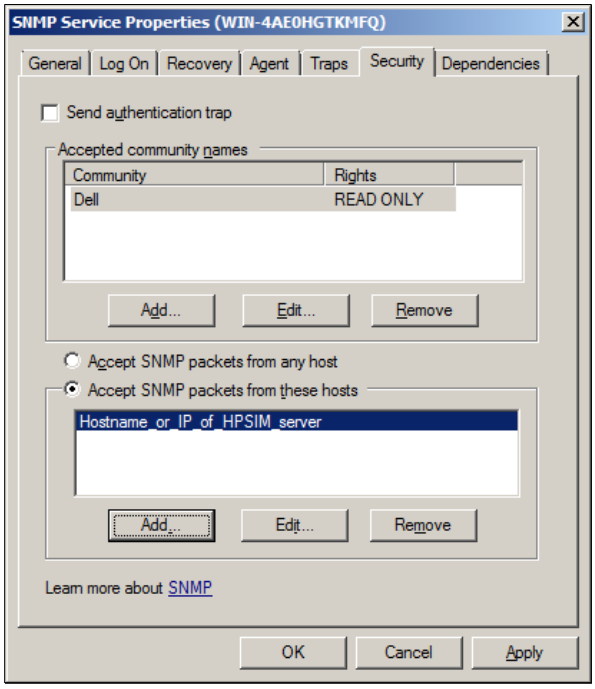
1. Click **Start > Administrative Tools > Server Manager.**
2. Expand **Configuration** in the left-hand pane and click **Services**.
3. Double-click **SNMP Service.**
4. On the **Traps** tab add a **Community name** and **Trap destinations** as shown in Figure 2.

Figure 2. SNMP Service Traps tab



5. On the **Security** tab uncheck **Send authentication trap**, and add a **community name** and configure packet security as shown in Figure 3.
6. Click **OK** to apply the changes.
   NOTE: The SNMP service does not need to be restarted for these changes to take effect.

Figure 3. SNMP Service Security tab



Loading Server Administrator

The latest version of Server Administrator for your Dell PowerEdge server managed node is available on Support.Dell.com. To find the latest version:

1. Navigate to Support.Dell.com in your browser.
2. Under **Support for Enterprise IT**, click the **Start Here** button**.**
3. Under **Product Support**, click the **Select a product** button**.**
4. If a product other than the PowerEdge server you intend to manage is selected, click **Select a Different Product** and choose the server you will manage. You are prompted through a series of menu options to navigate to your server model.
5. Click **Drivers & Downloads.**
6. Ensure that the OS selected matches that of your managed node.
7. Click **Systems Management.**
8. Click **OpenManage Server Administrator Managed Node**.
9. Click **Download file.**

In addition to manually loading Server Administrator on a single server, as covered in this paper, you can completely script and automate the install. For more information see the Dell OpenManage Server Administrator Version 7.1 Installation Guide.

To install Dell OpenManage Server Administrator on a PowerEdge server:

1. Double-click the downloaded file and click **Install.**
2. Click **Next.**
3. Read the Dell Software License Agreement, select **I accept the terms in the license agreement**, and click **Next.**
4. Ensure **Typical** is selected and click **Next.**
5. Click **Install**, and then click **Finish.**

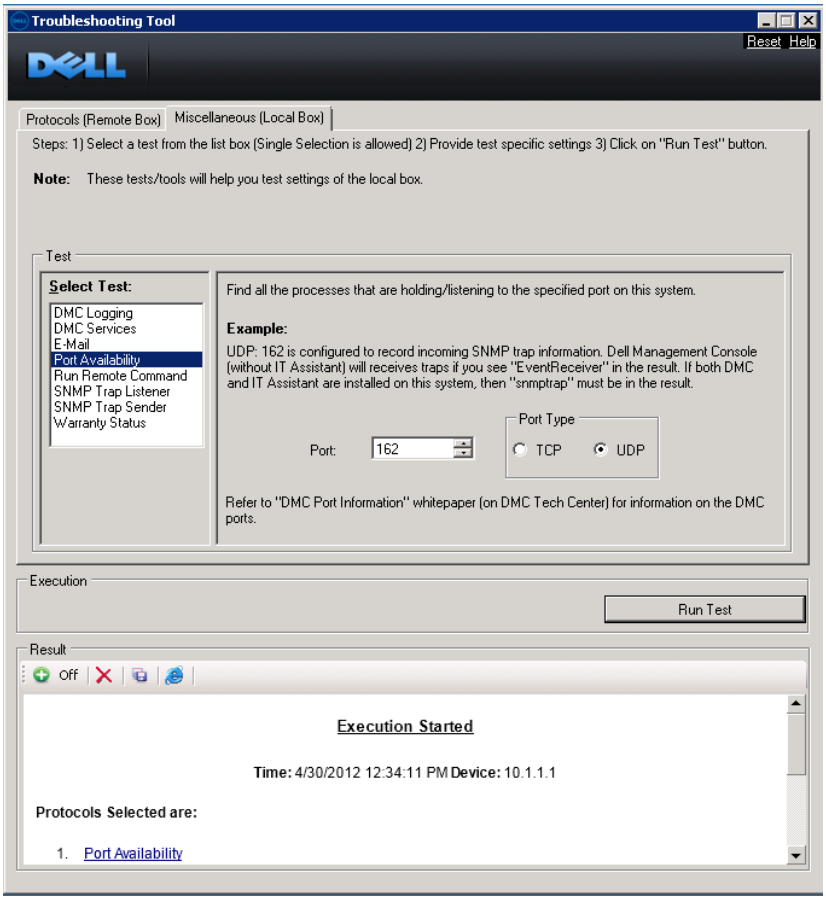
Testing Server Administrator

After installation, Server Administrator can be checked to see that it is operating correctly:

1. Launch Server Administrator from the server's desktop icon or open a browser and enter **https://IP_or_SystemName:1311** where IP_or_SystemName is the IP address or network name of the system.
   NOTE: The address **https://IP_or_SystemName:1311** can be used from any system with network access to the server to access Server Administrator.
2. Log in to Server Administrator as Administrator or other account with administrative privileges.
   NOTE: Because Server Administrator is an application, it uses operating system credentials.
3. Select **System** in the left-hand navigation tree. The status icons should all be green checks to indicate an error-free status.

At this point, everything should be working correctly on the Dell system. A further check would be to use the OpenManage Essentials Troubleshooting Tool available on Dell TechCenter. This extremely useful tool provides protocol testing on numerous levels including ICMP (ping) and SNMP.

Figure 4. Troubleshooting Tool



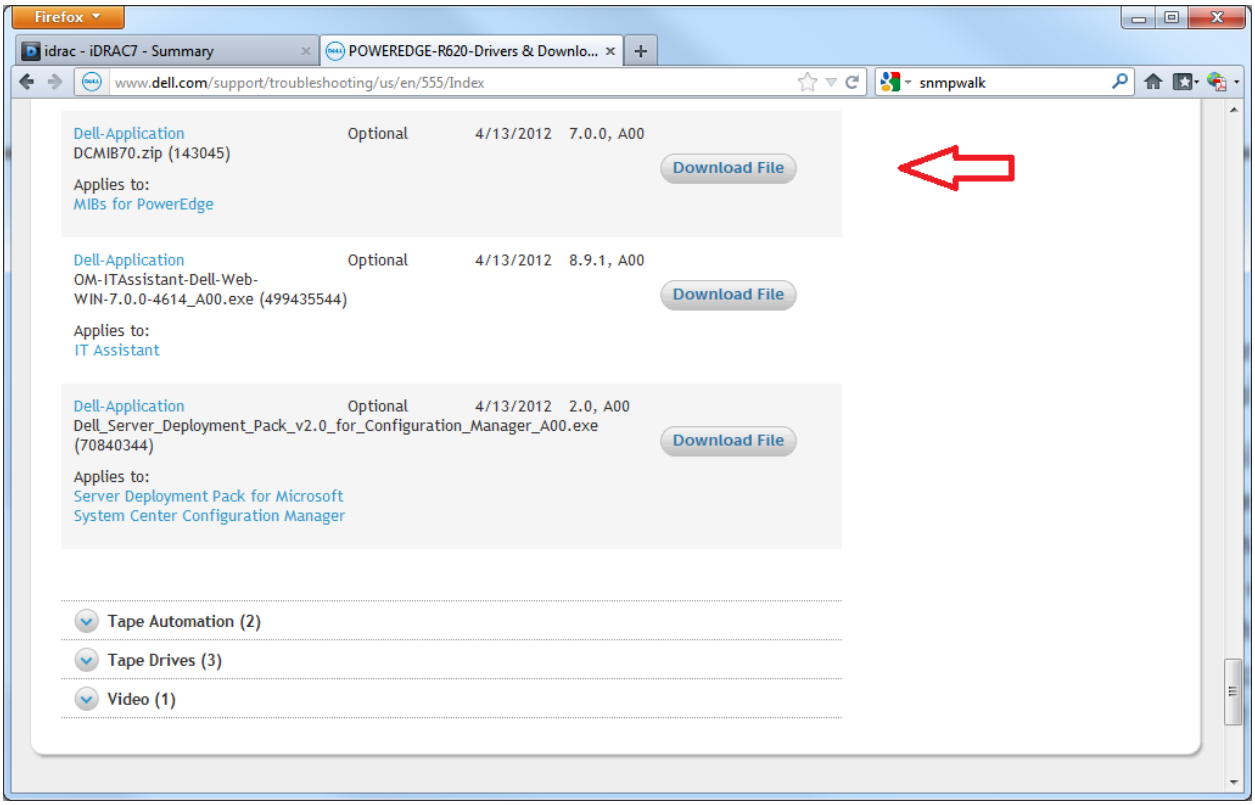
Importing the Dell MIBs into HPSIM

Now that SNMP is configured and Server Administrator is installed, the next step is to import the Dell MIB files into HPSIM so it can properly interpret the SNMP packets and traps that the Dell server will send to it.

Obtaining the Dell MIBs

Dell MIB files can be found under **Systems Management** on Support.Dell.com as shown in the Figure 5:

Figure 5. Dell MIBs on Support.Dell.com



After downloading the package, expand the package to a folder such as c:\DCMIB70. In general, the version of the MIB package matches that of the associated OpenManage software release and these versions should match, or at least be very close. For example, because OpenManage release 7.1 is used for server instrumentation for this paper, the DCMIB70 MIBs are used, which are the closest match at the time this paper was authored.

The two essential MIBs are:

- **10892**, which provides detailed information about the systems monitored by Server Administrator instrumentation software, such as system type, voltages, temps, and it is the primary MIB for PowerEdge systems.
- **dcstorag**, which provides detailed information about the storage hardware components and RAID configurations monitored by Server Administrator's Storage Management Service.

A number of other MIBs are included on the DCMIBxx download package, but are beyond the scope of this paper. A description of all the MIBs and their use is documented in Appendix A, and a full description can be found in the Dell OpenManage Server Administrator SNMP Reference Guide.

Uploading the Dell MIBs to HPSIM

To upload the MIBs, simply copy them from the **DCMIBxx** folder to the **\Program Files\HP\Systems Insight Manager\mibs** folder:

1. Copy **10892.mib** and **dcstorag.mib** from the **DCMIBxx** folder to **\Program Files\HP\Systems Insight Manager\mibs**.
2. Rename **\Program Files\HP\Systems Insight Manager\mibs\10892.mib** to **new10892.mib**
3. For consistency, also rename **dcstorag.mib** to **newdcstorag.mib**.

   NOTE: **dell10892.mib** and **dellarymgr.mib** (used with Dell's older Array Manager storage management tool) already exist in this folder because they come with the default installation of HPSIM. It is recommended that these names be avoided for the new files to avoid confusion with MIBs from HP and Dell.

Compiling the new Dell MIBs

Compiling the MIBs creates an intermediate **.cfg** file that HPSIM can later register. To compile the Dell MIBs:

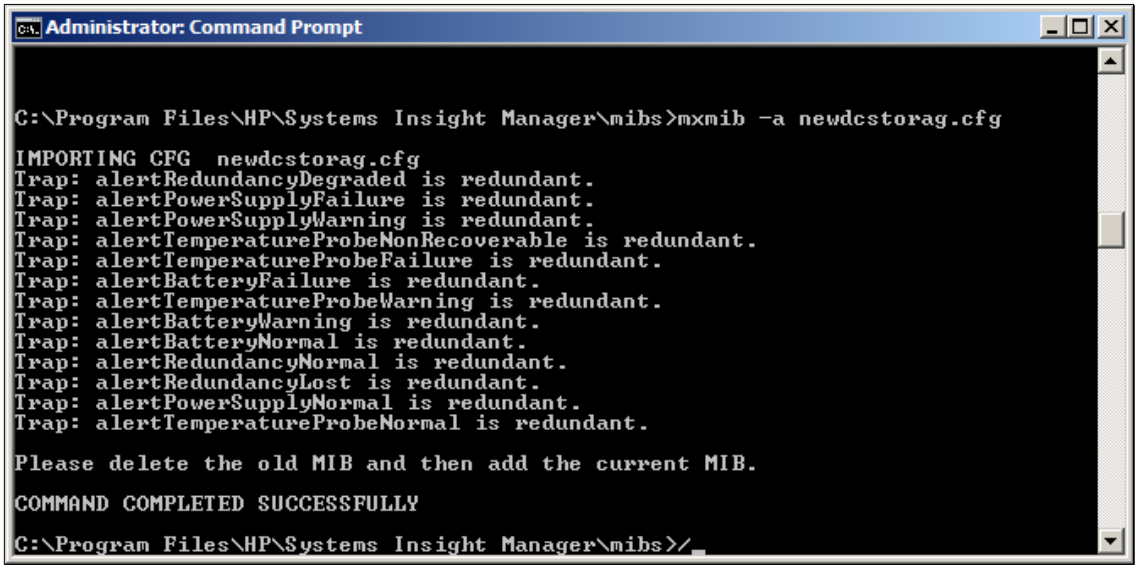
1. Open a command window (cmd.exe) as Administrator.
2. Using the **cd** command, change the working directory to:
   \Program Files\HP\Systems Insight Manager\mibs
3. Enter the command **mcompile new10892.mib**. The MIB should compile and return the message "**Mib Compilation completed successfully**".
4. Enter the command **mcompile newdcstorag.mib**. The MIB should compile and return the message "**Mib Compilation completed successfully".**

Registering the MIBs

Registering MIBs to HPSIM is the process that maps the SNMP information received from the Dell server to numbers and character strings that can then be used for identification and notification messages. Register both essential MIBs as follows:

1. Enter the command **mxmib -a new10892.cfg**. The cfg file should register and return the message "COMMAND COMPLETED SUCESSFULLY".
2. Enter the command **mxmib -a newdcstorag.mib**. The cfg file should register and return the message "COMMAND COMPLETED SUCESSFULLY", but with some redundancy warnings. These warnings are caused by traps duplicated in the Dell MIBs and can be ignored.

Figure 6. MIB registration



System Type Manager

When a new system is detected through a ping sweep or when receiving a SNMP Trap, it is added to the HPSIM database. The System Type Manager then does a sequence of queries to the new device to determine its identity. The following steps configure HPSIM to look for specific information in the Dell provided MIBs to tell System Type Manager that the device found is a PowerEdge server. This only needs to be done once, as all Dell servers running Server Administrator are displayed the same way to HPSIM.

To configure the Device Type Manager to recognize a Dell server:

1. Log in to HPSIM.
2. Select **Options -> Manage System Types**.
3. On the **Product model identification rules** list, scroll down and select **Dell Server**.
4. To prevent confusion and simplify administration, click the **Delete** button to delete the existing Dell Server entry, and click **OK** to confirm.

5. Click the **New…** button. The **New rule pane** will open below.

   NOTE: While values may be manually entered in the dialog boxes presented in the New Rule window, querying a Dell server for these values prevents typographical errors and provides verification that SNMP communication is working properly.

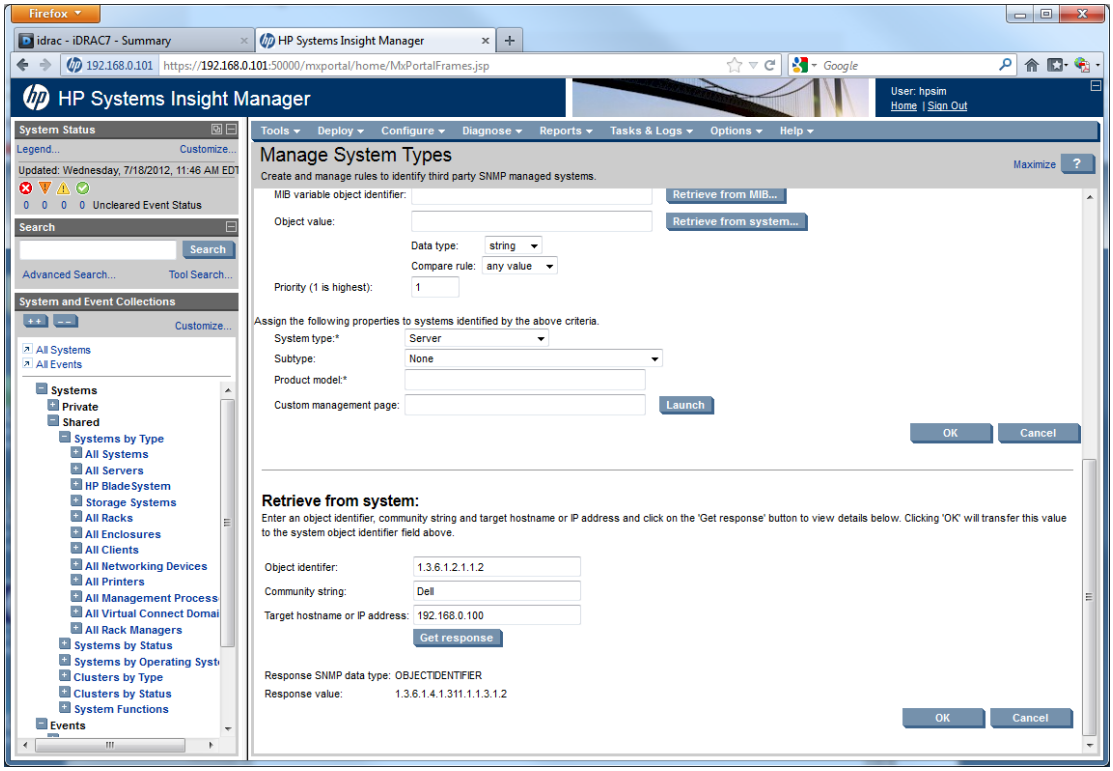
6. Click **Object identifier** and click the **Retrieve from system…** button. The **Retrieve from system** pane opens below the current pane.

7. In the **Retrieve from system** pane, change the **Community string** to the appropriate value.

8. Enter the hostname or IP address of the target Dell system in the **Target hostname or IP address** text box.

9. Click the **Get response** button. Note that the **Response value** is **1.3.6.1.4.1.311.1.1.3.1.2**. This is a generic Windows response value and indicates that SNMP communication is working properly.

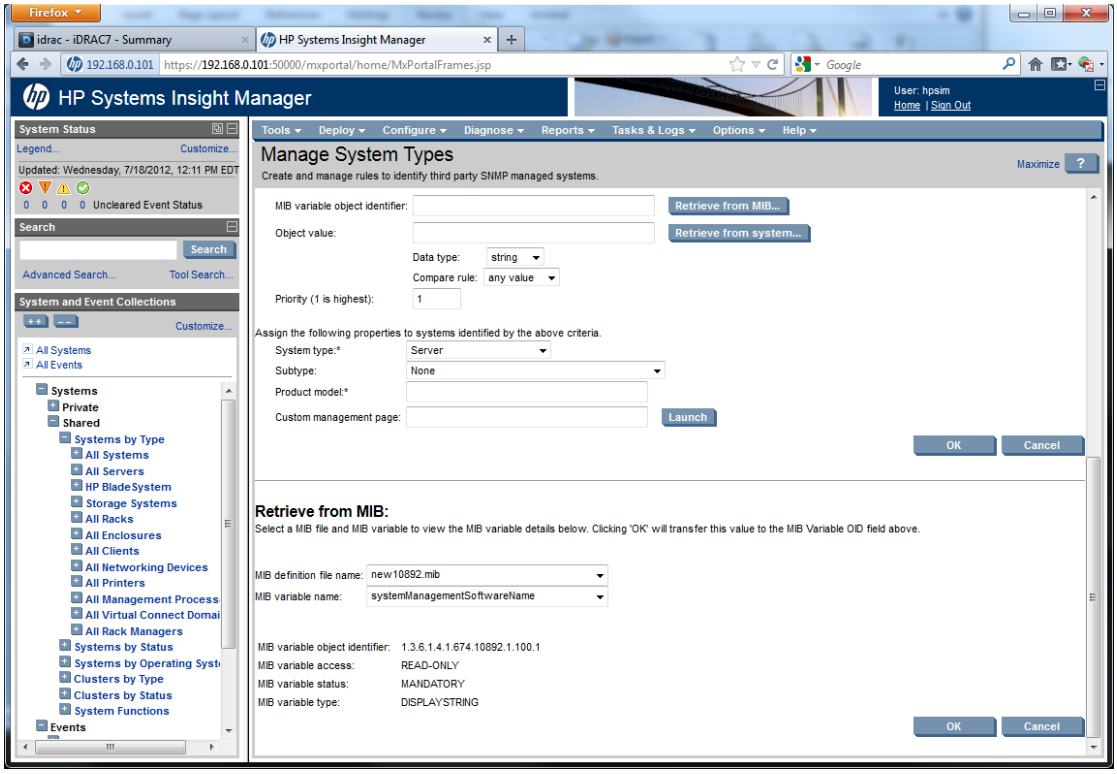
Figure 7. Retrieve from system



10. Click the **OK** button to accept this value and return to the **New rule** pane. The **System object identifier** text box will automatically populate.

11. Click the **MIB variable object identifier** and click the **Retrieve from MIB…** button. The **Retrieve from MIB** pane will appear below the current pane.
12. Select the **MIB definition file name** and choose **new10892.mib** from the list.
13. Select the **MIB variable name** and choose **systemManagementSoftwareName**.

Figure 8. Retrieve from MIB

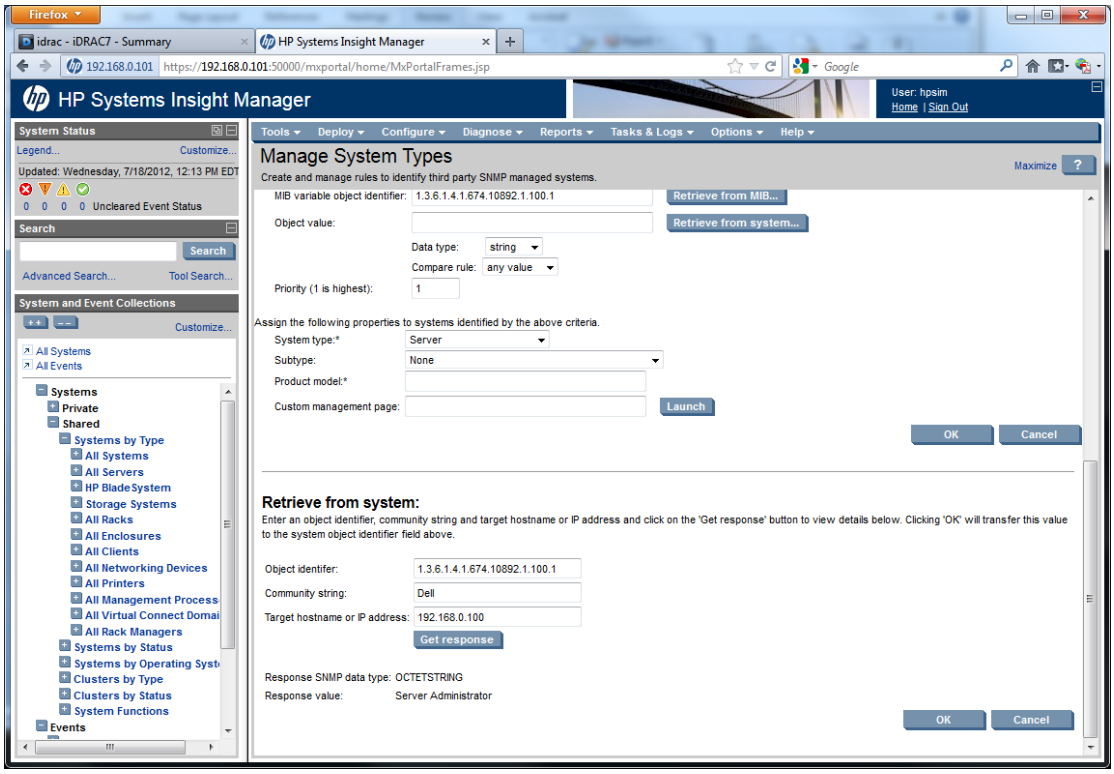


14. Click the **OK** button to accept this value and return to the **New rule** pane.
15. Click the **Object value and** click the **Retrieve from System** button. The **Retrieve from system** pane will appear below the current pane.

16. Change the **Community string** to the appropriate value and click the **Get response** button.

NOTE: The response value is “Server Administrator”.

Figure 9. Response value

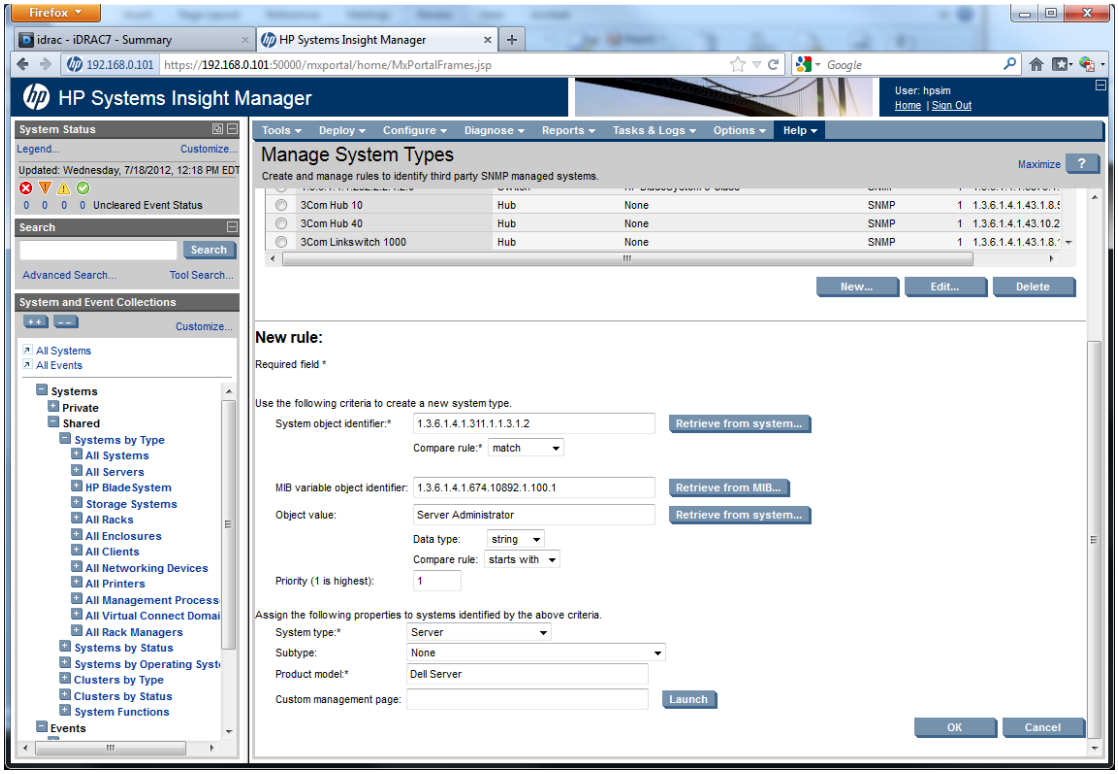


17. Click the **OK** button to accept this value and return to the **New rule** pane.
18. Choose **Compare rule** and select **starts with**.
19. Choose **Product model** enter **Dell Server**.

20. Leave the **Custom management page** field blank and click the **OK** button.

NOTE: HPSIM is already programmed to redirect users to Server Administrator for server administration on Dell servers.

Figure 10. Completed New rule



Discovering new Dell servers

Now that the new Dell Server device type has been added to the HPSIM database, HPSIM can properly discover and identify Dell PowerEdge servers running Server Administrator. The following procedure is an example of performing a manual discovery of the Dell server for demonstration purposes. In your environment, the discovery settings will likely be different.

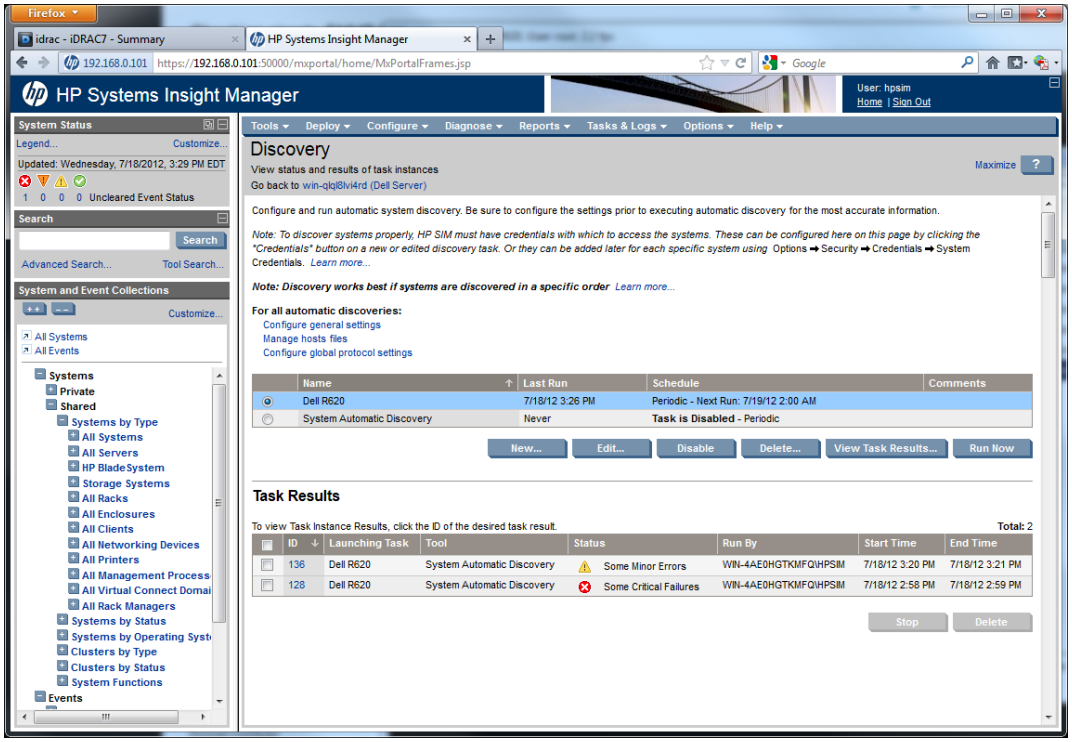
Discover the Dell server

In order to discover the Dell server, HPSIM's discovery and SNMP settings must be configured:

1. Click **Options -> Discovery**. The Discovery window is displayed.
2. Click the **New…** button.
3. Select the appropriate radio button to discover either a group of systems or a single system.
4. Give the discovery task a **name** and set the **schedule**.
5. Enter the **system name** or **IP address** of the Dell server(s).
6. To set the SNMP community, click **Credentials…**, and then click the **SNMP** tab.
7. Enter the appropriate **Read community string** and click **OK**.
8. Click **Save** to save the discovery settings, and click the **Run Now** button to initiate a discovery. The discovery task will complete with an error status. If no WMI Mapper is installed or configured, the task will complete with a status of **Some Critical Failures** as shown in Figure 11. Despite this error, SNMP trapping will still operate properly. If a WMI Mapper is installed and configured the task will complete with a status of **Some Minor Errors**, and, again, SNMP trapping will still operate properly. Both results are shown in Figure 11 and Figure 12.

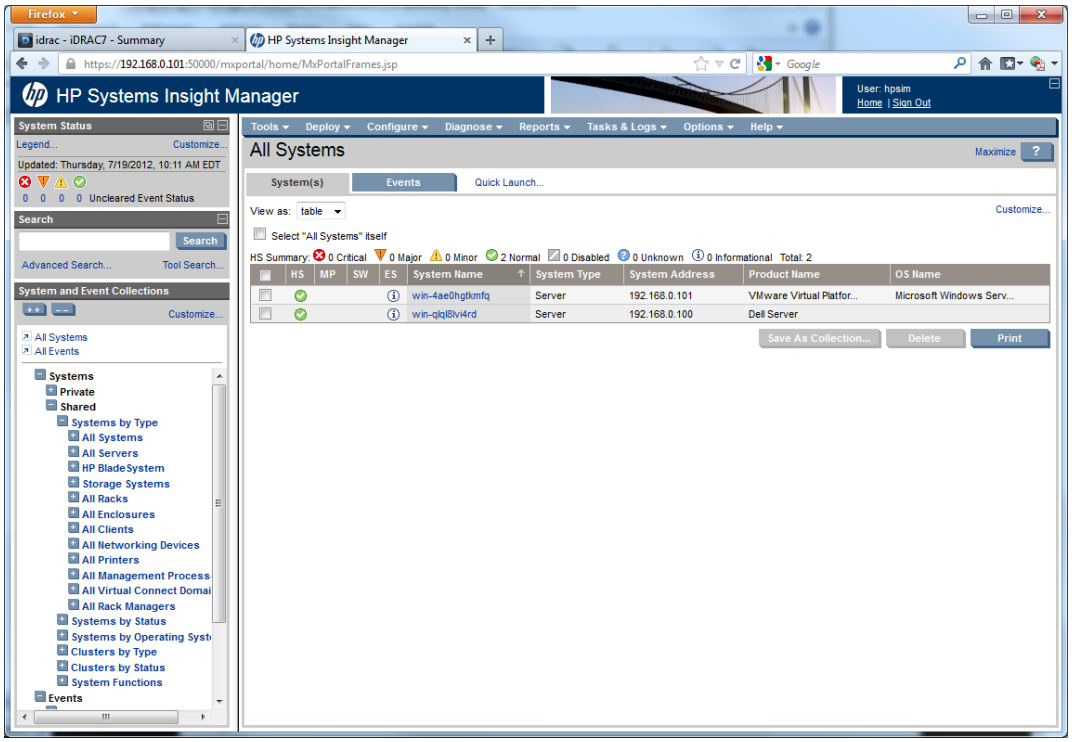
   NOTE: Installing and configuring a WMI Mapper provides detailed component information to HPSIM. HP provides a WMI Mapper on the HPSIM download website. After installation, ensure that **Sign In** credentials are supplied on the Discovery Credentials page.

Figure 11. Task results



9. In the **System and Event Collections** frame on the left-hand side of the screen, click **All Systems**. The Dell server should now be listed in the **All Systems** frame on the right.

Figure 12. Discovered Dell server



Testing events

Of all the information in the MIB files, the event traps sent by Server Administrator are of primary interest to an administrator. HPSIM can be configured to cause a notification, such as an email, to an administrator informing them of a failure. They have names like **alertCoolingDeviceNormal** with a text description, a severity, and a category.

Generating a test event

A complete end-to-end test can be performed by using OpenManage Server Administrator to change a threshold setting to place a component in a warning range. Disconnecting a power cord or removing a power supply will also generate an error event.

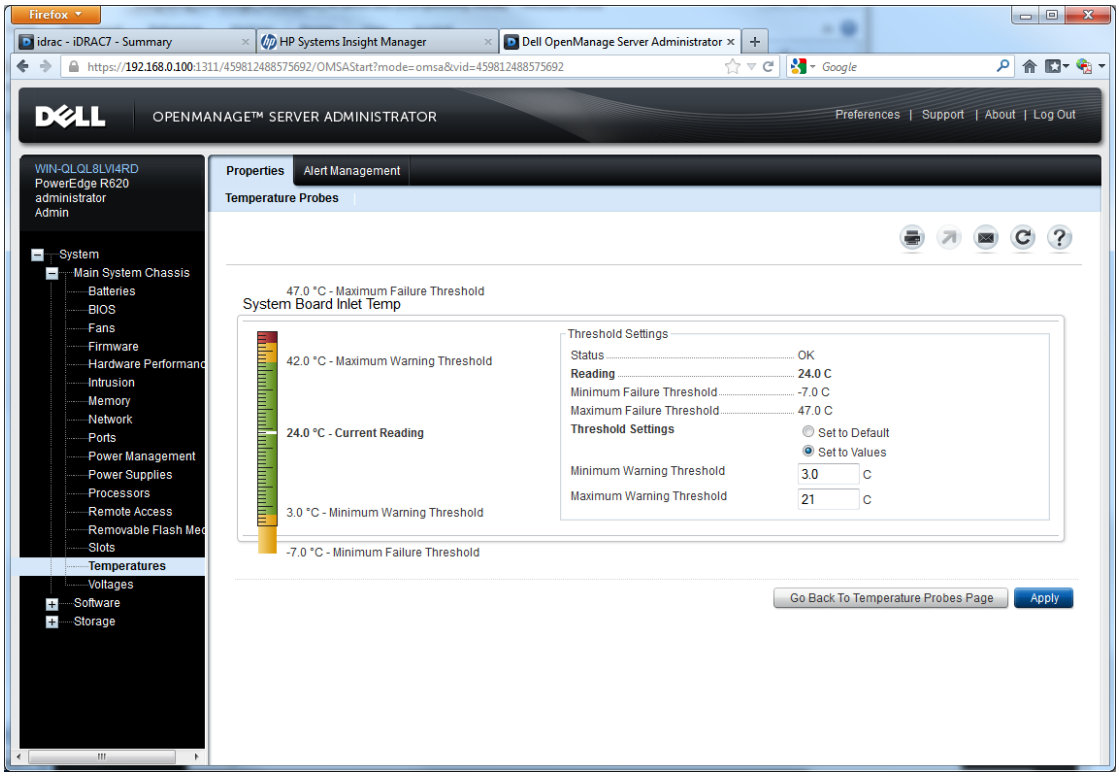
NOTE: The following procedure describes the steps necessary to generate an event remotely through Server Administrator running on a PowerEdge R620 server. Other platforms may have different temperature probes that can be manipulated in a similar fashion.

1. Log in to HP Systems Insight Manager and click on **All Systems** in the left-hand frame.
2. Click the name of the server in the **System Name** column link of the Dell server in the **All Systems** frame.
3. Click the **Tools & Links** tab.
4. Click the **Open Manage** link. Server Administrator is displayed in a new window.
5. Log in to Server Administrator using an administrative account.
6. In Server Administrator, expand **Main System Chassis** in the left-hand navigation tree.
7. Select **Temperatures**.
8. Click **System Board Inlet Temp**.

9. Note the **Current Reading**. Select the **Set to Values** button and enter a **Maximum Warning Threshold** value that is lower than the current reading.

   NOTE: For example, if the current reading is 24 degrees, set the Maximum Warning Threshold to 21 degrees.

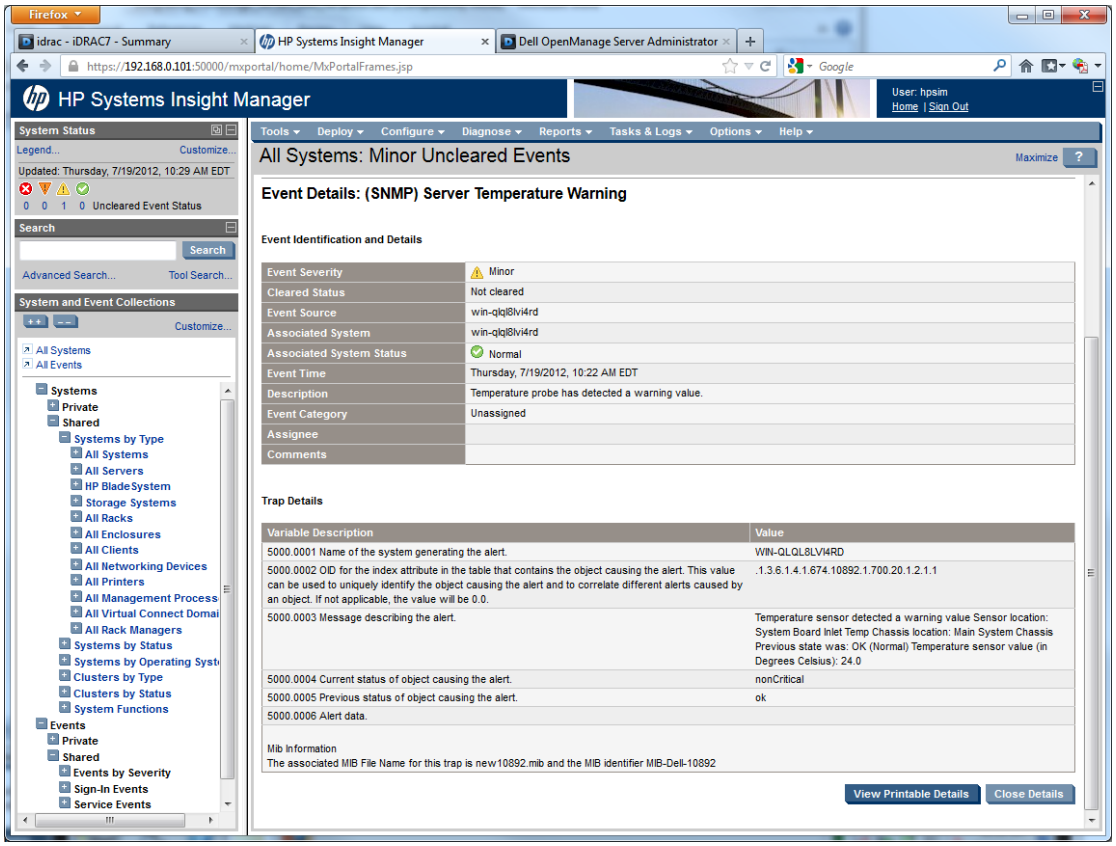
Figure 13. Server Administrator temperatures



10. Click the **Apply** button. The Current Reading is now above the Maximum Warning Threshold and a warning SNMP trap is generated by Server Administrator and forwarded to HPSIM.

11. In HPSIM, select **All Events** from the left-hand frame and note that a warning event has been generated. Clicking an event in the **Event Type** column provides more detail on the event, including a detailed description of the event from Server Administrator in the **Value** column.

Figure 14. Warning event



12. To set the temperature settings back to their defaults, return to Server Administrator. Ensure that **Set to Default** is selected and click **Apply**. Server Administrator generates a "normal" trap and forwards it to the HPSIM server.

Summary

Dell PowerEdge servers can be integrated into an environment monitored by HP Systems Insight Manager by following the steps outlined in this paper.

Dell OpenManage Essentials provides the best no-charge manageability for Dell servers, including detailed status, inventory information, and component updates. But for environments that are already monitored using HPSIM, integration would extend notification and alerts to Dell servers. The integration requires OMSA, which allows the Dell PowerEdge servers to communicate with HPSIM. By importing Dell MIBs into HPSIM, it can communicate with OMSA to provide notification if errors such as a temperature warning or power failure occur.

Limitations and caveats

It is worth mentioning that the HS (Health Status) in the All Systems query will continue to show green until HPSIM loses communication (no ping response), causing the HS to go red (critical). Also, as the PowerEdge server does not have the necessary software version agent, the MP and SW status will always be “unknown” or blank.

Appendix A

Dell MIBs

The following sections are descriptions of the MIBs contained within the DCMIB*xx* and any additional steps that are required to compile and register those MIBs in HPSIM.

Essential server MIBs

10892.mib

10892.mib provides detailed information about the systems monitored by Server Administrator instrumentation software. The 10892.mib is the primary MIB for PowerEdge systems. It compiles and registers without additional modification.

dcstorag.mib

dcstorag.mib provides detailed information about the storage hardware components and RAID configurations monitored by Server Administrator. It compiles and registers without additional modification, but generates alert redundancy warning messages that can be ignored.

M1000e and Remote Access Controller MIBs

DELL-RAC-MIB.txt

DELL-RAC-MIB.txt provides detailed information about the components monitored by the Remote Access Controllers versions 1, 2, 3, 4, and 5. It also provides information about the components monitored by the Chassis Management Controller (CMC) in an M1000e blade chassis. Dell Integrated Remote Access Controllers (iDRAC) versions 6 and 7 are monitored by iDRAC-MIB.txt. DELL-RAC-MIB.txt will not properly register due to the CATEGORY and SEVERITY properties that HPSIM does not interpret. To remedy:

1. Remove the "--#CATEGORY" lines from the MIB.
2. On line 799, change the word "NORMAL" to "INFORMATIONAL"
3. On line 850, change the word "NON-RECOVERABLE" to "CRITICAL"

The MIB will then compile and register successfully.

iDRAC-MIB.txt

iDRAC-MIB.txt provides detailed information about the components monitored by the Dell Integrated Remote Access Controllers versions 6 and 7. Remote Access Controllers versions 1, 2, 3, 4, and 5 are monitored by DELL-RAC-MIB.txt. It compiles and registers without additional modification, but generates alert redundancy warning messages if it is compiled on a system that also has DELL-RAC-MIB.txt registered. These warnings can be ignored.

Network interface MIBs

adptinfo.mib

adptinfo.mib provides information about Broadcom® Gigabit network adapters. It should be used in conjunction with baspCfg, bas pStat, and baspTrap.

baspCfg, baspStat, baspTrap.mib

baspCfg, baspStat, and baspTrap.mib collectively provide detailed information about Broadcom gigabit network adapters. They should be used in conjunction with adptinfo.

INTELLAN.mib

INTELLAN.mib provides detailed information about the Intel® PRO 100S, PRO 1000xT, PRO 100+ Dual Port, and PRO 1000F NIC adapters. It does not compile successfully due to an unexpected value on line 58 of the MIB. To remedy the issue, change the line from:

::= { enterprises 4300 1 }

to

::= { enterprises 343 }

343 is the enterprise number for Intel Corporation according to Internet Assigned Numbers Authority (iana), located at http://www.iana.org/numbers.

The MIB will then compile and register successfully, although functionality may be adversely affected by this change. It should be tested for proper functionality with your servers.

Other adapters, devices, and software

DcAsfSrv.mib

DcAsfSrv.mib specifies formatting for Dell server Platform Event Traps generated by the Baseboard Management Controller (BMC). Due to a typo on line 958 of the MIB, it will not register properly. To remedy the issue change the line from:

--#SEVERITY CRITIAL

to

--#SEVERITY CRITICAL

The MIB will then compile and register successfully.

ITassist.mib

ITassist.mib provides definitions for traps sent by the IT Assistant management application. It will not compile due to a keyword improperly placed in the MIB. To remedy this issue, move line 354 of the MIB (the word "END") to line 415. The MIB will then compile and register successfully.

Legacy MIBs

The following MIBS are from earlier versions of OpenManage and are not be needed if the current version of Server Administrator is used throughout the environment.

dcs3fru.mib

dcs3fru.mib provides detailed information about system Field Replaceable Unit (FRU) to SNMP management applications. It compiles and registers without additional modification.

dcs3rmt.mib

dcs3rmt.mib provides detailed information about the remote access components monitored by the Server Administrator Remote Access Service. It compiles and registers without additional modification.

dellcm.mib

dellcm.mib Provides detailed information about the change management data monitored by the Server Administrator Update Service. It compiles and registers without additional modification.