Monitoring Dell PowerEdge Servers With OpenManage Essentials

This Dell Technical White paper addresses the health statusing capability of OpenManage Essentials

OME Engineering team
Figures

Figure 1. Health Scoreboard ................................................................. 7
Figure 2. Drill down view of devices in critical state ........................................ 7
Figure 3. Device by Status Web Part .......................................................... 8
Figure 4. Health Status and Connection Status .............................................. 10
Figure 5. Roll-Up of Severity for a Server .................................................. 11
Figure 6. Roll-Up of Severity for the Server Group ....................................... 11
Figure 7. Configuring Status Polling ........................................................ 12
Figure 8. Alert Logs Displaying the SNMP Traps From a Managed Node .......... 13

Tables

Table 1. Dependencies for monitoring .................................................. 6
Table 2. Supported Dell PowerEdge Servers ............................................ 14
Table 3. Classification of Dell 12G Servers and the Health Status (With OMSA) .... 14
Table 4. Classification of Dell 12G Servers and the Health Status (Without OMSA) .... 16
Table 5. Agent Information Available When Devices are Discovered Using the Supported Protocol . 17
Executive Summary

OpenManage Essentials enable users to view the health status and connection status in a single centralized console.

This white paper helps users understand the functionality of statusing in OpenManage Essentials. The following topics are covered:

1) Health statusing
2) Statusing pre-requisites
3) Methods of statusing
4) Health roll-up of devices
5) Monitoring Dell PowerEdge servers through OMSA and iDRAC7

Introduction

OpenManage Essentials enables users to monitor the health status and connection status of discovered Dell servers, storage and networking devices in a single centralized console. Another significant change in OpenManage Essentials is that it supports agent-free monitoring of Dell 12G servers through iDRAC7.

How Does OpenManage Essentials Monitor the Health Status of a Device?

Monitoring/Statusing will help a user to:

1) Identify the overall health of the device
2) Define the cause - the severity of agents shows the cause for the status change.
3) Receive SNMP traps from the monitored server on occurrence of an event.

Use case: Let us take the example of OpenManage Server Administrator (OMSA) which is installed on the managed node.

The storage subsystem has components such as controllers, physical disk, virtual disk, enclosures, etc. If a component in the storage subsystem encounters a failure, the overall status of storage subsystem will change to warning or critical.

Solution: When such condition occurs in a data center where multiple systems are managed, it is difficult to consolidate the health of all the systems.

This is where the health statusing feature of OpenManage Essentials gets useful. OpenManage Essentials polls the status of all the devices in the data center at regular intervals and reflects the status in the device tree, enabling the user to view the status of all devices in a single centralized console.

Statusing Dependencies
For any managed node(s) to be successfully monitored, the following pre-requisites have to be met. Table 1 provides the dependencies for monitoring the status of devices.

### Table 1. Dependencies for monitoring

<table>
<thead>
<tr>
<th>Dependencies</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity</td>
<td>The device should be accessible (ping) from the management station (OpenManage Essentials) and vice versa.</td>
</tr>
<tr>
<td>Device agents</td>
<td>Statusing requires an agent on the monitored device to provide the data to OpenManage Essentials. For example, on Dell servers, Open Manage Server Administrator (OMSA) must be installed in order to monitor the server and retrieve its health. Likewise, a switch must have an embedded agent that supports SNMP in order to monitor its health. The agent and protocols must be installed and running. If the appropriate agents are not installed on the servers, the servers will be classified as unknown (Devices Tree).</td>
</tr>
<tr>
<td>Protocol support</td>
<td>The protocols supported in OpenManage Essentials for statusing devices are: SNMP, WMI, IPMI, EMC NaviCLI, PowerVault MD Array protocol, and WS-Man. For more information on the supported agents, see Table 5.</td>
</tr>
<tr>
<td>Discovery</td>
<td>The devices must be discovered and categorized to the respective groups, such as <strong>Servers</strong>, a <strong>Storage Device</strong> or <strong>Switches</strong> in order to get statusing data. <strong>NOTE:</strong> A device can only be monitored using the protocol in which it was discovered.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Ensure that the required services are working, and the protocol-specific ports are not blocked by the firewall. <strong>NOTE:</strong> Ensure that the SNMP protocol is open in the ESX firewall.</td>
</tr>
</tbody>
</table>

Where Can We Observe the Status Change?

The health status can be viewed in the **scoreboard** and the **Device by Status** web part.

**Scoreboard**

The scoreboard includes icons that represent the health status of all devices that are being monitored. The scoreboard is available at the top-right of the console as shown in Figure 1. It gives the overall health status of the systems, which are in critical and warning state, represented by the respective icons. The users can click the icon to drill-down and view the list of devices as shown in Figure 2.
Monitoring Dell PowerEdge Servers with OpenManage Essentials

Figure 1. Health Scoreboard

Figure 2. Drill down view of devices in critical state
Device by Status Web Part

The **Device by Status** web part displayed on the Home portal provides a pie-chart representation of the overall health status of all the devices. This chart is divided into multiple segments based on the severity of all the discovered devices as shown in Figure 3.

The user can click on any of the segments in the chart to drill-down to a more detailed view of the overall status of the corresponding devices. The detailed status view is similar to the list of devices shown in Figure 2.

![Device by Status Web Part]

**Figure 3. Device by Status Web Part**

Supported Status Types

OpenManage Essentials supports **“Health status”** and **“Connection Status.”**

Health Status

The health status reflects the overall health of the device contributed by their agent/agents (see Table 5 for software agent information). The health status can be **Normal**, **Warning**, **Critical** or **Unknown**. See Figure 4 for details on the Health status.

- Normal health status is represented by a green icon ![Green Icon](image)
  This indicates that the device is working as expected.

- Warning health status is represented by a yellow icon ![Yellow Icon](image)
  This indicates that the component is in working condition, but there is a fault. This is an indication of a possible failure in future.

- Critical health status is represented by a red icon ![Red Icon](image)
  This indicates a failure of a server component which will make the device status critical. Immediate attention is required.
Monitoring Dell PowerEdge Servers with OpenManage Essentials

- Unknown Health status is represented by the question mark icon. This indicates that the health status of the device cannot be determined.

Use Case 1

This use case gives an example of ‘Health Status.’

‘System A’, 'System B'…. System G'…. till ‘System M’ have been discovered in OpenManage Essentials. The storage management of ‘System G’ changed from Normal to Critical as one of the physical disks is offline.

Solution

In OpenManage Essentials, all the devices are polled at regular intervals to get the status and the status is reflected in the device tree. After polling is completed, the health status of the ‘System G’ turns Critical.

The user can view the health status of ‘System G’ and drill-down further to see the root cause of the issue by logging in to the Server Administrator or the web console. Perform one of the following steps in the OpenManage Essentials console:

- Right-click ‘System G’ and select Application launch→ Server Administrator and log in to OMSA/web console
- Click the Server Administrator hyperlink provided under Software Agents Information in the Details view for ‘System G’.
- Right-click ‘System G’ and select Application launch→ Open Remote Desktop. Provide valid credentials to login.

Connection Status

The connection status reflects the power status of the monitored device. The connection status can either be ‘ON’ or ‘OFF’. The connection status is ‘OFF’ when either the network connectivity is lost or the system is shut down. For more information, see Figure 4.

Use Case 2

This use case gives an example of ‘Connection status.’

‘System A’, ‘System B’…. ‘System G’…. till ‘System M’ have been discovered in OpenManage Essentials. ‘System M’ shuts down as a result of a thermal event (overheating).

Solution

In OpenManage Essentials, all the devices are polled at regular intervals to get the status and the status is reflected in the device tree. On the next poll the monitoring solution is unable to access ‘System M.’ As a result the connection status of ‘System M’ is changed to ‘OFF’. The user can determine the cause by reviewing the alert logs or physically checking the device. The user can also power on the system manually or by creating a power management task.
NOTE: When a system is discovered using SNMP/WMI protocol, the connection status is displayed as ‘OFF’ if the system is powered off. But when the IPMI/SNMP or WSMAN protocol is used to discover a Remote access controller card (RAC), the connection status is displayed as On even if the system is turned off and just the power cable is connected. This is because of the IPMI/SNMP or WSMAN protocol does not require an operating system to communicate with the management station when interacting with the RAC.

**Figure 4. Health Status and Connection Status**

Health Roll-Up

The overall health status of a discovered device is based on the most critical severity of the agents on that device. For more information, see Figure 5.

Example: If the severity of the Server Administrator agent is critical and that of the DRAC agent is normal, then the overall health of the server would be **Critical**.

The same holds good for the device group as well. For more information, see Figure 6.

Example: If server 1 is in normal state and server 2 is in critical state, then the overall health of the server group would roll-up to **Critical**.
Figure 5. Roll-Up of Severity for a Server

Figure 6. Roll-Up of Severity for the Server Group
Method of Determining Health Status

The **Health Status** of a device is reflected in the device tree as well as in the right pane on the **Device Summary** page. For more information, see Figure 4.

The **Connection Status** of a device is reflected in the right pane on the **Device Summary** page. For more information, see Figure 2.

The health status can be determined by “Polling” and/or “On-demand” (on receiving a SNMP trap).

**Polling**

Polling refers to an operation where a managed node is checked at regular intervals, with pre-defined settings.

The polling cycle retrieves the health and connection status for each discovered device and the status is updated in the device tree.

By default, polling is enabled once every hour. This setting can be configured as required. The polling settings can be configured at **Manage** → **Discovery and Inventory** → **Configuration** → **Status configuration**.

![Figure 7. Configuring Status Polling](image)

The user can start status polling at any time using one of the following methods:

- Under **Manage** → **All Devices**, right-click a discovered device and then select **Refresh status**.
- Under **Manage** → **Discovery and Inventory** → **Discovery Ranges**, right-click an IP address and then select **Perform Status Polling Now**.
On-Demand

On-demand refers to an operation where a managed node is checked for health status by OpenManage Essentials when any SNMP trap is received from the managed node.

To receive the trap in the OpenManage Essentials console, the IP of the OpenManage Essentials system (management station) has to be configured as the trap destination address in the SNMP service of the managed node. Once the SNMP trap is received in the OpenManage Essentials console, the status of the device is updated if there is a change in the status.

An SNMP trap is received from the managed node on occurrence of an event (for example, issues/failures of any server component). These traps can be viewed for a specific device by selecting that device at: Manage → Devices → <Device> → Alerts, or the user can view the alerts for all the devices at: Manage → Alerts → Alert Logs. These alerts show the severity of the trap, the managed node's IP/hostname generating it, brief description of the alert (or problem of the component) etc. For more information, see Figure 8.

NOTE: Alerts provide an immediate notification after an event occurs on a device. OpenManage Essentials also uses this notification to trigger a global health poll to the device. A critical SNMP alert, however, does not necessarily mean that the device is in a critical state.

Figure 8. Alert Logs Displaying the SNMP Traps From a Managed Node
Monitoring Dell PowerEdge Servers Through OMSA

Supported Dell Servers

The supported generations of servers are listed in the following table

<table>
<thead>
<tr>
<th>Generation of server</th>
<th>Representation</th>
<th>Examples of generation of servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 (9G)</td>
<td>x9xx</td>
<td>PE2900, PE6950 etc.</td>
</tr>
<tr>
<td>10 (10G)</td>
<td>yy0x</td>
<td>M600, R300, T105 etc.</td>
</tr>
<tr>
<td>11 (11G)</td>
<td>yy1x</td>
<td>M610, R310, T110 etc.</td>
</tr>
<tr>
<td>12 (12G)</td>
<td>yy2x</td>
<td>M620, R620, T620 etc.</td>
</tr>
</tbody>
</table>

NOTE: ‘x’ denotes numbers; ‘y’ denotes alphabets (such as M, R, or T). M = Modular; R = Rack; T = Tower.

The supported OMSA versions are from 5.5 to 7.3.

Status Roll-Up With OMSA

Whenever a PowerEdge server (from 9G - 11G) with OMSA installed is discovered using the supported protocol, then the server is classified under the Servers groups. The overall health status of this server will be contributed only by the severity of Dell OpenManage Server Administrator (OMSA).

The overall health status of a Dell 12th Generation server (12G) will be determined by combining OMSA and iDRAC7 agent status. This means that the overall health roll-up involves the most critical severity of OMSA and iDRAC7. For more information, see the Health Roll-Up section. The following table provides more information on the protocols and the agents.

<table>
<thead>
<tr>
<th>S. No</th>
<th>Protocol Combination for Server (With OMSA) + RAC</th>
<th>Device Tree Classification</th>
<th>Health Status</th>
<th>Agents contributing to the overall Health Status (The worst case status of OMSA or RAC will be reflected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SNMP</td>
<td>Server</td>
<td>Known</td>
<td>OMSA and RAC</td>
</tr>
<tr>
<td>2</td>
<td>SNMP+SNMP/IPMI/WSMAN</td>
<td>Server and RAC</td>
<td>Known</td>
<td>OMSA and RAC</td>
</tr>
<tr>
<td>3</td>
<td>WMI (for Windows Only)</td>
<td>Server</td>
<td>Known</td>
<td>OMSA</td>
</tr>
</tbody>
</table>
The following is the description of the titles of the columns in Table 3:

**Protocol combination**: The various protocols used for discovering the device. For the specified protocol combination, the server IP address and RAC IP address must be provided during discovery in order to get a known health status.

When the WMI protocol is used for discovery, the server will be classified under the **Servers** group and no RAC entry is available.

**Device tree Classification**: The classification of the server in the device tree when discovered using the corresponding protocols. The server is classified under the **Servers** group based on the protocols used.

**Health Status**: The health status of the server as identified through OMSA.

**Agents Contributing to the Overall Health Status**: The only 2 agents contributing to the overall Health status are *Dell OpenManage Server Administrator (OMSA)* and/or *Remote Access Controller (RAC)*. Based on the protocols used and the agents available during discovery, the agents will be populated under *Software Agent Information* on the right pane for the device.

**Alert Management**

The SNMP alerts received from servers or devices will be shown under the alerts tab of the respective devices. As described in the Method of Determining Health Status section, the status of the device will be polled when an SNMP trap is received.

But in case of Dell 12G servers, the traps generated from iDRAC7 will be shown under alerts tab of RAC as well as under the correlated server in the device tree. Under the server, the traps will be received with the host name of the server.

**NOTE**: When the server and iDRAC7 are discovered using the WMI protocol, the iDRAC7 will not be classified as there is no relevant protocol to discover it. Hence, only the server will be classified under the **Servers** group. Hence a trap generated from iDRAC7 will not be displayed in the **Alerts** tab of the server.

**Health Status feature helps in diagnostics**

For an Administrator, the warning and critical status of a device is a cause for concern. If the device status is **Warning** or **Critical**, the following can be performed:

1. Select the device which is in warning/critical status in the device tree.
2. On the right pane, scroll down to the **Software Agent Information** table.

3. Identify the agent which is in warning/critical state and click the link provided for the agents or right-click the device and launch application.

4. Once the application is launched, identify the component which is in warning/critical state and perform the required remedial actions.

**Monitoring of Dell PowerEdge Servers Through iDRAC7 (Agent-Free Monitoring)**

**Supported Dell Servers**

Dell PowerEdge 12th Generation servers support agent-free monitoring through iDRAC7 using WSMAN protocol. Other PowerEdge servers (8G-11G) will be classified as ‘unknown’ if OMSA is not installed. In Dell 12G servers, even if OMSA is not installed, the overall health status of the server can be determined through iDRAC7.

**Status Roll-Up Without OMSA**

1. For a PowerEdge server (from 9G - 11G) to be classified as Server and to display appropriate health status, OMSA has to be installed.

2. For a Dell 12G server which does not have OMSA installed, the overall Health status will be based on the Integrated Dell Remote Access Controller 7 (iDRAC7) status. For more information, see the Health Roll-Up section. The following table provides more information on the protocols and the agents.

**Table 4. Classification of Dell Servers and the Health Status (Without OMSA)**

<table>
<thead>
<tr>
<th>S. No</th>
<th>Protocol combination Server(without OMSA)+RAC</th>
<th>Device tree Classification</th>
<th>Health Status</th>
<th>Agents contributing to the overall Health Status (iDRAC 7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SNMP</td>
<td>Unknown</td>
<td>Unknown</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>SNMP+SNMP/IPMI/WSMAN</td>
<td>RAC</td>
<td>Known</td>
<td>RAC</td>
</tr>
<tr>
<td>3</td>
<td>WMI (for Windows Only)</td>
<td>Server</td>
<td>Unknown</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>WMI+SNMP/IPMI/WSMAN</td>
<td>Server+RAC</td>
<td>Known</td>
<td>RAC</td>
</tr>
<tr>
<td>5</td>
<td>SSH (for linux only)</td>
<td>Server</td>
<td>Unknown</td>
<td>NA</td>
</tr>
<tr>
<td>6</td>
<td>SSH+SNMP/IPMI/WSMAN</td>
<td>Server+RAC</td>
<td>Known</td>
<td>RAC</td>
</tr>
<tr>
<td>7</td>
<td>Any protocol + SNMP/IPMI/WSMAN</td>
<td>RAC</td>
<td>Known</td>
<td>RAC</td>
</tr>
</tbody>
</table>
Alert Management

In case of Dell 12G servers, the traps generated from iDRAC7 will be shown under the Alerts tab of iDRAC as well as the correlated server, where the device name in the trap will show the hostname of the server.

If the server is classified under Unknown, then no alerts are displayed for the server.

Agent Information

The following table describes the agent(s) information which is populated when devices are discovered with the specified protocols along with their description.

Table 5. Agent Information Available When Devices are Discovered Using the Supported Protocol

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Software agent(s) information available when a device is discovered using the specified protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>• Server Administrator&lt;br&gt;• Server Administrator (Storage Management)&lt;br&gt;• Inventory Collector&lt;br&gt;• DRAC</td>
<td>Server Administrator: Management Software for Dell Systems.&lt;br&gt;Server Administrator (Storage Management): Configuration and Monitoring of disk storage devices.&lt;br&gt;Inventory Collector: Provides information about devices running on the local system.&lt;br&gt;DRAC/iDRAC: This system component provides a complete set of remote management functions for Dell PowerEdge servers.</td>
</tr>
<tr>
<td>WMI with OMSA</td>
<td>• Server Administrator&lt;br&gt;• Inventory Collector&lt;br&gt;• DRAC&lt;br&gt;• Hardware agent</td>
<td>Server Administrator: Management Software for Dell Systems.&lt;br&gt;Inventory Collector: Provides information about devices running on the local system.&lt;br&gt;DRAC/iDRAC: This system component provides a complete set of remote management functions for Dell PowerEdge servers.&lt;br&gt;Hardware Agent: Microsoft Windows Hardware agent</td>
</tr>
</tbody>
</table>
Monitoring Dell PowerEdge Servers with OpenManage Essentials

| WMI without OMSA | • Windows Management  
|                  | • Instrumentation  
|                  | Provides a common interface and object model to access management information about the operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start |
| IPMI | • IPMI  
|      | IPMI Management software  
| WSMAN | • Server Administrator  
|      | • VMware ESXi OS build  
|      | Embedded ESX Agent  
| EQL | • EqualLogic SNMP agent  
|      | EqualLogic SNMP agent  
| EMC | • Navisphere Array Agent  
|      | EMC Navisphere Array Agent Software  
| MD Array | • MD Storage Array  
|      | Monitors MD Storage Devices  
| Switch | • Power Connect xxxx  
|      | • Force10 S, C and E series  
|      | Ethernet Switch  
|      | Dell Force10 SNMP Agent  
| Dell Compellent | • SC8000  
|      | Dell Compellent Storage Center  

Conclusion

OpenManage Essentials version 1.2 allows users to monitor the health status and connection status of discovered Dell servers, storage and network devices. OpenManage Essentials also provides agent (OMSA) and agent-free (without OMSA) monitoring.