Managing Dell PowerEdge Server Alerts

Using Dell OpenManage Server Administrator

Eighth-generation Dell™ PowerEdge™ servers are enabled by Dell OpenManage™ systems management tools to provide a set of alerting mechanisms that proactively notify system administrators of abnormalities before failures occur. This article introduces and explains the three different alerting mechanisms provided by Dell OpenManage Server Administrator.

BY HAIHONG ZHUO, MICHAEL O’HARA, AND JIANWEN YIN, PH.D.

Enterprise servers that run mission-critical applications should be designed to run error-free to help maximize performance and minimize downtime. It is critical that system administrators be notified of any system abnormalities before hardware failures occur if feasible—otherwise, as soon as possible. Eighth-generation Dell servers such as the PowerEdge 1850, PowerEdge 2800, and PowerEdge 2850 help achieve this goal by providing a set of three different alerting mechanisms that can be viewed or configured through the Dell OpenManage systems management suite.

Dell PowerEdge servers managed through Dell OpenManage tools can be configured to generate and send Simple Network Management Protocol (SNMP) traps, trigger local alert actions (such as beeping the speakers on a system that needs attention), or generate and send Platform Event Traps (PETs) when they detect system error events or status changes. Configuration of these alerting mechanisms is done using Dell OpenManage Server Administrator (OMSA), a software tool that allows administrators to manage individual servers locally or remotely using a graphical user interface (GUI), or locally using the OMSA command-line interface (CLI).¹

Local alert actions

Dell PowerEdge servers that are managed by OMSA can be configured to trigger certain local actions on the occurrence of specified events—for instance, when a system’s temperature probe or voltage probe detects a warning or failure. OMSA alerts the administrator by beeping the speaker on the affected system, popping up an alert message on the system, invoking an application on the system, or broadcasting an alert message through a messenger service to other systems that are on the same network and have drives mapped to the affected system.

The OMSA Web-based GUI lists all system events for which local alert actions can be configured (see Figure 1). Administrators can also view a list of events

¹For online documentation that provides detailed instructions on how to use Dell OpenManage Server Administrator, visit docs.us.dell.com/docs/software/svradmin/index.htm.
related to a category of monitored components—for example, temperature sensors—by selecting a component category from the left navigation bar of the GUI (see Figure 2).

Local alert action configurations can also be viewed and managed using the OMSA CLI. Administrators can display a list of events for which local alert actions can be configured using the command omreport system alertaction. The CLI provides an online help system, which can be displayed by typing -? after any command.

In today’s enterprises, IT environments are becoming ever more complicated. As the number of computing systems that administrators must manage continues to grow, remote management becomes more popular. Locally managed alert actions may be insufficient in circumstances where administrators are not working in close physical proximity to the systems under management—for example, they cannot hear a system’s speakers beep or see an alert message on a system’s monitor. Remote alerting mechanisms are therefore an indispensable feature of a total systems management software package. OMSA provides two remote alerting methods to meet this need: SNMP traps and PETs.

Remote alerts using SNMP traps

When properly configured, Dell PowerEdge servers equipped with OMSA can generate and send SNMP traps for system events such as component failure or status change. While alerting using local alert actions is configured strictly by the category of the monitored components, alerting using SNMP traps in OMSA provides more flexibility and granularity.

Systems managed using OMSA can be configured to generate SNMP traps for a status change of the system, for a category of monitored components such as temperature sensors, or even for an individual component such as the temperature sensor for a specific CPU. Additionally, systems can be configured to generate SNMP traps for different severity levels of a system event: informational, warning, or critical.

By default, the generation of all SNMP traps is enabled. SNMP traps can be enabled or disabled by system, by category of component, by individual component, and by severity level. In the OMSA GUI, administrators can indicate the severity level for which they would like to enable alerts for the system. Administrators can select from a list of all categories of monitored components for a system, and then also indicate the severity level for which they would like to enable alerts for each category. Additionally, after enabling a category of components, the administrator can select components to enable from a list of individual components within that category if they do not want to enable every component in the category (see Figure 3).
SNMP trap destinations and the SNMP community to which the traps should be sent are configured in the server’s operating system (OS). SNMP trap configuration can also be viewed and managed using the CLI. For example, executing the command `omconfig system events type=fans source=snmptraps severity=warning` tells the server not to generate SNMP traps for events with an informational severity level for fans.

Remote alerts using PETs

In addition to local alert actions and SNMP traps, eighth-generation Dell PowerEdge servers support generating and sending alerts at the hardware and firmware levels. These servers are equipped with a microcontroller called the baseboard management controller (BMC) that is compliant with the Intelligent Platform Management Interface (IPMI) 1.5 specification. The BMC provides the intelligence behind the autonomous monitoring and recovery features at the hardware and firmware levels.

When an event occurs on the platform, an event message is generated and logged in the BMC hardware system event log (SEL). The BMC checks whether the event meets the Platform Event Filter (PEF) criteria configured by the administrator through OMSA. If so, the BMC generates an SNMP PET and sends the PET to the destination or destinations designated by the administrator. Once established, this process does not require the OS or OMSA systems management software and allows alerts to be sent even when the system is powered down or unable to boot to the OS.

For platform events to be filtered properly and PETs to be generated and sent as desired, administrators must first perform certain configuration steps. OMSA provides an interface that allows administrators to configure when PET alerts should be generated and sent and where they should be sent.

Administrators must first configure PEFs on the BMC to indicate which actions the BMC should take when a filter is triggered. Figure 4 shows a list of such event filters, and Figure 5 illustrates how actions for each event filter can be configured. The Reboot Action for platform events should be configured with caution because the platform events can cause the server to reboot if the specified trigger event occurs. Reboots initiated by platform events occur without the knowledge of the OS—hence, the OS does not have an opportunity to perform a graceful shutdown first. Note: For PET alerts to be generated and sent, the Enable box in the Generate Alert section of the GUI should be selected, as shown in Figure 5.

The PET alerting feature of the BMC can be globally enabled or disabled by selecting and deselecting the Enable Platform Event Filter box in the Platform Event Filters Configuration section of the GUI. This setting does not affect any of the platform event–triggered shutdown actions.

For PETs to be transmitted as desired, SNMP trap destinations and the SNMP community must also be configured. Administrators should click “Configure Destinations” on the Platform Events screen, shown in Figure 4, to view the Platform Event Alert Destinations screen and configure the SNMP community. Clicking on a destination number in the destination list displays the Set Platform Events Alert Destination screen. On this screen, administrators can
check the Enable Destination box and enter the IP address of the destination system to which the PET alerts should be sent.

Finally, the network interface card (NIC) of the BMC should be enabled and correctly configured so that PET alerts can be sent. Administrators should select System > Main System Chassis > BMC on the left navigation bar of the OMSA GUI, and select Configuration > LAN. Administrators should make sure that the Enable IPMI Over LAN box in the NIC Configuration section of the GUI is selected, and that the NIC has the correct IP address assigned to it—either by using Dynamic Host Configuration Protocol (DHCP) or a static IP address.

PET configuration can also be viewed and managed using CLI commands. Detailed instructions can be found in the OMSA online documentation.

### SNMP traps versus PET alerts

The destination system for SNMP traps and PET alerts must have an SNMP manager program installed, such as Dell OpenManage IT Assistant (ITA), which receives, recognizes, filters, and acts upon SNMP traps and PET alerts. PET alerts are, in fact, SNMP traps with specified trap fields defined in the IPMI Platform Event Trap format.

If both SNMP traps and PET alerts are configured for the same type of component and event (for example, when a temperature sensor detects a warning state), an SNMP trap is generated and sent by OMSA when the event occurs, while a PET alert is generated and sent by the affected system’s BMC. If destinations for both of the alerts are set to the same management station, which has ITA installed, both the SNMP trap and the PET alert will reach the management station and be recognized, as shown in Figure 6. The SNMP trap (the first line item in Figure 6) and the PET alert (the second line item in Figure 6) have different values for the host name.

The SNMP trap uses the OS host name as its host name because the trap is generated and sent by OMSA and the OS, while the PET alert uses the BMC host name because the PET is generated and sent by the BMC. These two alerts also display different values in the description.

### Maximized uptime and performance through alerting

Alerting mechanisms provided by OMSA allow administrators to be notified of system events, or status changes of system components or of the system itself. Different alerting mechanisms—at the local, remote, or hardware and firmware levels—provide administrators with options and flexibility regarding how they can be warned of system abnormalities. The sooner and more accurately administrators are notified of potential and actual system failures, the more time they have to discover the root cause of a given problem and take appropriate action to help maintain continuous system uptime.

Haihong Zhuo is a software engineer consultant working in the System Management Instrumentation team in the Dell Enterprise Software Development Group. She participated in the development of ITA 6.x. Haihong has an M.S. in Computer Engineering from The University of Texas at Austin and a B.S. in Electrical Engineering from Tsinghua University in China.

Michael O’Hara is a software engineer senior consultant on the Managed Node Framework Development team in the Dell Product Group. He focuses on OMSA user interfaces, with particular emphasis on the CLI. Michael has a BSc. in Mathematics from the University of Warwick in England.

Jianwen Yin, Ph.D., is a software engineer senior consultant on the Managed Node Framework Development team in the Dell Product Group. His major focus is on OMSA and systems management. Jianwen has a Ph.D. in Computer Science from Texas A&M University.

### SNMP traps can be enabled or disabled by system, by category of component, by individual component, and by severity level.

---

**FOR MORE INFORMATION**

- **IPMI 1.5 overview and specification:**
  - [www.intel.com/design/servers/ipmi/index.htm](http://www.intel.com/design/servers/ipmi/index.htm)

- **IPMI PET 1.0 specification:**
  - “IPMI Platform Event Trap Format Specification v1.0” by Intel, Hewlett-Packard, NEC, and Dell, [ftp://download.intel.com/design/servers/ipmi/pet100.pdf](ftp://download.intel.com/design/servers/ipmi/pet100.pdf)

- **OMSA online documentation:**
  - [docs.us.dell.com/docs/software/swadmin/index.htm](http://docs.us.dell.com/docs/software/swadmin/index.htm)