Best practices for Alert Management using Dell EMC OpenManage Enterprise Power Manager

Abstract

This technical white paper describes the process of configuring and following some best practices of using the Alerts features in Dell EMC OpenManage Enterprise Power Manager version 1.0 to manage the data center better by leveraging the power monitoring and management capabilities.

September 2019

Revisions

Date	Description
September 2019	Initial Release for Power Manager 1.0.

Acknowledgements

This paper was produced by the following:

Author:

Anand J, Test Engineer 2, Enterprise Software Validation

Support:

Mahendran P, Test Senior Engineer, Enterprise Software Validation

Shruthi Ravoor, Technical Content Developer 2, BDC - InfoDev

Table of contents

Executive summary

This technical whitepaper provides an overview about configuring and following some best practices of using the Alerts features in Dell EMC OpenManage Enterprise Power Manager version 1.0. It contains Open Manage Enterprise existing capabilities with respect to alerts and how to leverage it for Power Manager events and following alert actions.

- Alert Email Action
- Alert Trap Forward Action
- Alert Forward Action for Syslog Watcher
- Alert Ignore Action

1 Introduction

This white paper illustrates several examples and provides complete steps on how to gain maximum benefit of Alerts feature. Also, the paper describes the alert actions in OpenManage Enterprise and provides information on how IT administrator can leverage them.

1.1 Power Manager Events

- Threshold alerts
  - Critical Alert for Power—If the critical power threshold is set on a device or group and the threshold is exceeded, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Warning Alert for Power—If the warning power threshold is set on a device or group and the threshold is exceeded, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Power Return to Normal—If the critical or warning power threshold is set on a device or group and the power return to normal, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Critical Alert for Thermal—If the critical thermal threshold is set on a device or group and if this threshold is exceeded, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Warning Alert for Thermal—If the warning thermal threshold is set on a device or group and if this threshold is exceeded, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Thermal Return to Normal—If the critical or warning thermal threshold is set on a device or group and if the thermal value exceeds the threshold and returns to normal, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
- Group membership
  - Warning Alert for Group Membership Changes—If the power cap policy is set on a group and if the group membership changes by either adding or removing devices from that group, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
- Group Power policy
  - Critical Alert for Power Policy - If the power cap policy is set on a group and present power value exceeds the power cap, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.
  - Power Return to Normal—If the power cap policy is set on a group and power value exceeds the power cap later returns to normal, then there is an internal notification or alert generated in OpenManage Enterprise in Alert Log.

2 Alert Definition

Alert definition is a meta data of alerts, defined by Open Manage Enterprise. You can view alerts that are generated for errors or informational purposes. An Error and Event messages have the following information:

- Message ID—Messages are classified based on components such as threshold violation, power policy violation, and group membership changes.
- Message—The actual cause of an event. Events are triggered for information purpose only, or when there is an error in performing tasks.
- Category—Class to which the error message belongs to. For information about categories, see the Event and Error Message Reference Guide for Dell EMC PowerEdge Servers available on the support site.
- Recommended Action—Resolution to the error by using GUI, RACADM, or WS-Man commands.
- Detailed Description—More information about an issue for easy and fast resolution.
- Severity—Relative impact of the issue such as critical or warning or information

Any alerts generated internally or coming from device, is compared with alert definition and then it is displayed with respective severity and message ID. In case the alert is not defined it is displayed as unknown.

3 Alert Filter

To filter only Power Manager alerts, you can filter by selection of category such as **System Health** and sub-category as **Metric** or **Power Configuration** in Alert Log page.

Metrics - Threshold Violation Alerts.

Power Configuration – Group membership changes and power policy violation alerts.

4 Alert Forward Prerequisite Settings

Following are the prerequisites for forwarding Power Manager alerts:

- Configure the target IP address, where Power Manager alerts need to be forwarded and community string in Open Manage console in below path.
  - Application Settings→Alerts→SNMP Configuration
- Configure trap forward format in below path.
  - Application Settings→Console Preference→Trap Froward Format→Normalized (Valid for all Formats)

Note: To forward Power Manager alerts from Console1 → Console2, trap forward format should be Normalized (Valid for all Format).

Note: In this case you have alerts forwarded from Console1 → Console2 (In SNMP Format) and later this needs to be forwarded from Console2 → Console3 (In Original Format), trap forward format should be Original Format (Valid for SNMP traps only).

---

5 Alert Trap Forward Action

- OME receives alerts from various SNMP agents and Platform Event Traps (PETs) configured on the network. These traps may be required by another OME instance or other Network Management Systems (NMS).
- The system administrator can set the rules to define which traps will be forwarded based on the traps severity, traps categories, and devices or device groups.
- When there are multiple instances of OME configured, where each instance is monitoring a subset of devices in a data center, a system administrator may want to consolidate the alerts from multiple OME instances for alert management. Else, the system administrator should individually check all the OME servers for monitoring the devices.
- Instead, a system administrator can configure a master OME server to which all the other OME instances will forward the alerts or traps. Instances also provide the system administrator a consolidated view of all the alerts and enable the system administrator to manage the data center from a single master OME server.
- An SNMP trap carries data in form of trap variable, commonly known as trap varbinds, which provides enough information about the event, based on which, an administrator can take corrective measures.

5.1 Creating an Alert Trap Forward Action

1. Click create alert policy as shown in figure1. The Alert Policy Wizard is displayed in figure 2. In the Alert Policy Wizard provide a name and description.

Figure 1 Create policy

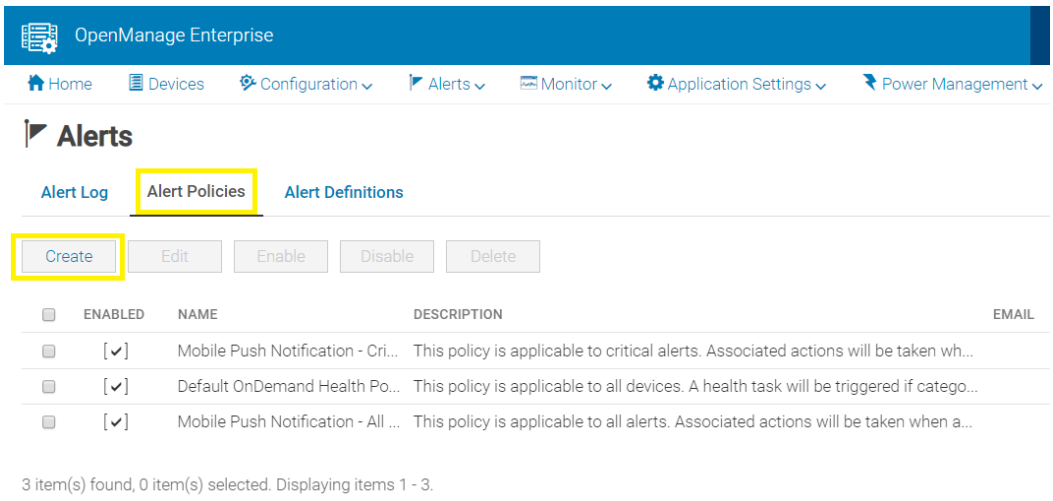
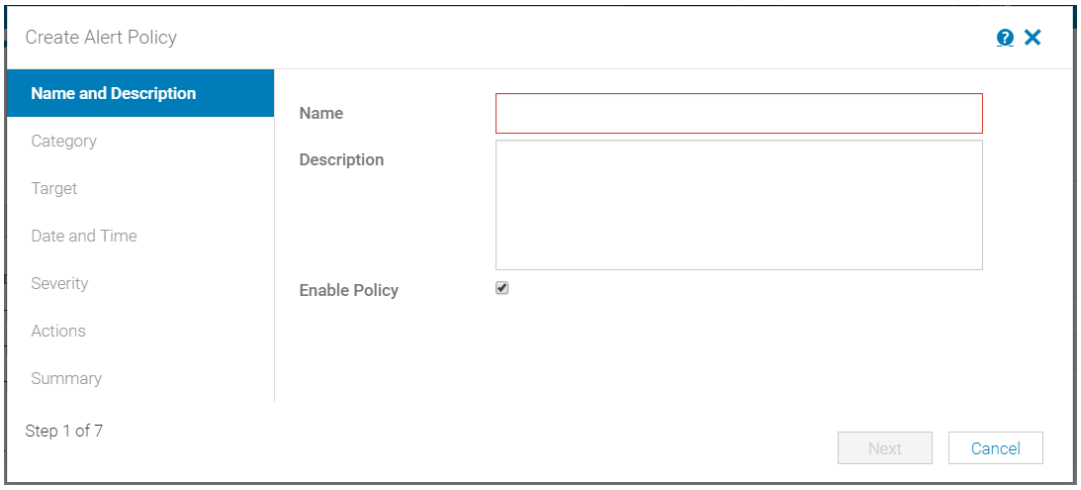


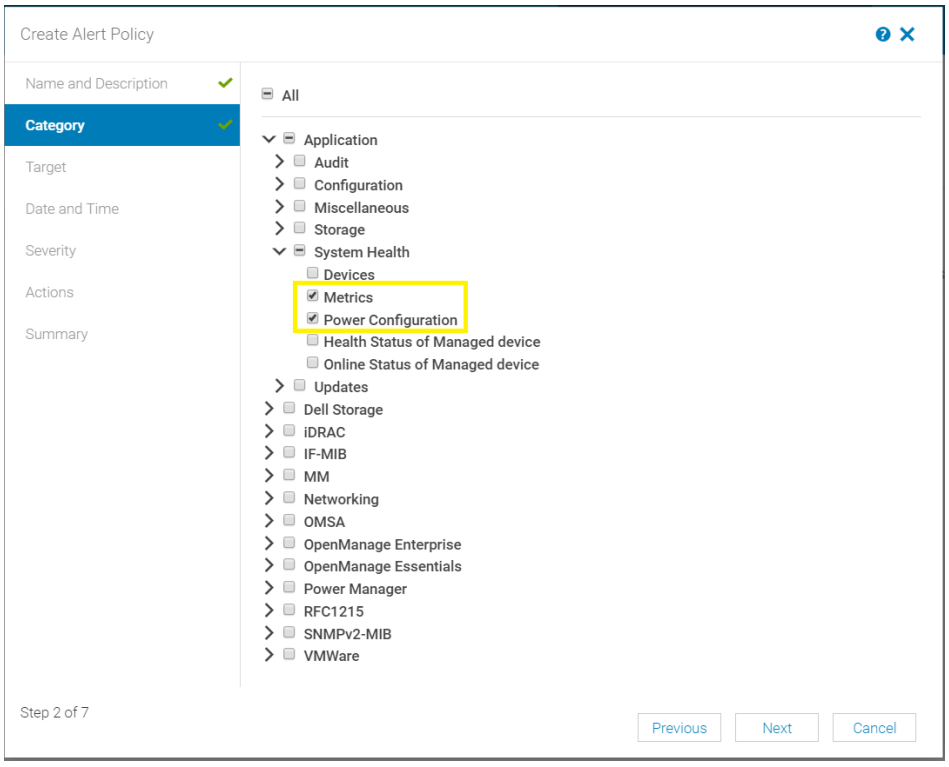
Figure 2 Name and Description



2. Choose the below mentioned categories for Power Manager related alerts, as shown in Figure 3.

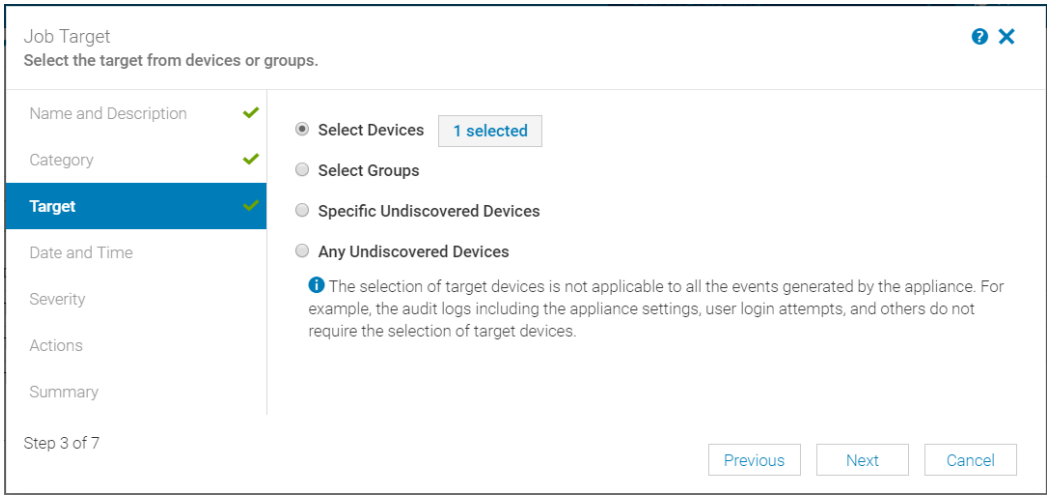
Note: Metrics→ Threshold violation, Power configuration→ Power policy violation

Figure 3 Category Association



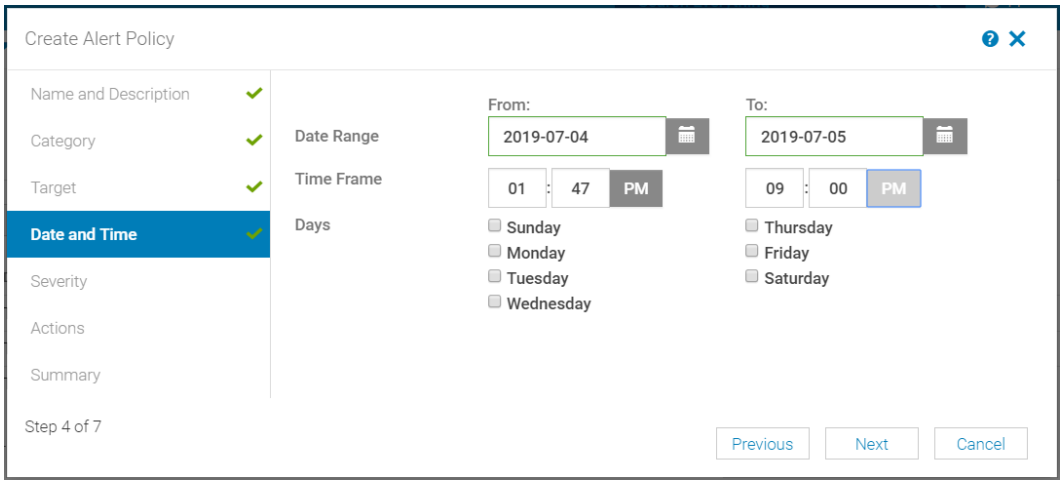
3. A specific devices or groups that needs to be monitored can only be selected through the device tree.

Figure 4 Device/Device Group Association



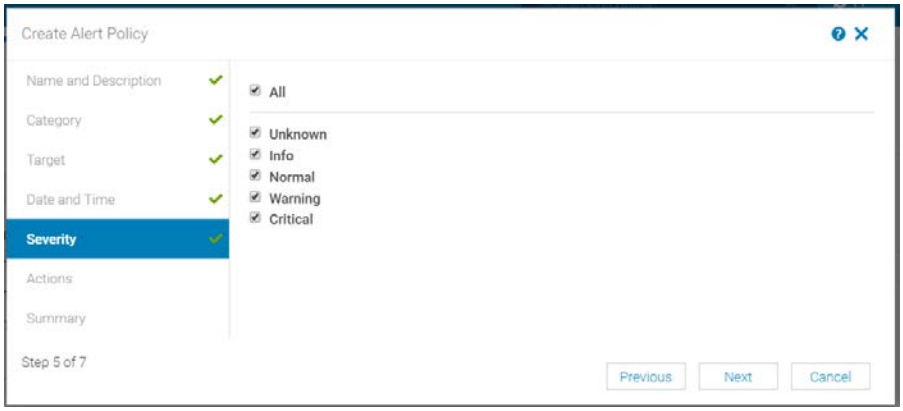
4. SNMP trap forwarding can be configured to send alert during a specific date or time range. If none of the options are selected in this wizard, trap forwarding is sent without any time restriction.

Figure 5 Date and time configuration



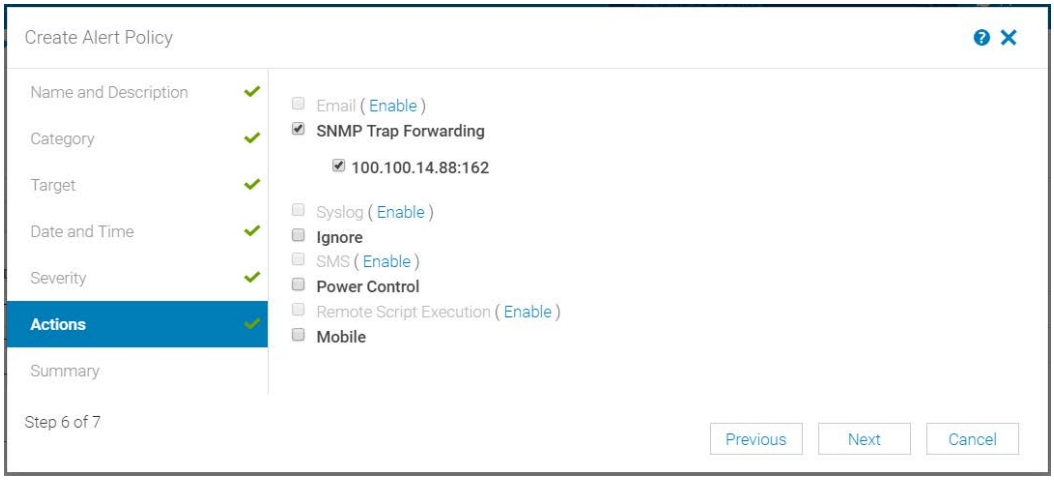
5. User can choose the below available severity based on their requirement.

Figure 6 Severity configuration



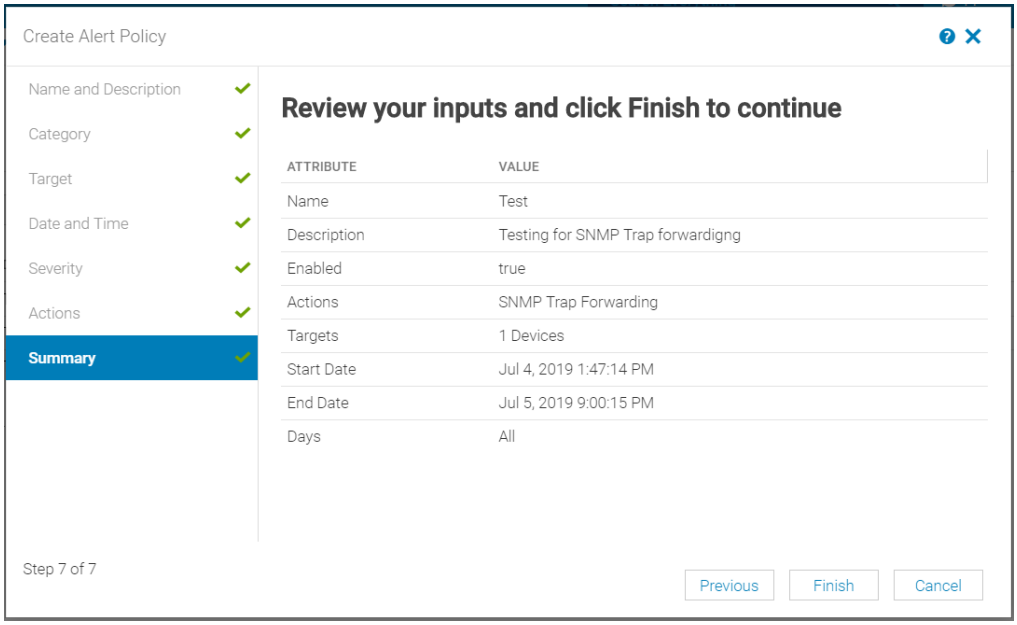
6. Select the SNMP trap forwarding destination as shown in figure7.

Figure 7 Action configuration



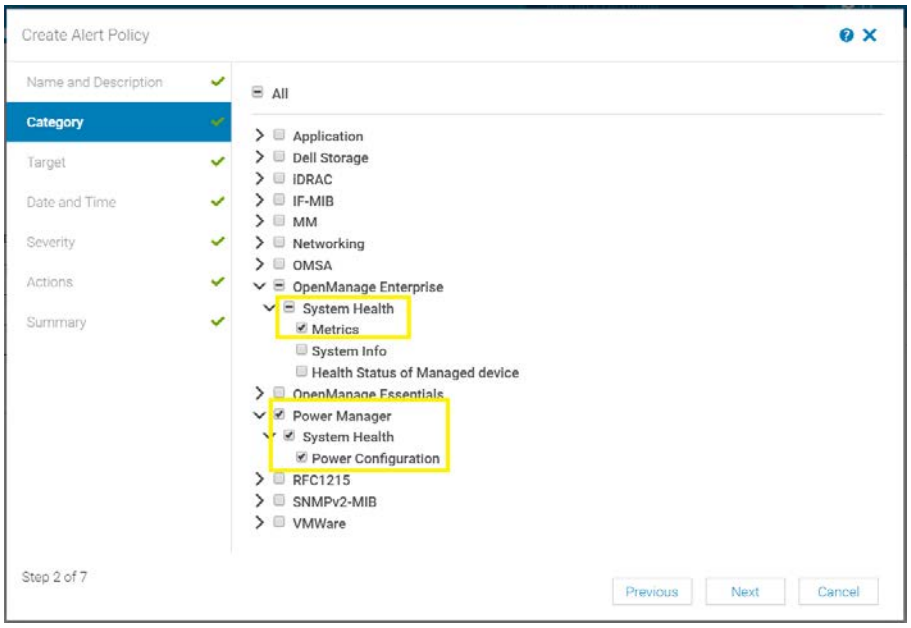
7. User can view overall summary of the configuration.

Figure 8 Summary



8. If you have alerts forwarded from OME1 to OME2 (In SNMP Format) and later this needs to be forwarded from OME2 to OME3 (In Original Format), you must choose the category as shown in Figure 9 and modify the trap forward format as mentioned in alert forward prerequisite settings.

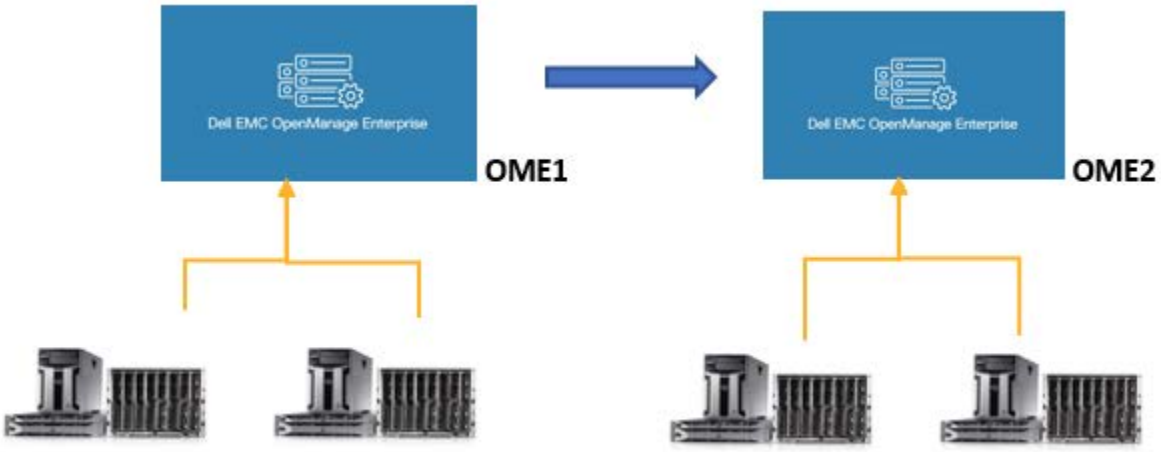
Figure 9 Category Configuration



5.2 Open Manage Enterprise Event Management

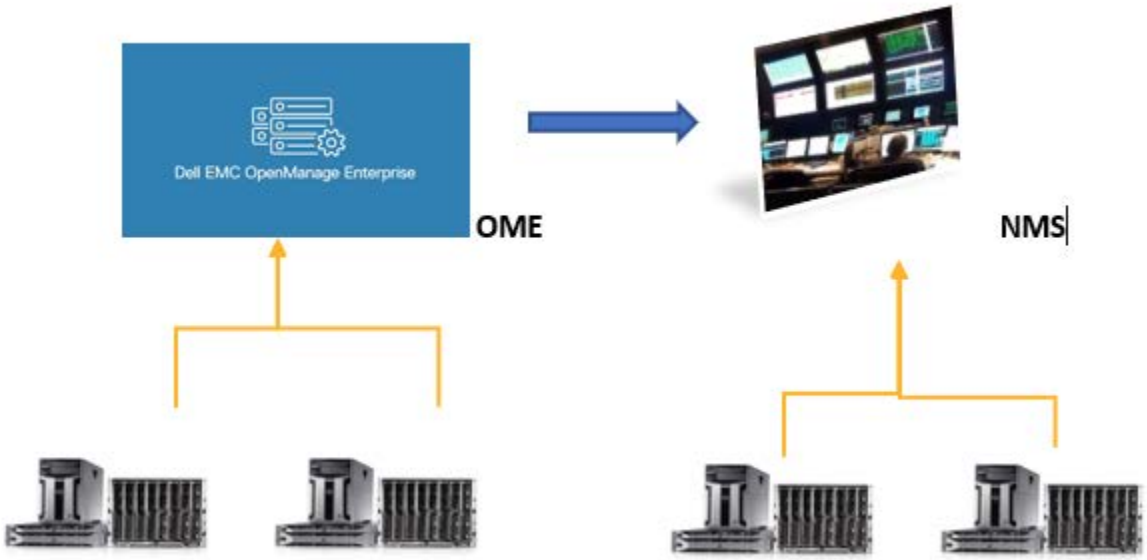
- To forward alerts from one Open Manage Enterprise console to other Open Manage Enterprise console, do not import MIB as it is pre-defined.

Figure 10 Forwarding alerts from OME1 to OME2



- To forward alerts from Open Manage Enterprise to other Network Management System (NMS), import Open Manage Enterprise Power Manager MIB to NMS.

Figure 11 Forward alerts from Open Manage Enterprise to NMS

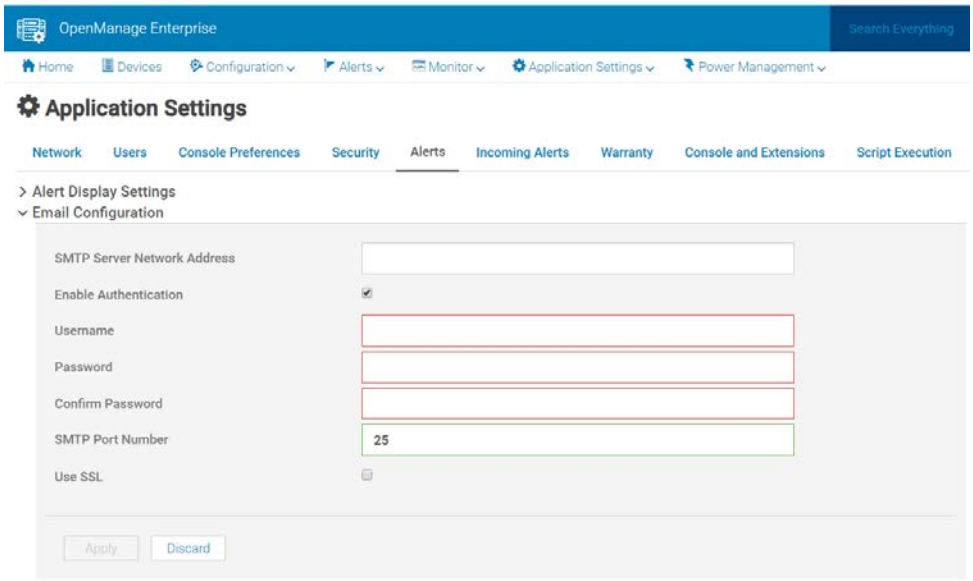


- To Download Open Manage Enterprise MIB files, see Dell EMC OpenManage Enterprise Version 3.2.1 User's Guide.
- To Download Open Manage Enterprise Power Manger MIB files, see Power Manager software downloads page.

6 Alert Email Action

- The Alert Email Action feature notifies you if a device or group exceeds the threshold or exceeds the power cap, without you having to log in to the Open Manage Enterprise console.
- Alert Email Action forwards the above alerts through email.
- You can customize alert severity, type, date, device, and days for alert email action.
- For IT administrator to receive emails through the support desk, an SMTP server is required. The SMTP settings can be configured when an email alert action task is created.
- For SMTP settings see below in Figure12, by default port 25 is selected. You can customize the port according to your environment. For secured communications, you can enable SSL.

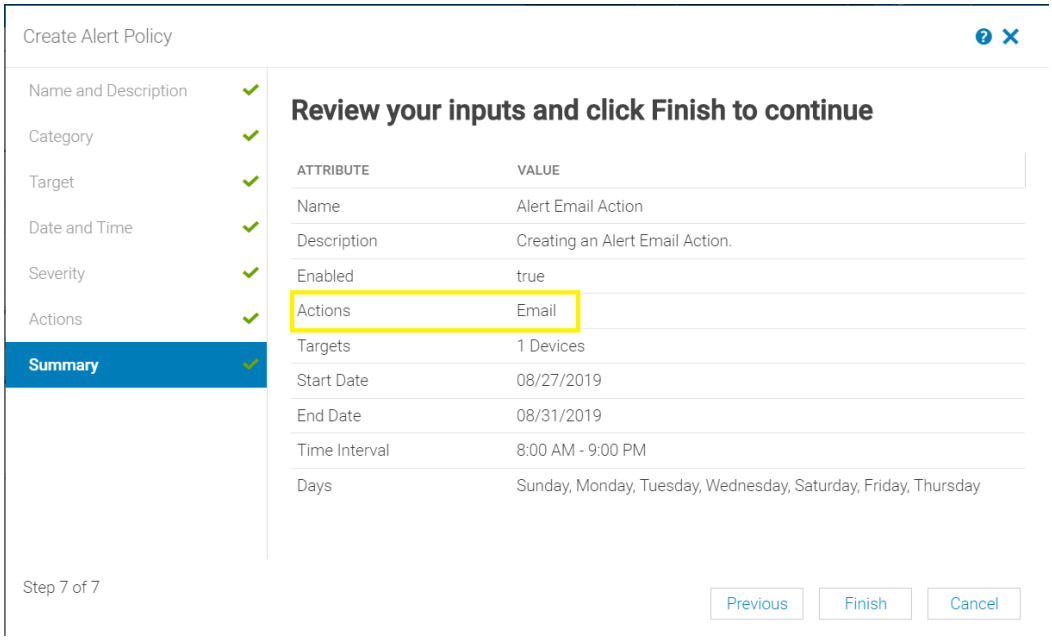
Figure 12 SMTP Settings page.



6.1 Creating an Alert Email Action

To create an Alert Email Action policy, follow the steps from Step 1 Step 5 as described in **Creating an Alert Trap Forward Action** section. For step 6, select the email action instead of SNMP traps and verify the summary.

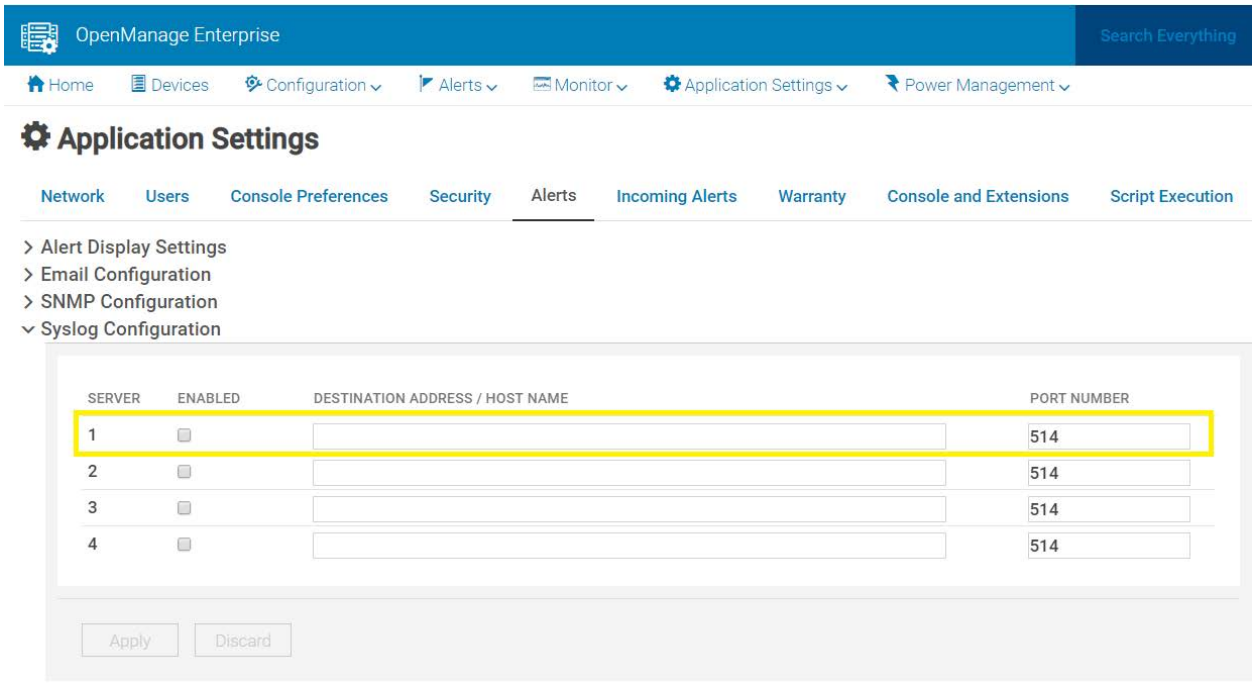
Figure 13 Email Summary



7 Alert Forward Action for Syslog Watcher

- The syslog protocol is a network logging standard supported by a wide range of network devices, appliances, and servers.
- Syslog messages deliver information on network events and errors. System administrators use Syslog for network management and security auditing. With a dedicated syslog server, the syslog protocol consolidates event records from all over the network into a single central repository.
- Syslog Watcher installs a dedicated syslog server, integrating log data from multiple network devices into a single, easily manageable and accessible place.
- Syslog Watcher supports IPv4 or IPv6 interfaces.
- Syslog Watcher supports exporting syslog messages to any text file types, for example CSV, XML, and JSON.
- For configuring syslog server setting see Figure14, by default the port number is 514.

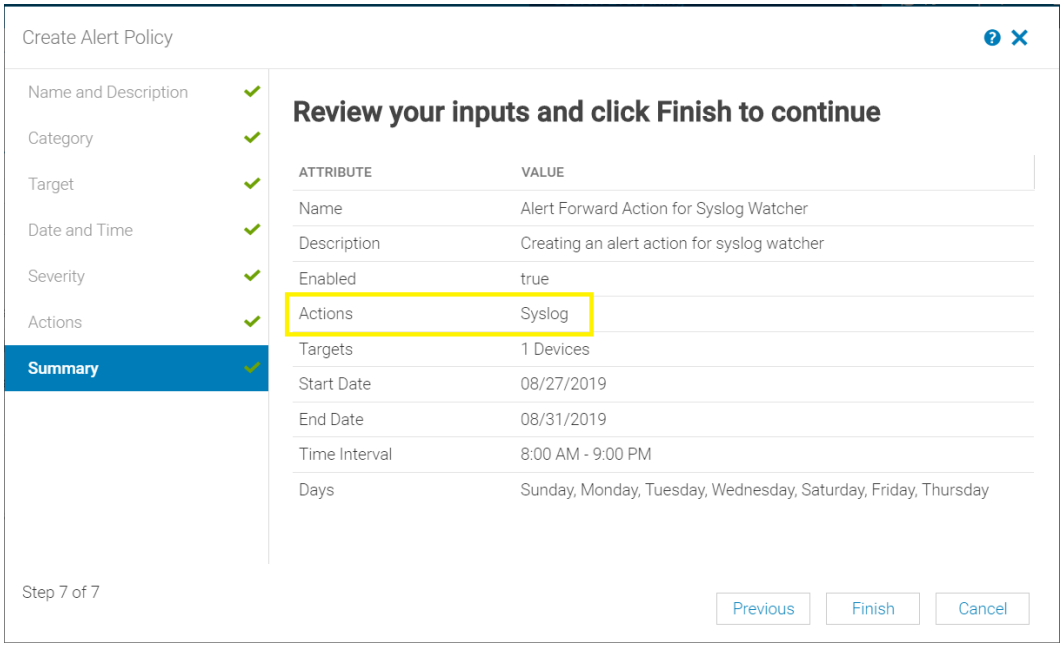
Figure 14 Syslog Configuration.



7.1 Creating an Alert Action for Syslog Watcher

To create an alert action for syslog watcher policy, follow the steps from step 1 to 6 as described in **Creating an Alert Trap Forward Action** section. For step 7, select the syslog watcher action instead of SNMP traps and verify the summary.

Figure 15 Syslog Summary



8 Alert Ignore Action

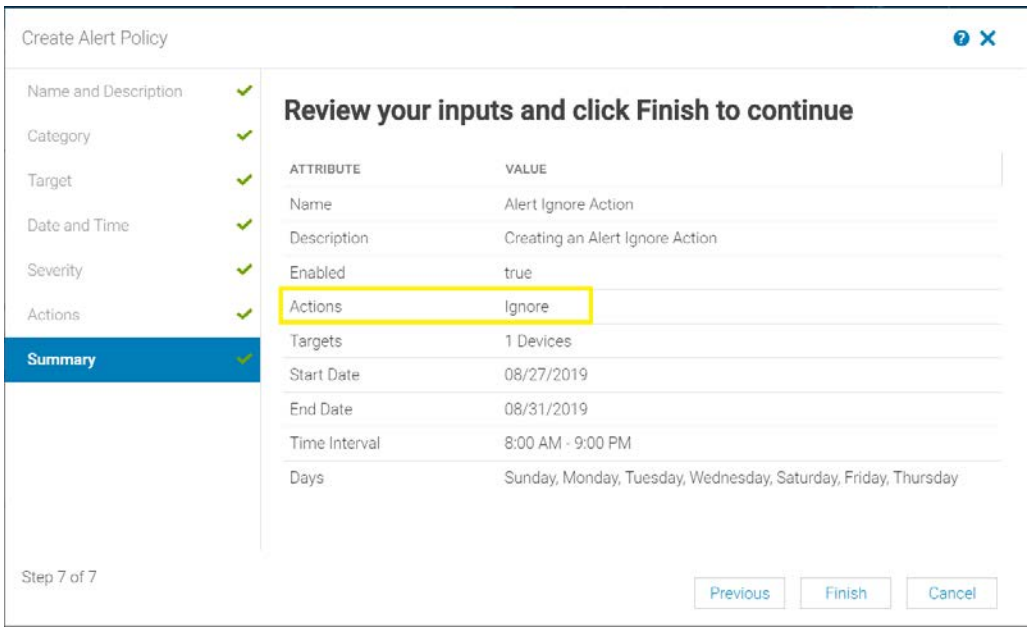
An IT administrator can choose to ignore alerts for various reasons:

- If a maintenance task is scheduled in a data center, alerts are received in bulk and the alert log is recorded in large numbers in OME. These are known alerts and can be ignored instead of overloading the database.
- When you are aware that there are a few faulty devices in the data center that keep generating alerts frequently, alerts from these devices can be ignored.
- In case the devices are sending similar alerts continuously, you can choose to avoid receiving duplicate alerts in the console.

8.1 Creating an Alert Ignore Action

To create an alert action for Ignore policy, follow the steps from step 1 to 6 as described in **Creating an Alert Trap Forward Action** section. For step 7, select the syslog watcher action instead of SNMP traps and verify the summary.

Figure 16 Syslog Watcher Summary



9 Generic Recommendations

- Create static groups in below structure and set the threshold for better management.
  - Data center→Room→Aisle→Rack
- Avoid group membership changes. However, Power Manager generates internal alerts for group membership changes.
- When Power Manager generates any alerts for power policy violation, take necessary actions.
- You can create below policies to leverage it for Power Manager events:
  - Alert Email Action
  - Alert Trap Forward Action
  - Alert Forward Action for Syslog Watcher
  - Alert Ignore Action

10 Conclusion

All the different ways of configuring and managing your alerts from Power Manager through OpenManage Enterprise are explained in detail. For more information about different Dell EMC PowerEdge servers, see the Dell PowerEdge Servers Portfolio Guide.

11 Technical Support

- Dell.com/support is focused on meeting customer needs with proven services and support.
- To watch quick and short videos about handling the PowerEdge server components, visit the QRL video website.
- Storage technical documents and videos provide expertise that helps to ensure customer success on Dell EMC storage platforms.