Technical Whitepaper

Mitigate Thermal Issues in a Data Center Using OpenManage Enterprise Power Manager

Abstract

This technical whitepaper provides an overview about the Alert Policy feature of OpenManage Enterprise Power Manager.

November 2024

Revisions

Date	Description
November 2024	Initial release

Acknowledgements

Author:

- **Anil Kumar Maharana**—Software Principal Engineer, OpenMange Enterprise Power Manager
- **Sreelakshmi Prakash**—Software Principal Engineer, OpenMange Enterprise Power Manager

Support:

- **Pavithra Sundar**—Technical Content Developer 3, Content Engineering & Translation

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Contents

Executive Summary

This technical whitepaper provides recommendations about using the Alert Policies feature of OpenManage Enterprise on the device, GPU, and CPU threshold feature of the Power Manager Plugin. Some of the key features are:

- Thresholds and alerts:
  - Define optimal power and temperature thresholds.
  - Configure alert policies for metrics.
- Operational actions:
  - Automate actions like turning on or off power based on power or temperature alerts.

1 Introduction

Alert policy provides the flexibility to take specific actions based on alerts generated for threshold violations. These thresholds are typically set for power or temperature metrics. You can configure the various actions to be taken when an alert occurs.

Use Cases:

- Critical situations: For critical alerts (excessive load or overheating), immediate action (like powering off) may be necessary to prevent hardware damage.
- Scheduled maintenance: During planned maintenance, customers can schedule actions like restarting servers to address noncritical alerts.

Available Actions:

You can configure various actions to be taken when an alert occurs:

- Power off: Automatically power off the affected device or group of devices to prevent further issues.
- Power on: Power on the device after addressing the alert condition.
- Notify Administrators: Send notifications to relevant personnel by using an email or SMS. Also, alerts can be forwarded to other consoles.

2 Purpose of alert policies

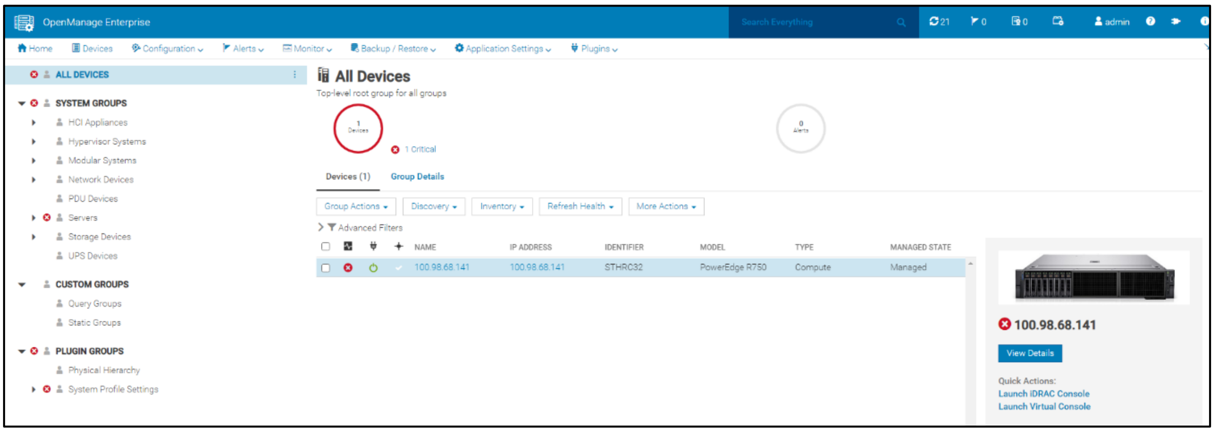
You can perform the following actions using the Alert Policies feature when you receive alerts:

- Forward alerts to other management console.
- Send an SMS or email alerts.
- Power off a server in response to specific error.
- Power on a server in response to error recovery.

3 Add devices to monitoring list

To configure threshold and apply alert policy on devices, they must be discovered in OpenManage Enterprise. After the discovery is successful, add the devices to the monitoring list in Power Manager.

To discover the devices, use the OpenManage Enterprise discovery feature.

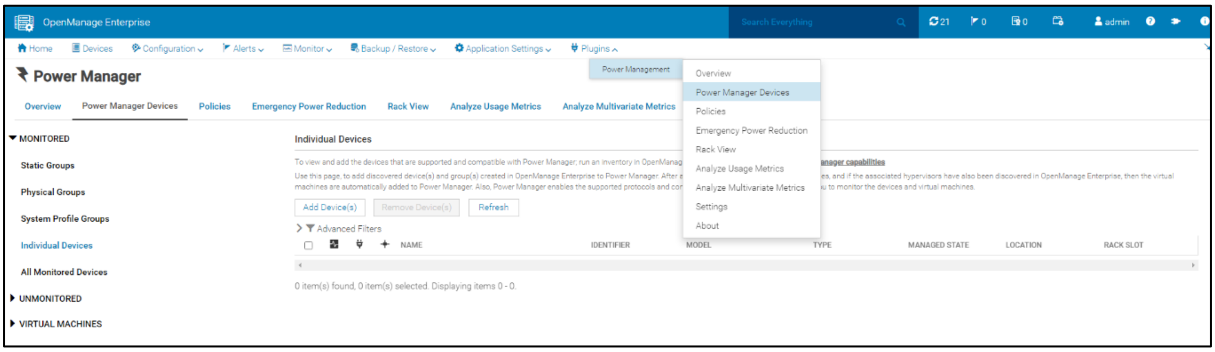


Top-level root group for all groups

NAME	IP ADDRESS	IDENTIFIER	MODEL	TYPE	MANAGED STATE
100.98.68.141	100.98.68.141	STHRC32	PowerEdge R750	Compute	Managed

Figure 1 All device page

1. Click **Plugins → Power Management → Power Manager Devices → Individual Devices → Add Device**.



Individual Devices

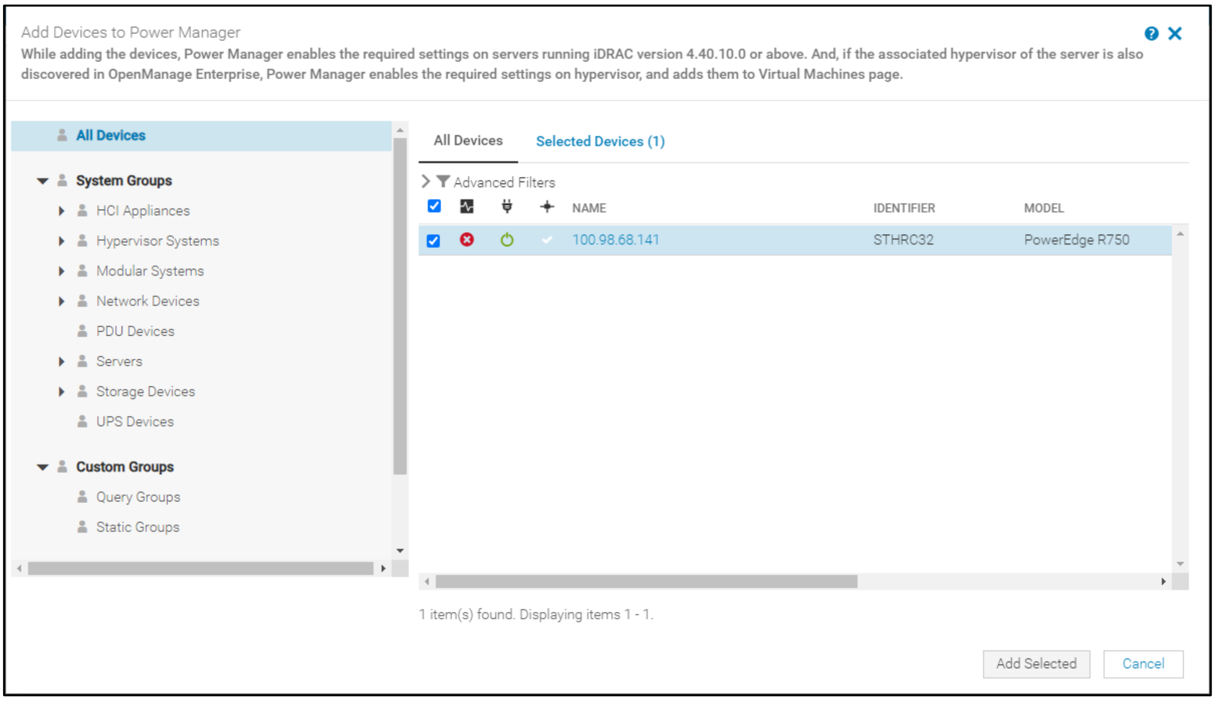
To view and add the devices that are supported and compatible with Power Manager, run an inventory in OpenManag anager capabilities

Use this page, to add discovered device(s) and group(s) created in OpenManage Enterprise to Power Manager. After a es, and if the associated hypervisors have also been discovered in OpenManage Enterprise, then the virtual machines are automatically added to Power Manager. Also, Power Manager enables the supported protocols and cor u to monitor the devices and virtual machines.

0 item(s) found, 0 item(s) selected. Displaying items 0 - 0.

Figure 2 Add device to monitoring list

2. On the **Add Devices to Power Manager** page, select the device you want to add to the monitoring list and click **Add Selected**.



Add Devices to Power Manager

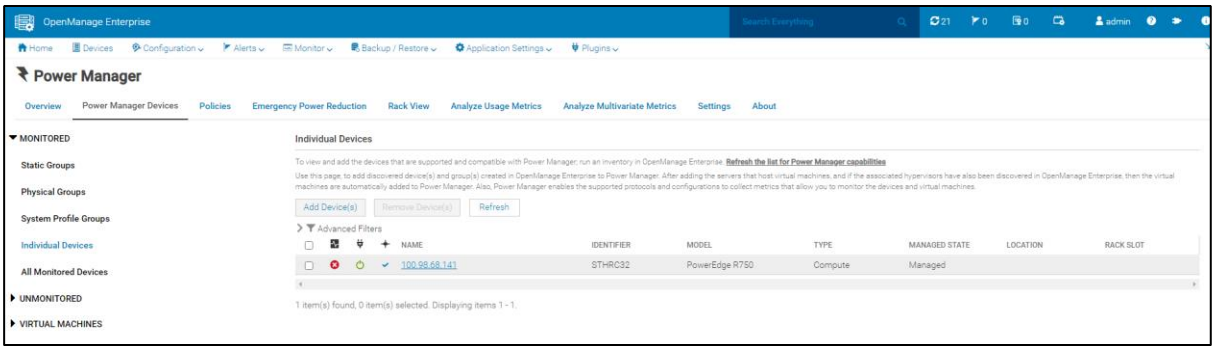
While adding the devices, Power Manager enables the required settings on servers running iDRAC version 4.40.10.0 or above. And, if the associated hypervisor of the server is also discovered in OpenManage Enterprise, Power Manager enables the required settings on hypervisor, and adds them to Virtual Machines page.

☑				NAME	IDENTIFIER	MODEL
☑	⊗	⏻	✓	100.98.68.141	STHRC32	PowerEdge R750

1 item(s) found. Displaying items 1 - 1.

Figure 3 Monitoring list page

3. To view the device metrics or to set device-level or component-level (GPU or CPU) threshold, click the name of the device on the **Individual Devices** page.



Individual Devices

To view and add the devices that are supported and compatible with Power Manager, run an inventory in OpenManage Enterprise. **Refresh the list for Power Manager capabilities**

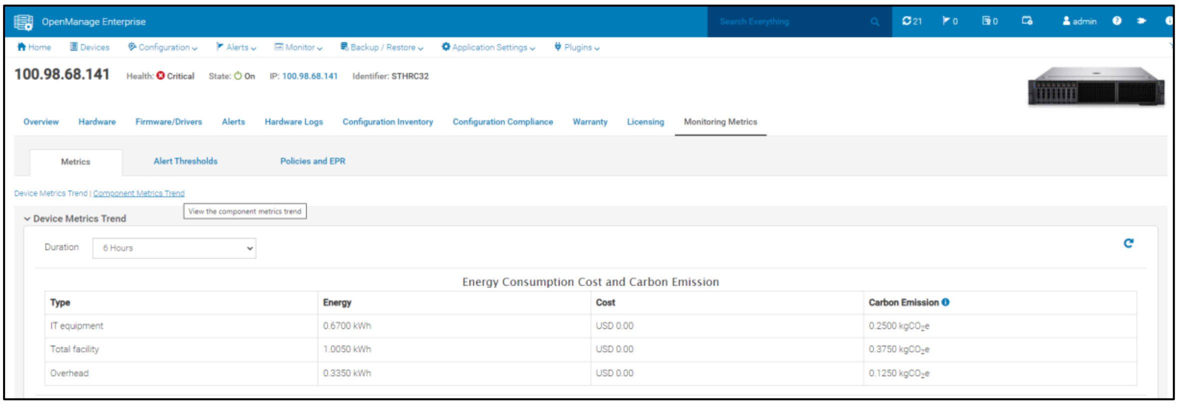
Use this page, to add discovered device(s) and group(s) created in OpenManage Enterprise to Power Manager. After adding the servers that host virtual machines, and if the associated hypervisors have also been discovered in OpenManage Enterprise, then the virtual machines are automatically added to Power Manager. Also, Power Manager enables the supported protocols and configurations to collect metrics that allow you to monitor the devices and virtual machines.

□				NAME	IDENTIFIER	MODEL	TYPE	MANAGED STATE	LOCATION	RACK SLOT
□	⊗	⏻	✓	100.98.68.141	STHRC32	PowerEdge R750	Compute	Managed		

1 item(s) found, 0 item(s) selected. Displaying items 1 - 1.

Figure 4 Power Manager devices page

4. To view metrics, go to the **Monitoring Metrics** tab, and then click the **Metrics** tab.
5. For device metrics, click **Device Metrics Trend**. For component metrics—CPU and GPU—click **Component Metrics Trend**.



100.98.68.141 Health: Critical State: On IP: 100.98.68.141 Identifier: STHRC32

Duration: 6 Hours

Energy Consumption Cost and Carbon Emission

Type	Energy	Cost	Carbon Emission
IT equipment	0.6700 kWh	USD 0.00	0.2500 $kgCO_2e$
Total facility	1.0050 kWh	USD 0.00	0.3750 $kgCO_2e$
Overhead	0.3350 kWh	USD 0.00	0.1250 $kgCO_2e$

Figure 5 Monitoring Metrics page

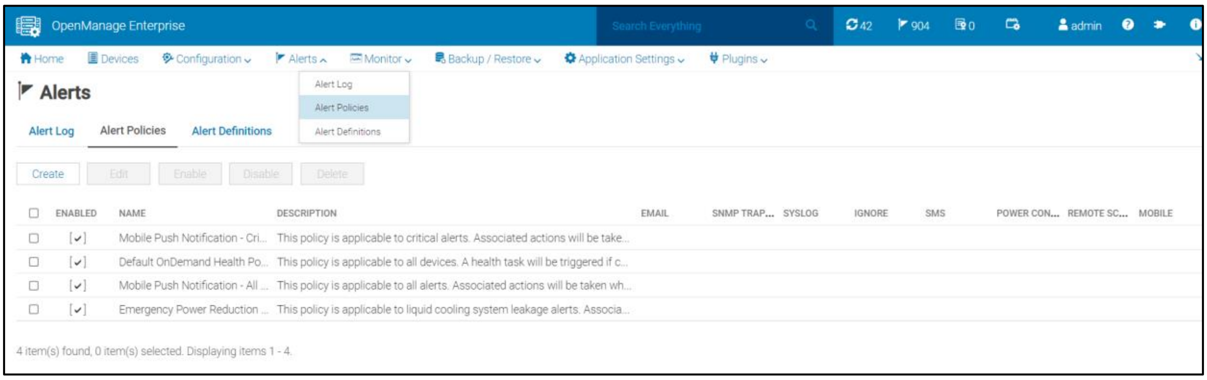
4 Configure alert policy and threshold

After a device is discovered and added to the monitoring list in Power Manager, metrics get collected for monitored devices and groups. You can configure thresholds for devices and components (CPU and GPU). This enables actions to be triggered based on the alert policies that have been configured.

4.1 Configure alert policy and threshold for component metrics

4.1.1 Create alert policy for component metrics

1. Log in to OpenManage Enterprise.
2. From the **Alerts** drop-down menu, select **Alert Policies**.
3. Click **Create**.



□	ENABLED	NAME	DESCRIPTION	EMAIL	SNMP TRAP...	SYSLOG	IGNORE	SMS	POWER CON...	REMOTE SC...	MOBILE
□	[✓]	Mobile Push Notification - Cri...	This policy is applicable to critical alerts. Associated actions will be take...								
□	[✓]	Default OnDemand Health Po...	This policy is applicable to all devices. A health task will be triggered if c...								
□	[✓]	Mobile Push Notification - All ...	This policy is applicable to all alerts. Associated actions will be taken wh...								
□	[✓]	Emergency Power Reduction ...	This policy is applicable to liquid cooling system leakage alerts. Associa...								

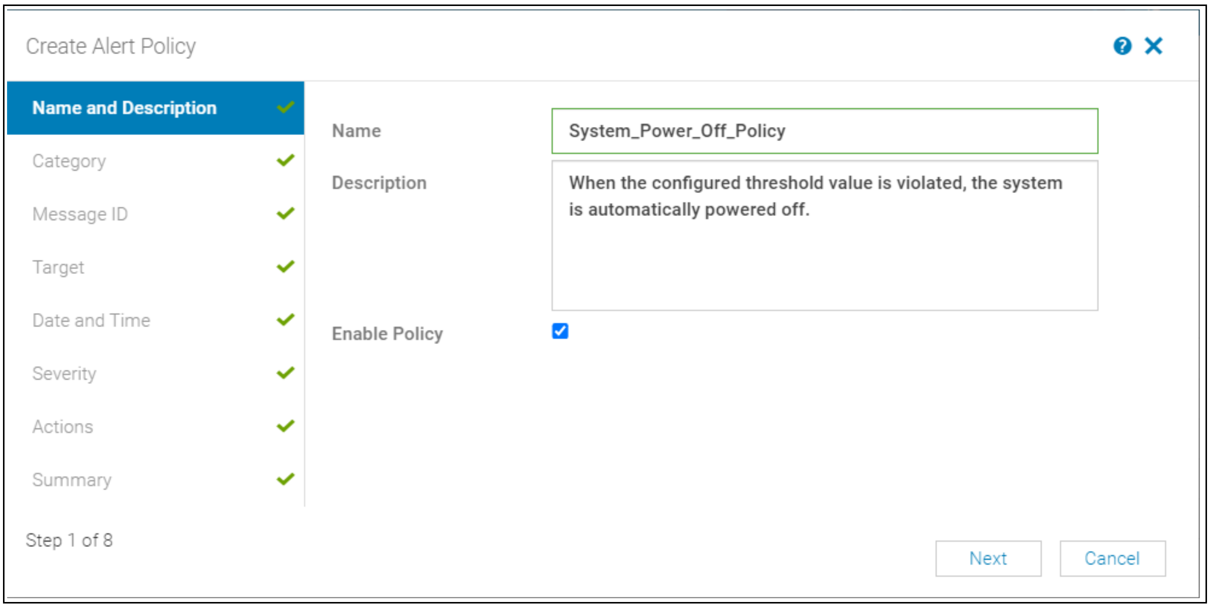
4 item(s) found, 0 item(s) selected. Displaying items 1 - 4.

Figure 6 Alert policy

4.1.1.1 Configure alert policy for critical alert

On the Create Alert Policy page, do the following to create an alert policy for a critical alert on CPU or GPU temperature metrics:

1. Enter a name and description for the policy that gets triggered when critical alert is generated for GPU or CPU components.
   By default, the **Enable Policy** check box is selected to activate the policy after it is created.



Create Alert Policy

Name: System_Power_Off_Policy

Description: When the configured threshold value is violated, the system is automatically powered off.

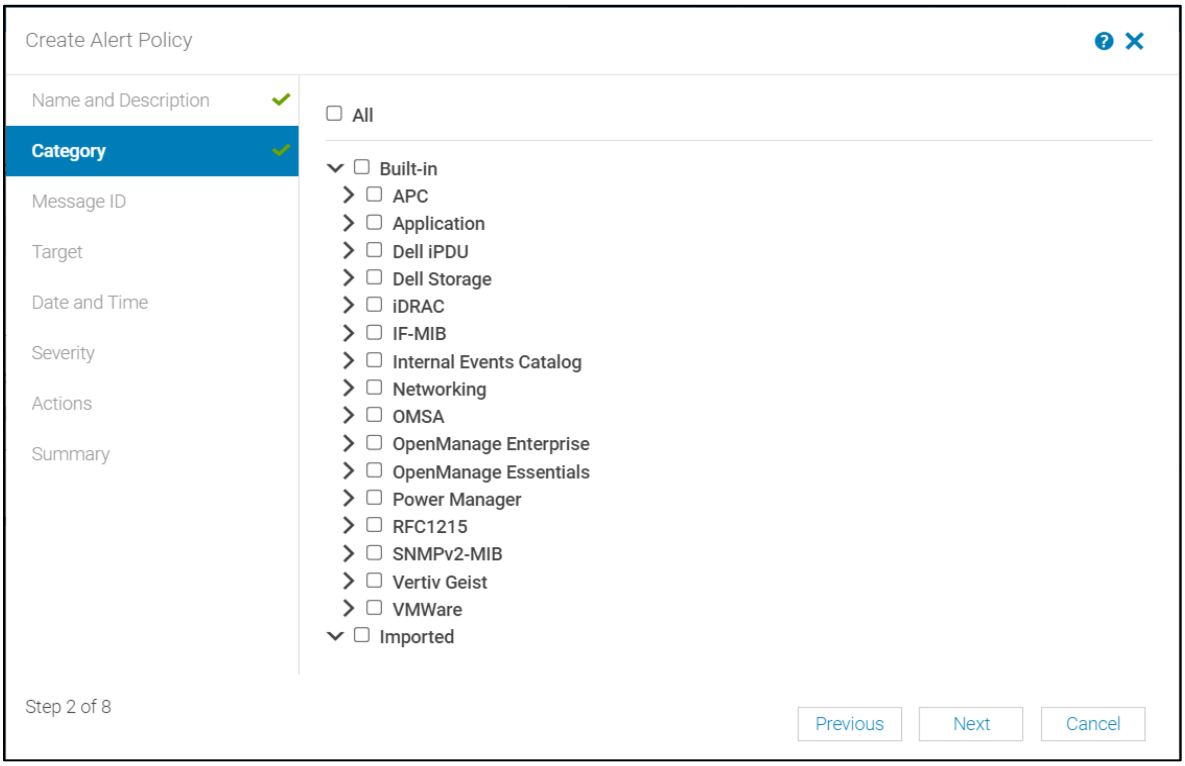
Enable Policy ☑

Figure 7 Alert policy name and description

In the **Category** section, the built-in categories for OpenManage Enterprise and associated plug-ins are available. Power Manager workflows are associated with the following categories:

- Application → System Health → Metrics
- Application → System Health → Power Configuration
- PDU Support – APC, Vertiv, and Dell iPDU

The Category section is generic and an optional step.

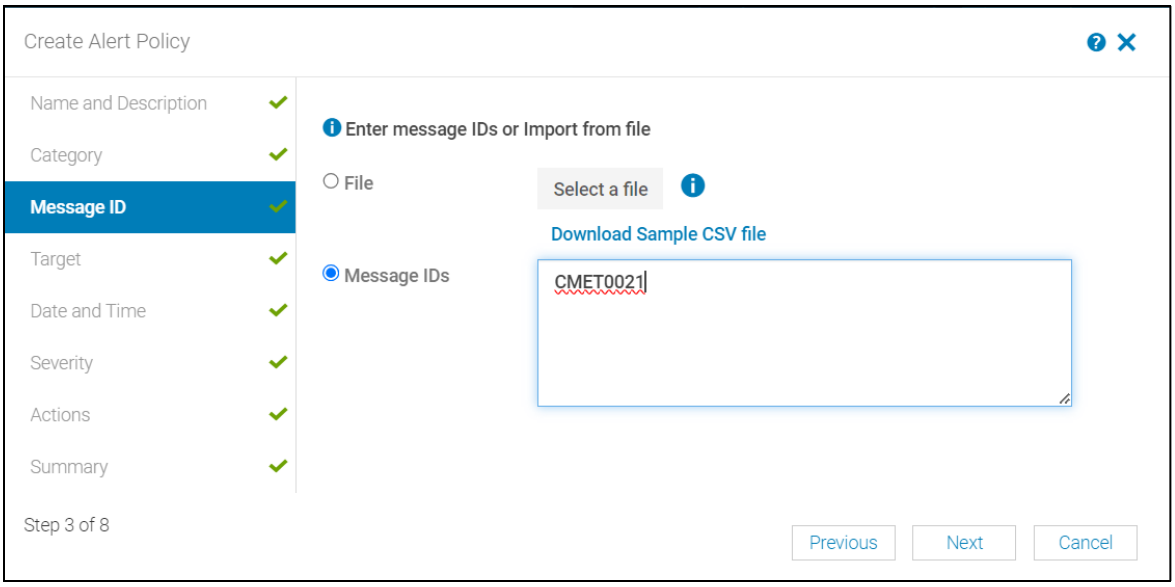


Create Alert Policy

- □ All
- □ Built-in
  - □ APC
  - □ Application
  - □ Dell iPDU
  - □ Dell Storage
  - □ iDRAC
  - □ IF-MIB
  - □ Internal Events Catalog
  - □ Networking
  - □ OMSA
  - □ OpenManage Enterprise
  - □ OpenManage Essentials
  - □ Power Manager
  - □ RFC1215
  - □ SNMPv2-MIB
  - □ Vertiv Geist
  - □ VMWare
- □ Imported

Figure 8 Alert policy category

2. To configure the alert policy for CPU or GPU temperature critical alert, enter the message ID.
   - For CPU, the message ID is **CMET0021**.
   - For GPU, the message ID is **CMET0018**.



Create Alert Policy

- Name and Description ✓
- Category ✓
- **Message ID** ✓
- Target ✓
- Date and Time ✓
- Severity ✓
- Actions ✓
- Summary ✓

Enter message IDs or Import from file

○ File Select a file

Download Sample CSV file

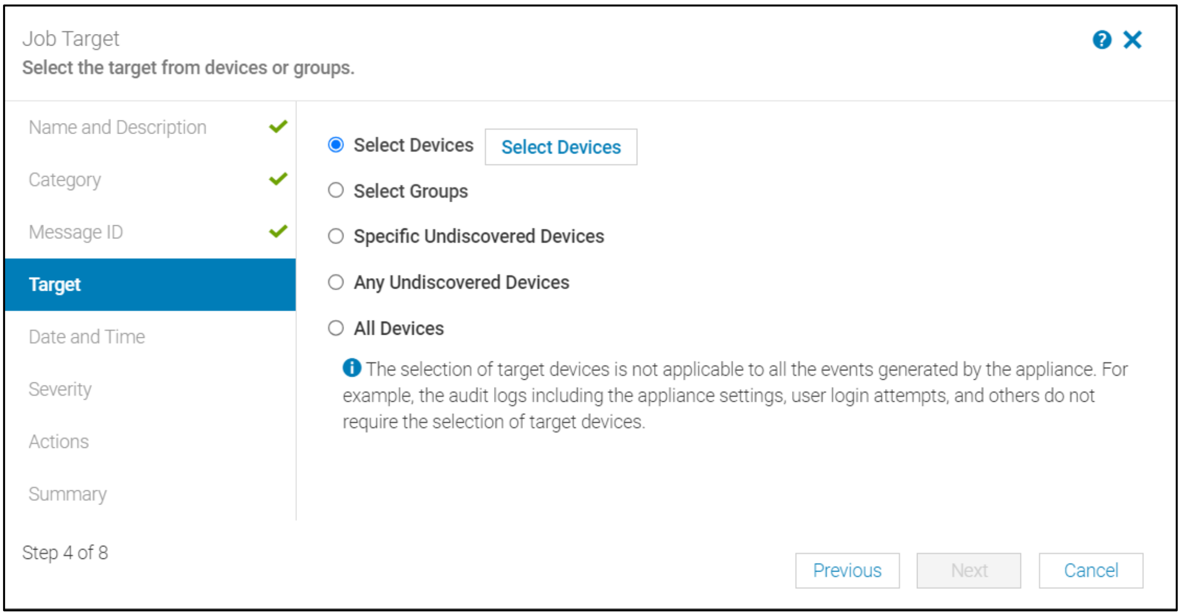
● Message IDs CMET0021

Step 3 of 8

Previous Next Cancel

Figure 9 Alert policy message IDs

3. In the **Target** section, select the required target devices by clicking the **Select Devices** list on which this policy must be applied. Groups are not applicable for component metrics because component-level threshold feature is not supported for groups.



Job Target

Select the target from devices or groups.

- Name and Description ✓
- Category ✓
- Message ID ✓
- **Target**
- Date and Time
- Severity
- Actions
- Summary

● Select Devices Select Devices

○ Select Groups

○ Specific Undiscovered Devices

○ Any Undiscovered Devices

○ All Devices

The selection of target devices is not applicable to all the events generated by the appliance. For example, the audit logs including the appliance settings, user login attempts, and others do not require the selection of target devices.

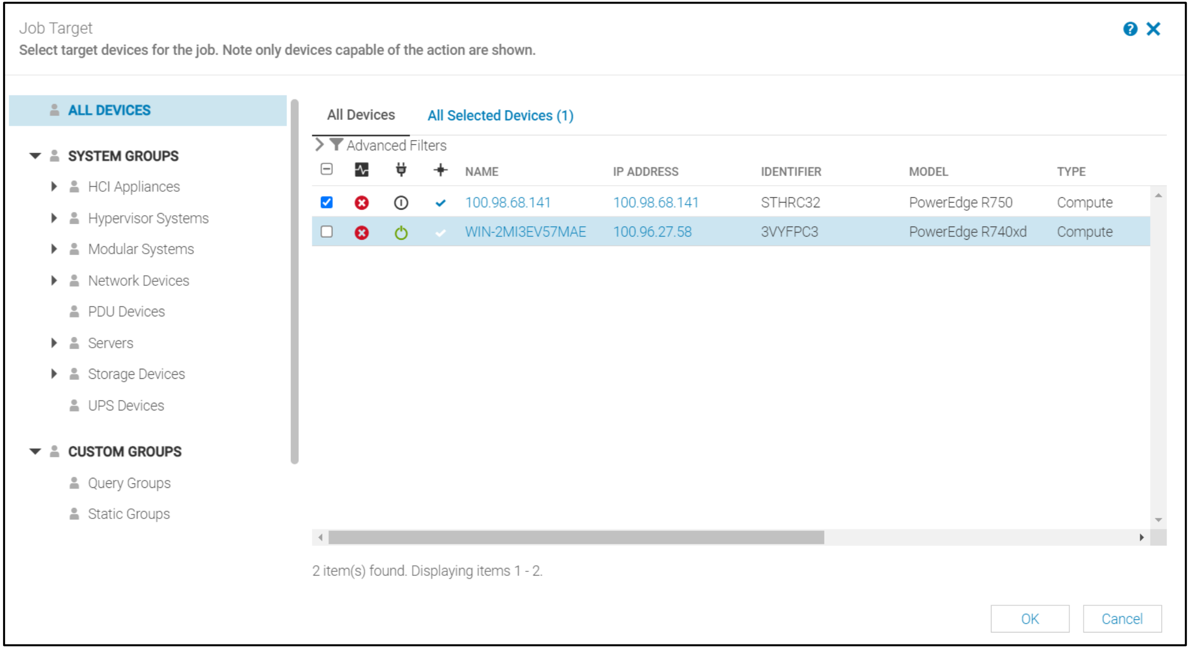
Step 4 of 8

Previous Next Cancel

Figure 10 Alert policy target

4. Select the device from the list and click **OK**.

Select the target devices on the Create Alert Policy page.



Job Target

Select target devices for the job. Note only devices capable of the action are shown.

- ALL DEVICES
- SYSTEM GROUPS
  - HCI Appliances
  - Hypervisor Systems
  - Modular Systems
  - Network Devices
  - PDU Devices
  - Servers
  - Storage Devices
  - UPS Devices
- CUSTOM GROUPS
  - Query Groups
  - Static Groups

All Devices | All Selected Devices (1)

Advanced Filters

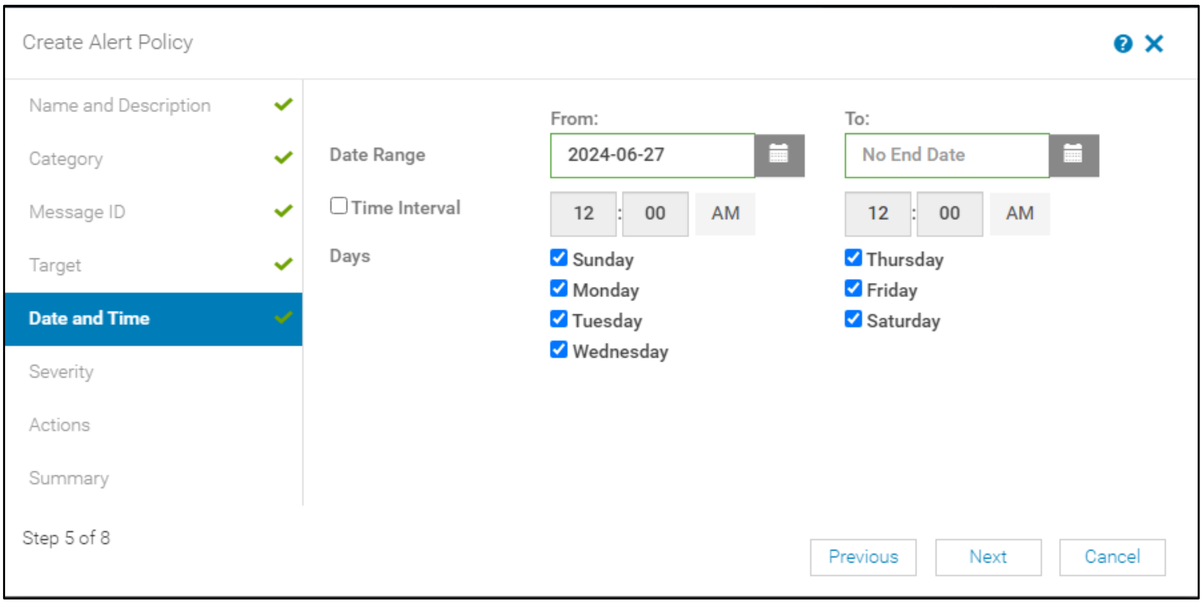
				NAME	IP ADDRESS	IDENTIFIER	MODEL	TYPE
☑	☒	ⓘ	✓	100.98.68.141	100.98.68.141	STHRC32	PowerEdge R750	Compute
□	☒	⏻	✓	WIN-2MI3EV57MAE	100.96.27.58	3VYFPC3	PowerEdge R740xd	Compute

2 item(s) found. Displaying items 1 - 2.

OK | Cancel

Figure 11 Select device for policy

5. It is recommended to use the default date and time settings for a perpetual policy. If the policy action needs to be applied only for a specific period, specify using the **Date Range**, **Time Interval**, and **Days** options.



Create Alert Policy

- Name and Description ✓
- Category ✓
- Message ID ✓
- Target ✓
- Date and Time ✓
- Severity
- Actions
- Summary

Date Range — From: 2024-06-27 — To: No End Date

□ Time Interval — 12 : 00 AM — 12 : 00 AM

Days

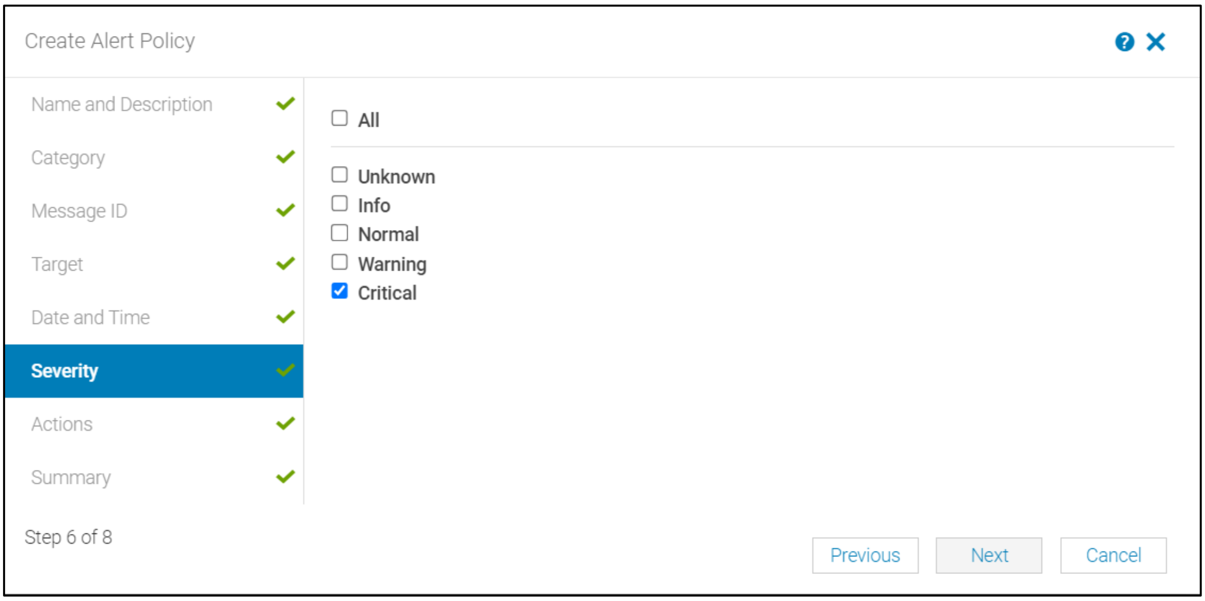
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Step 5 of 8

Previous | Next | Cancel

Figure 12 Alert policy date and time selection

6. Select the severity level as **Critical** for the alert.

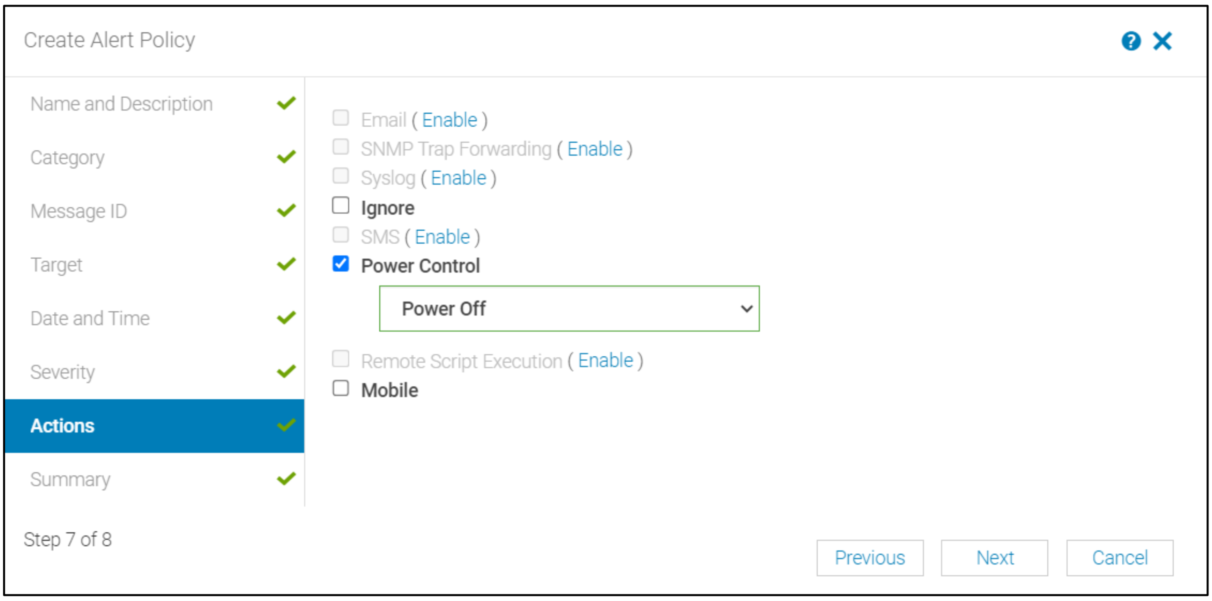


□ All

□ Unknown
□ Info
□ Normal
□ Warning
☑ Critical

Figure 13 Alert policy severity selection

7. In the **Actions** section, select the **Power Control** check box, and then select **Power Off** from the drop-down list. This is to power off the target device when a critical alert is generated on its CPU or GPU.



□ Email (Enable)
□ SNMP Trap Forwarding (Enable)
□ Syslog (Enable)
□ Ignore
□ SMS (Enable)
☑ Power Control

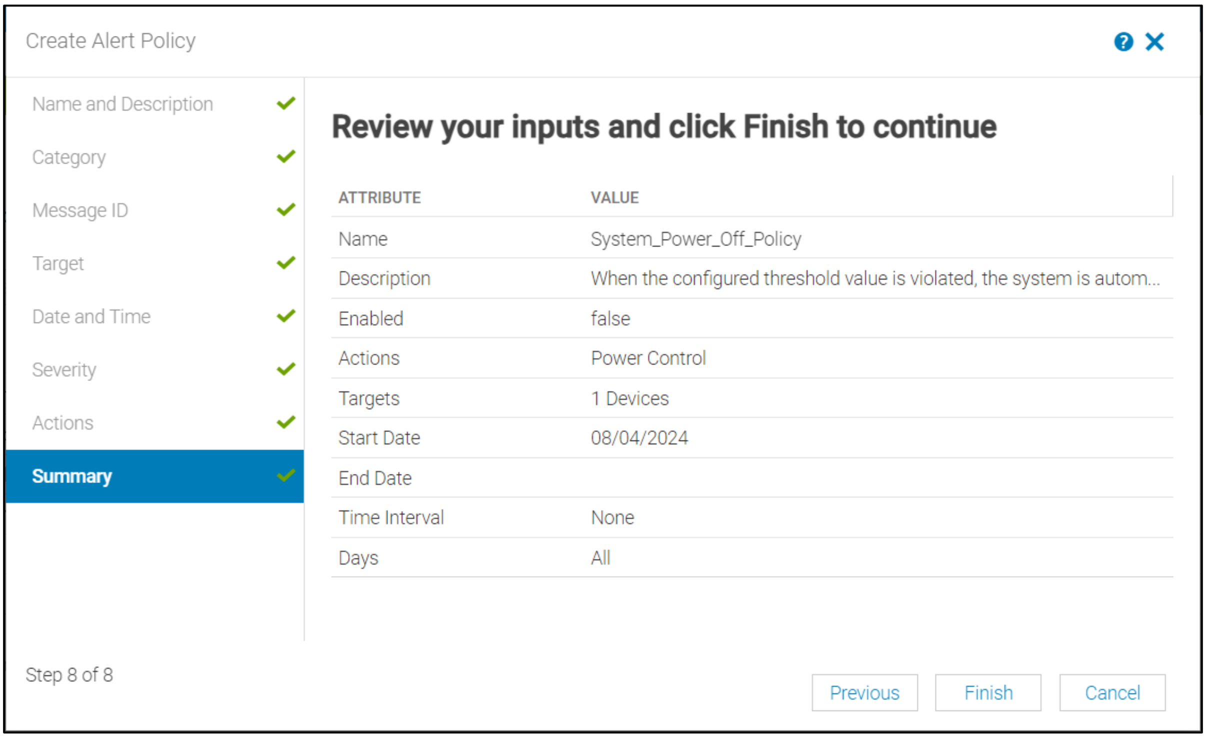
Power Off

□ Remote Script Execution (Enable)
□ Mobile

Figure 14 Alert policy actions

8. The **Summary** section displays all the details of the alert policy to be reviewed before creation. To update any values, go to the respective page and update it.

9. Click **Finish** to complete the Alert Policy creation for critical alert.



Create Alert Policy

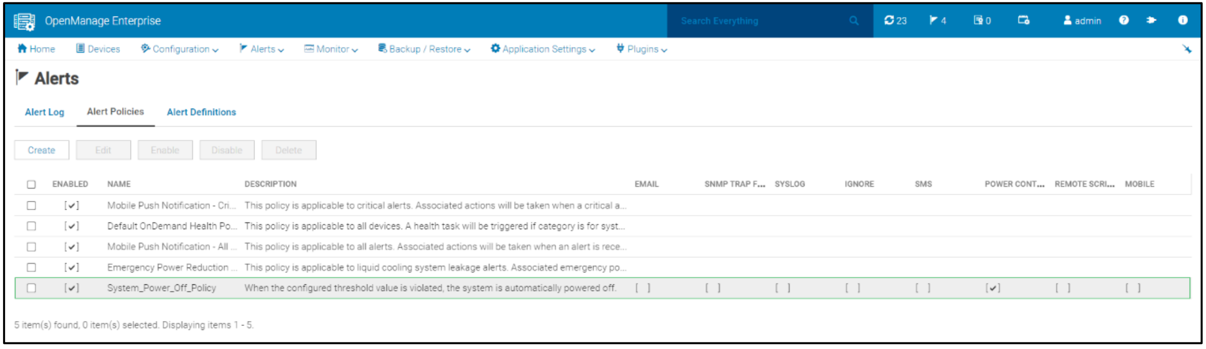
Review your inputs and click Finish to continue

ATTRIBUTE	VALUE
Name	System_Power_Off_Policy
Description	When the configured threshold value is violated, the system is autom...
Enabled	false
Actions	Power Control
Targets	1 Devices
Start Date	08/04/2024
End Date	
Time Interval	None
Days	All

Step 8 of 8

Figure 15 Alert policy summary

After the alert policy is created, you can edit, delete, disable, or enable the policy by selecting the respective policy.



Alerts

☐	ENABLED	NAME	DESCRIPTION	EMAIL	SNMP TRAP F...	SYSLOG	IGNORE	SMS	POWER CONT...	REMOTE SCRI...	MOBILE
☐	[✓]	Mobile Push Notification - Cri...	This policy is applicable to critical alerts. Associated actions will be taken when a critical a...								
☐	[✓]	Default OnDemand Health Po...	This policy is applicable to all devices. A health task will be triggered if category is for syst...								
☐	[✓]	Mobile Push Notification - All ...	This policy is applicable to all alerts. Associated actions will be taken when an alert is rece...								
☐	[✓]	Emergency Power Reduction ...	This policy is applicable to liquid cooling system leakage alerts. Associated emergency po...								
☐	[✓]	System_Power_Off_Policy	When the configured threshold value is violated, the system is automatically powered off.	[ ]	[ ]	[ ]	[ ]	[ ]	[✓]	[ ]	[ ]

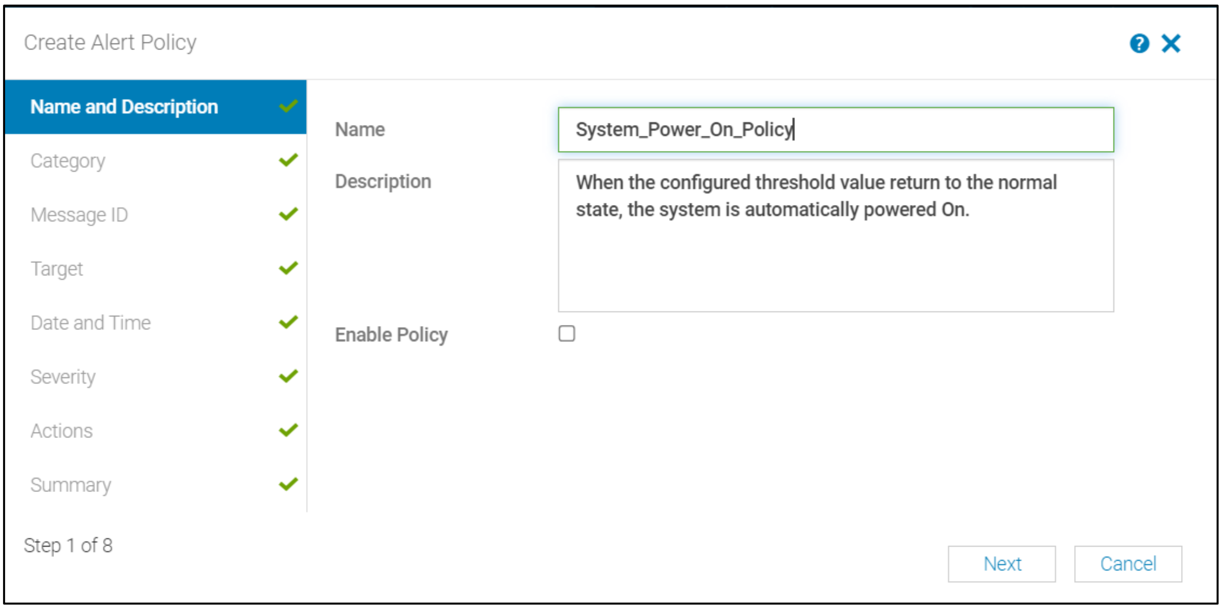
5 item(s) found, 0 item(s) selected. Displaying items 1 - 5.

Figure 16 Alert policy page

4.1.1.2 Configure alert policy for normal alert

When a threshold value for temperature metrics of CPU or GPU components returns to a normal range, the device must be powered on. To automatically power on the devices to recover, alert policy must be created for normal alert. On the Create Alert Policy page, do the following to create an alert policy for a normal alert on CPU or GPU temperature metrics:

1. Enter a name and description for the policy that gets triggered when a normal alert is generated for components.
   By default, the **Enable Policy** check box is selected to activate the policy after it is created.



Create Alert Policy

Name: System_Power_On_Policy

Description: When the configured threshold value return to the normal state, the system is automatically powered On.

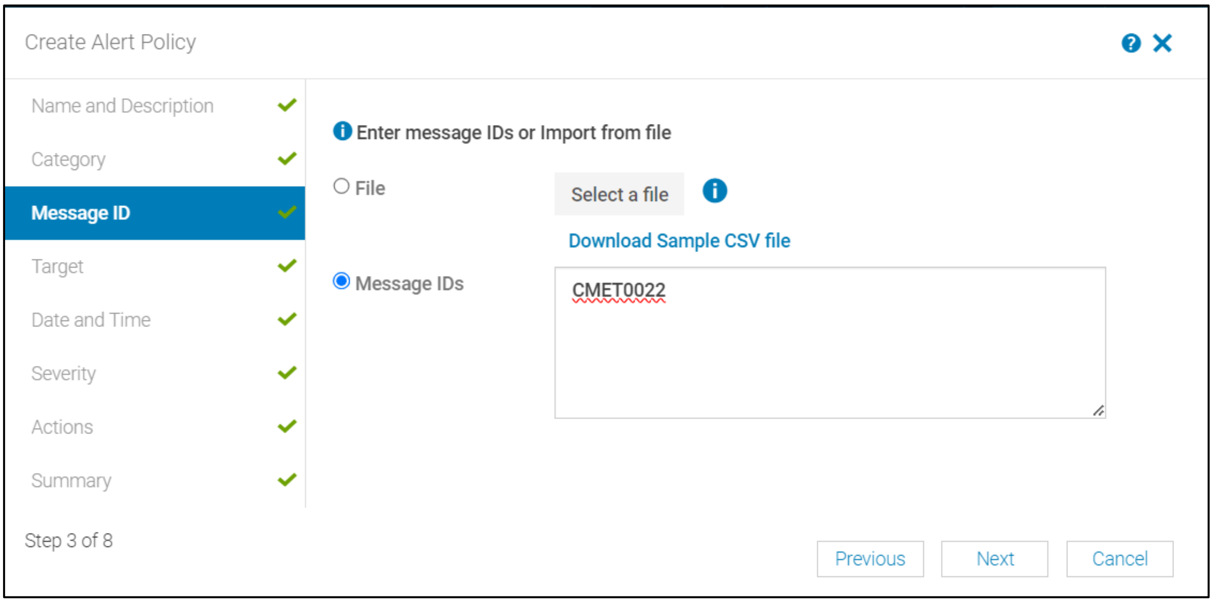
Enable Policy □

Step 1 of 8

Figure 17 Alert policy name and description

The Category section is generic and an optional step.

2. To configure the alert policy for normal temperature alert, enter the message ID.
   - For CPU, the message ID is **CMET0022**.
   - For GPU, the message ID is **CMET0019**.



Create Alert Policy

Enter message IDs or Import from file

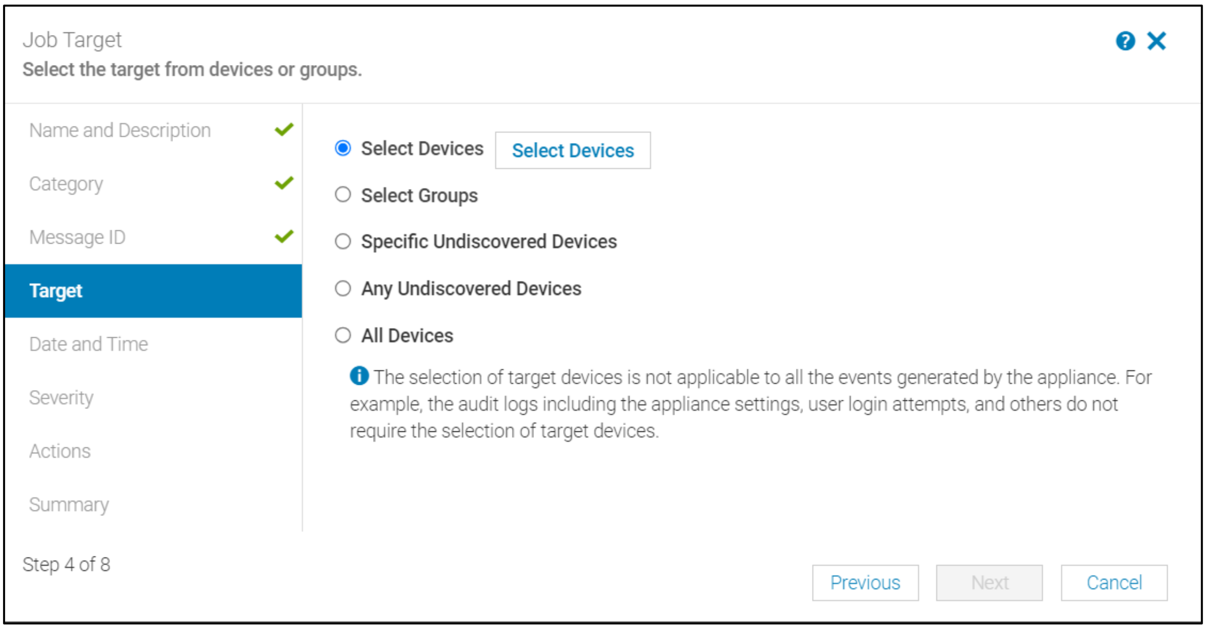
○ File

● Message IDs: CMET0022

Step 3 of 8

Figure 18 Alert policy message ID

3. In the **Target** section, select the target devices on which the critical alert policy is applied and requires a recovery.



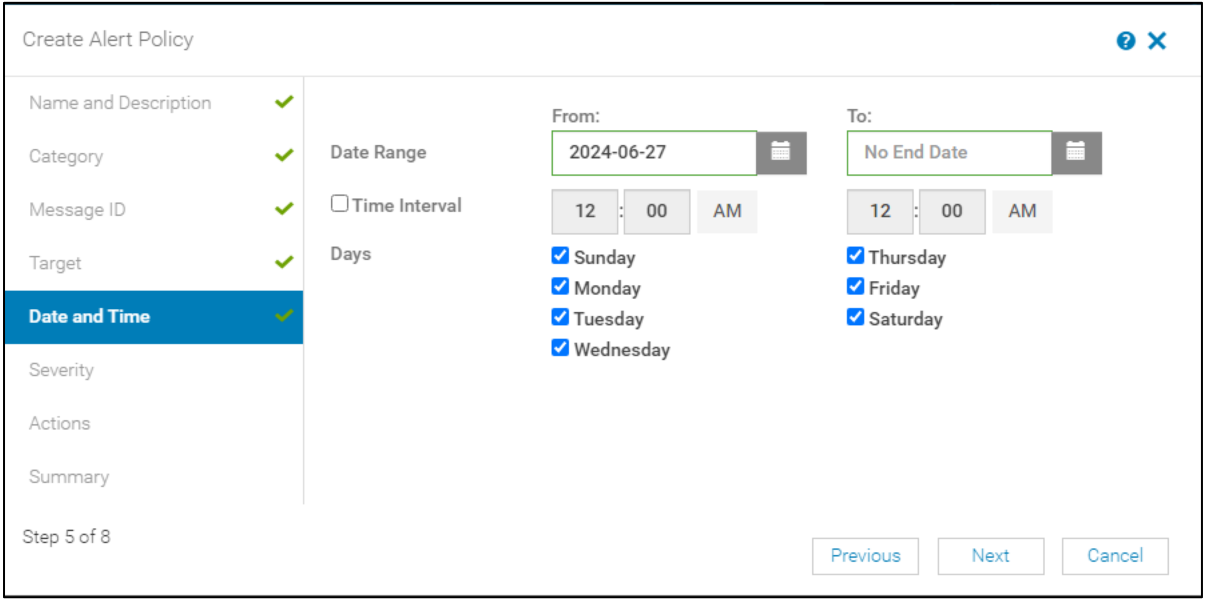
Select the target from devices or groups.

● Select Devices
○ Select Groups
○ Specific Undiscovered Devices
○ Any Undiscovered Devices
○ All Devices

The selection of target devices is not applicable to all the events generated by the appliance. For example, the audit logs including the appliance settings, user login attempts, and others do not require the selection of target devices.

Figure 19 Alert policy target

It is recommended to use the default date and time settings for a perpetual policy.



Date Range From: 2024-06-27 To: No End Date

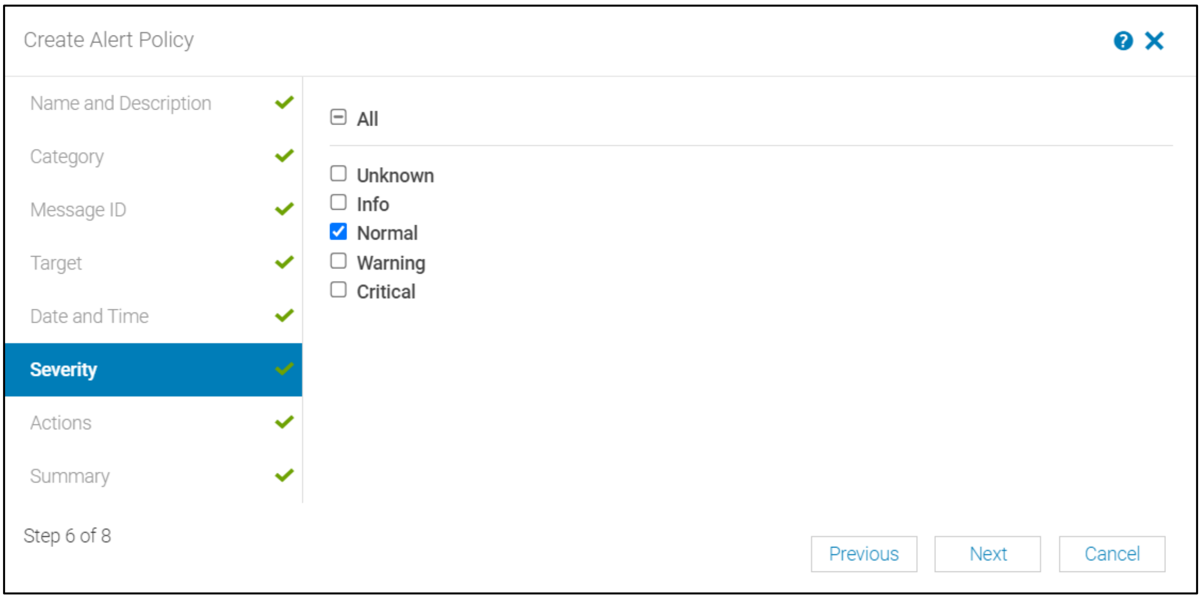
□ Time Interval From: 12 : 00 AM To: 12 : 00 AM

Days

☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

Figure 20 Alert policy date and time selection

4. Select the severity level as **Normal** for the alert.

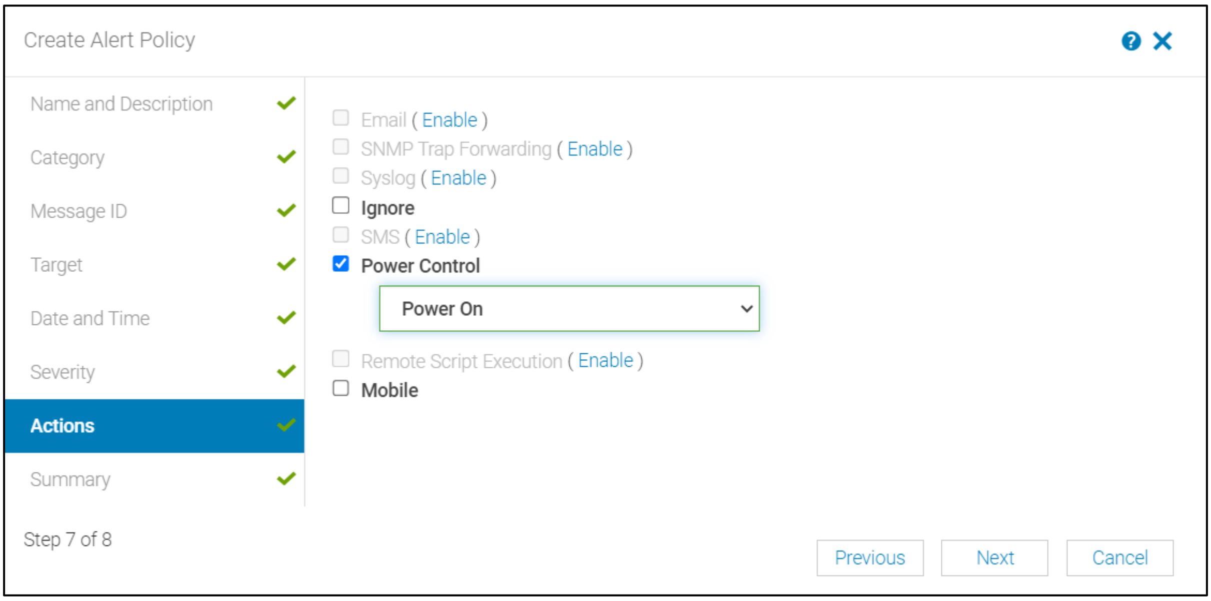


⊟ All

☐ Unknown
☐ Info
☑ Normal
☐ Warning
☐ Critical

Figure 21 Alert policy severity selection

5. In the **Actions** section, select the **Power Control** option as **Power On** to power on the target devices after receiving normal alert that are generated on relevant CPU or GPU components.

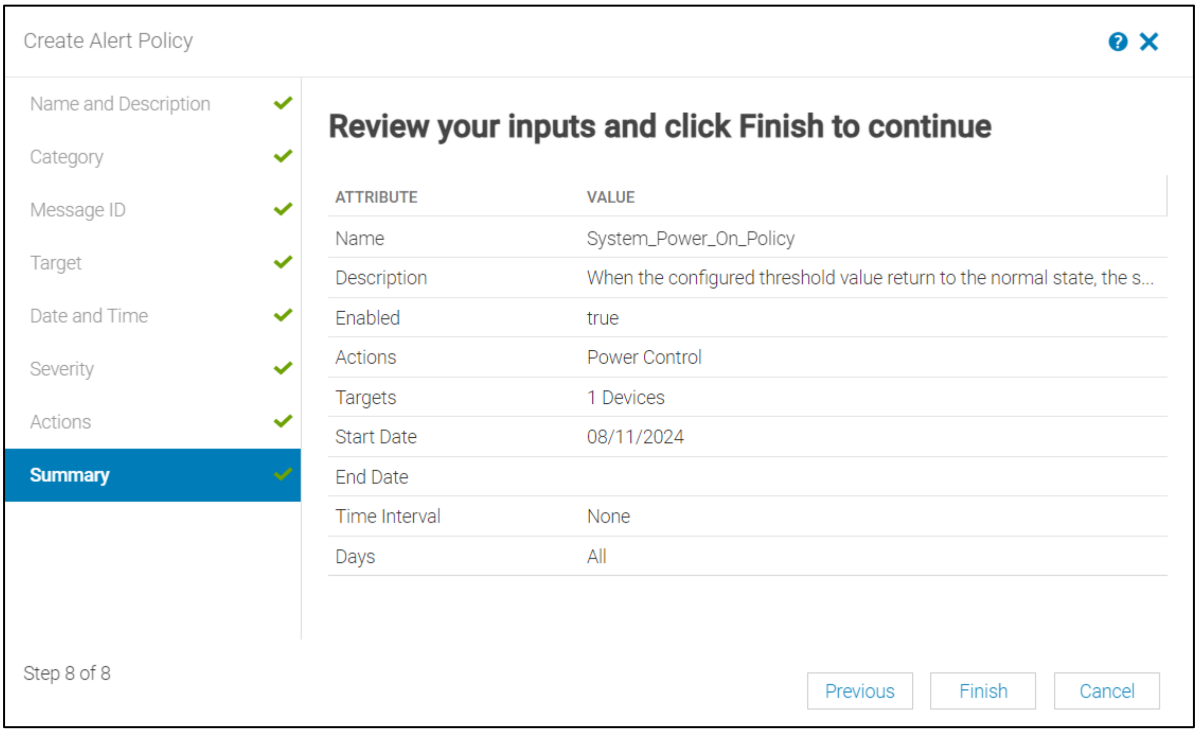


☐ Email (Enable)
☐ SNMP Trap Forwarding (Enable)
☐ Syslog (Enable)
☐ Ignore
☐ SMS (Enable)
☑ Power Control
Power On
☐ Remote Script Execution (Enable)
☐ Mobile

Figure 22 Alert policy actions

The **Summary** section displays all the details of the alert policy to be reviewed before creation.

6. To update any values, go to the respective page and update it.
7. Click **Finish** to complete the Alert Policy creation for normal alert.



Review your inputs and click Finish to continue

ATTRIBUTE	VALUE
Name	System_Power_On_Policy
Description	When the configured threshold value return to the normal state, the s...
Enabled	true
Actions	Power Control
Targets	1 Devices
Start Date	08/11/2024
End Date	
Time Interval	None
Days	All

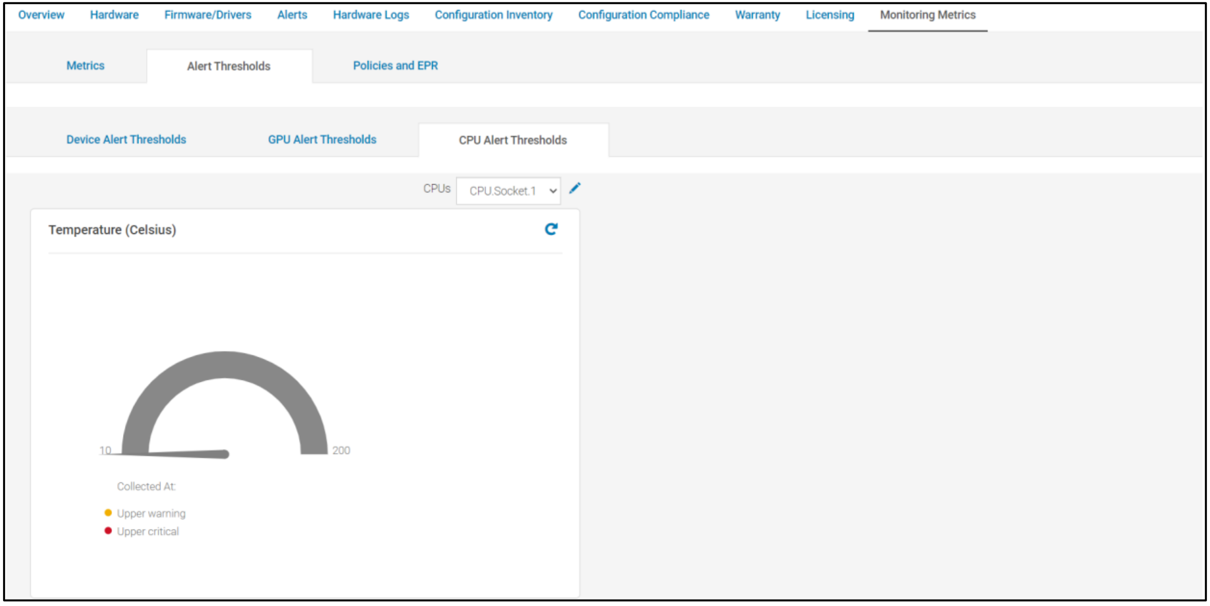
Step 8 of 8

Figure 23 Alert policy summary

4.1.2 Configure component-level threshold

You can configure the temperature threshold of CPU or GPU components of a device after the policy is created. See the following example for CPU (for GPU, the steps are similar):

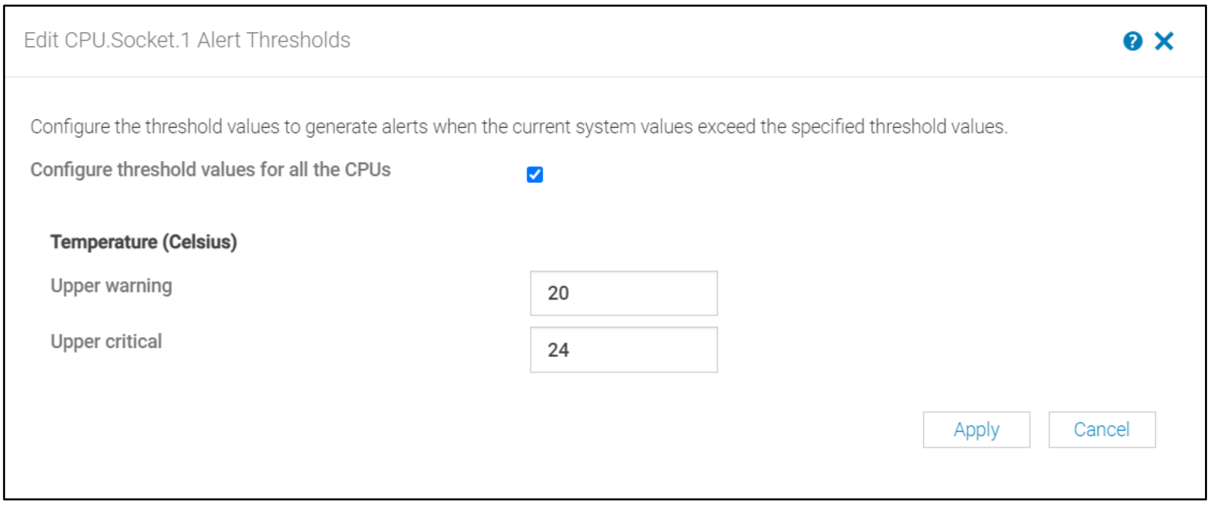
To configure threshold for CPU, go to the **Monitoring Metrics → Alert Thresholds → CPU Alert Thresholds** tab. For GPU, go to the **GPU Alert Thresholds** tab.



CPUs CPU.Socket.1

Figure 24 CPU threshold page

1. Click the Edit icon to configure the threshold value.
2. You can configure both the warning and critical values for temperature, or just one of them. You can configure the same for all the available components by selecting the **Configure threshold values for all CPUs** check box.
3. Click **Apply**.



Edit CPU.Socket.1 Alert Thresholds

Configure the threshold values to generate alerts when the current system values exceed the specified threshold values.

Configure threshold values for all the CPUs ☑

Temperature (Celsius)

Upper warning 20

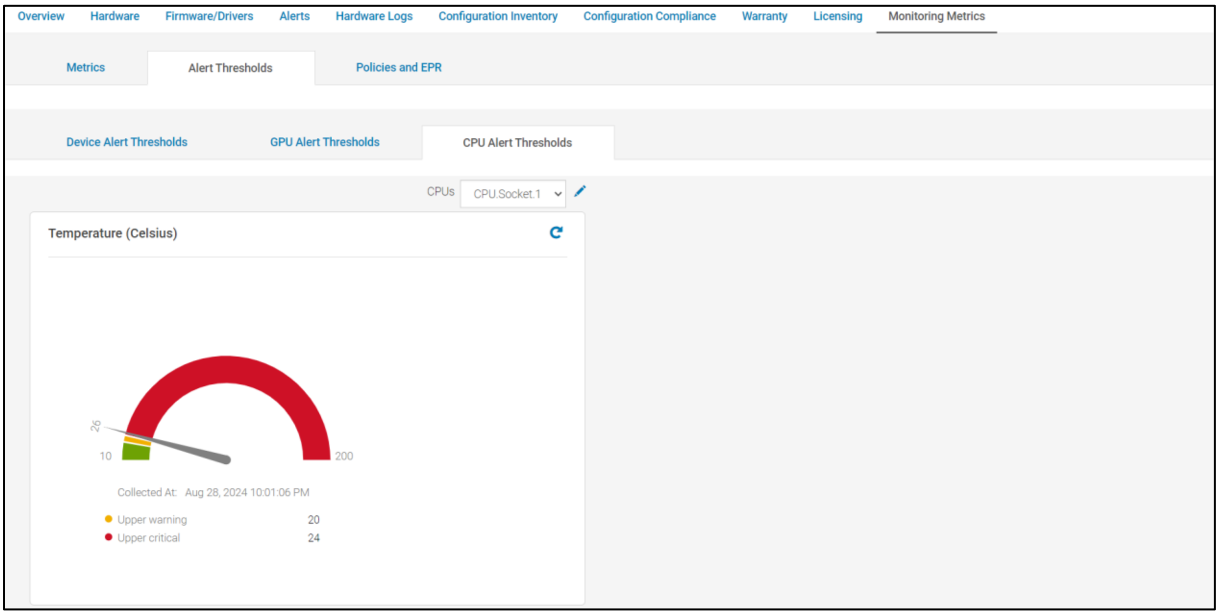
Upper critical 24

Figure 25 Configure CPU threshold

4.1.3 Evaluate threshold values

4.1.3.1 Threshold violation

1. After configuring the value, if the CPU or GPU temperature metrics exceed the configured threshold, you receive a critical alert. Additionally, the threshold violation status can be viewed in a threshold graph in the **CPU Alert Thresholds** tab for CPU and in the **GPU Alert Thresholds** tab for GPU.



CPUs CPU.Socket.1

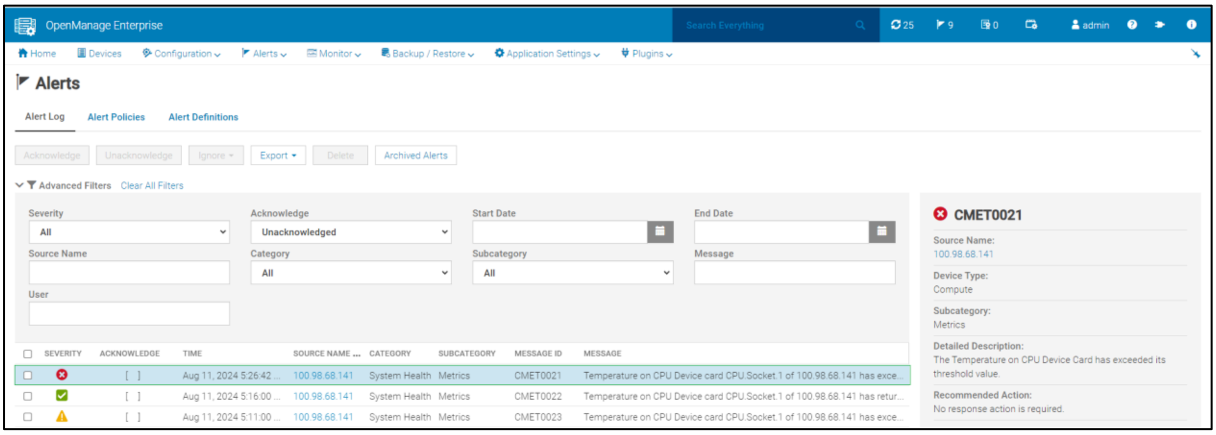
Collected At: Aug 28, 2024 10:01:06 PM

● Upper warning 20

● Upper critical 24

Figure 26 CPU threshold graph

2. View the violation alert on the **Alert Log** page under the **Alerts** tab.



Severity: All

Acknowledge: Unacknowledged

Start Date:

End Date:

Source Name:

Category: All

Subcategory: All

Message:

User:

☐	SEVERITY	ACKNOWLEDGE	TIME	SOURCE NAME ...	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
☐	☒	[ ]	Aug 11, 2024 5:26:42 ...	100.98.68.141	System Health	Metrics	CMET0021	Temperature on CPU Device card CPU.Socket.1 of 100.98.68.141 has exce...
☐	☑	[ ]	Aug 11, 2024 5:16:00 ...	100.98.68.141	System Health	Metrics	CMET0022	Temperature on CPU Device card CPU.Socket.1 of 100.98.68.141 has retur...
☐	⚠	[ ]	Aug 11, 2024 5:11:00 ...	100.98.68.141	System Health	Metrics	CMET0023	Temperature on CPU Device card CPU.Socket.1 of 100.98.68.141 has exce...

☒ CMET0021

Source Name:
100.98.68.141

Device Type:
Compute

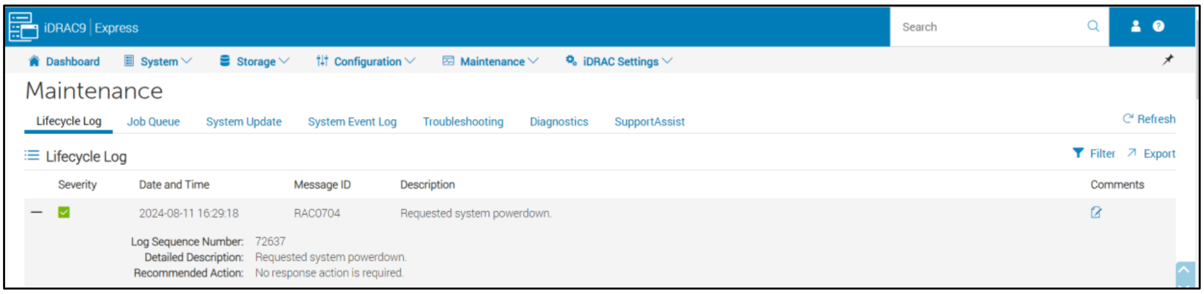
Subcategory:
Metrics

Detailed Description:
The Temperature on CPU Device Card has exceeded its threshold value.

Recommended Action:
No response action is required.

Figure 27 Alert log page

3. After the violation becomes effective, you can log in to the iDRAC web interface for which the policy is violated and view the log which shows the shutdown message as per the policy action.

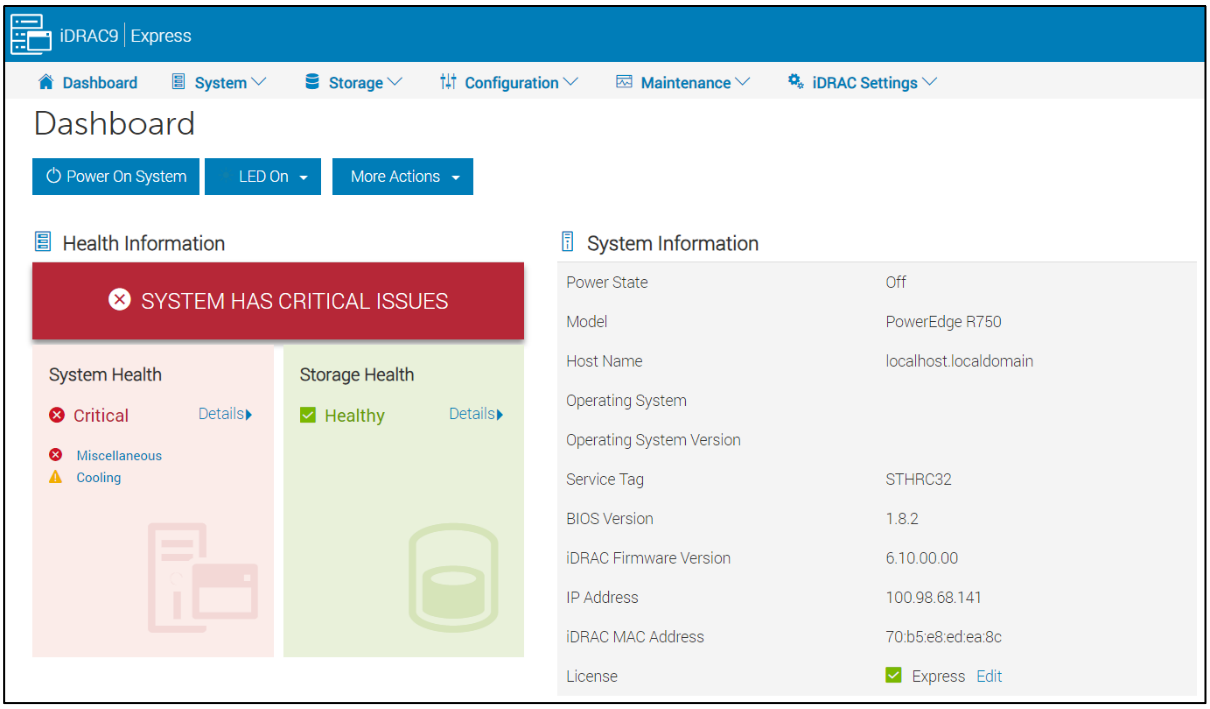


	Severity	Date and Time	Message ID	Description	Comments
—	☑	2024-08-11 16:29:18	RAC0704	Requested system powerdown.	

Log Sequence Number: 72637
Detailed Description: Requested system powerdown.
Recommended Action: No response action is required.

Figure 28 iDRAC log data after power off

View the system power state on the iDRAC page.

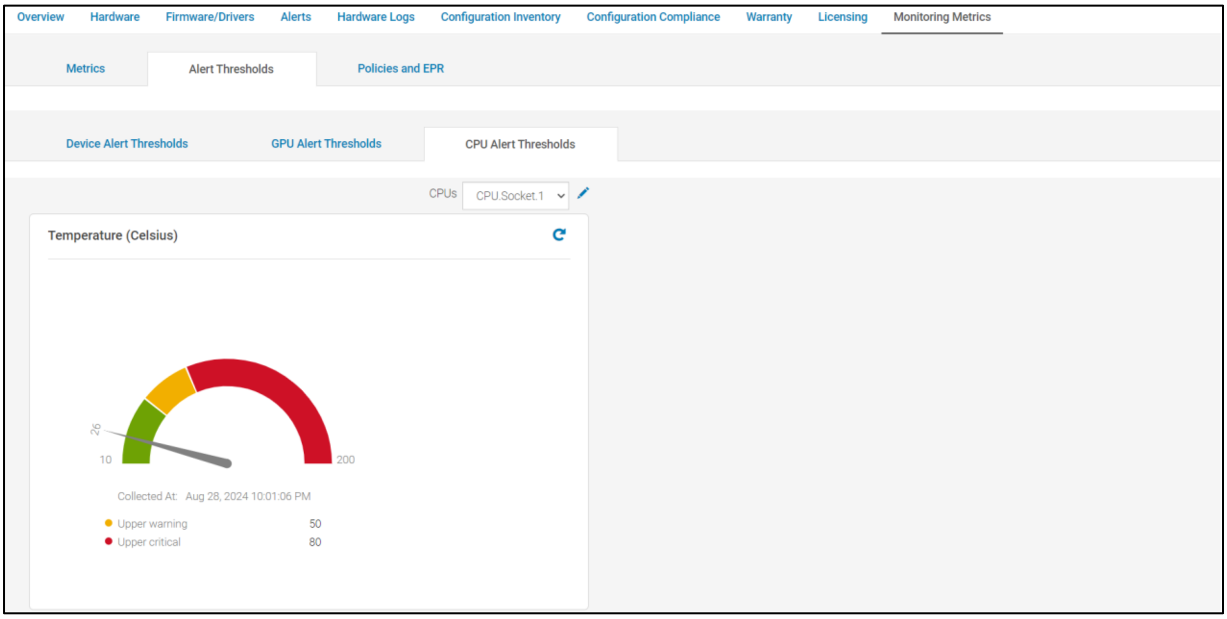


Power State	Off
Model	PowerEdge R750
Host Name	localhost.localdomain
Operating System	
Operating System Version	
Service Tag	STHRC32
BIOS Version	1.8.2
iDRAC Firmware Version	6.10.00.00
IP Address	100.98.68.141
iDRAC MAC Address	70:b5:e8:ed:ea:8c
License	☑ Express Edit

Figure 29 iDRAC power state

4.1.3.2 Threshold violation recovery

1. When CPU or GPU temperature metrics return to the configured threshold normal limit, you receive a normal alert. Additionally, the status gets updated in the threshold graph in the **CPU Thresholds Alert** tab for CPU and in the **GPU Thresholds Alert** tab for GPU.

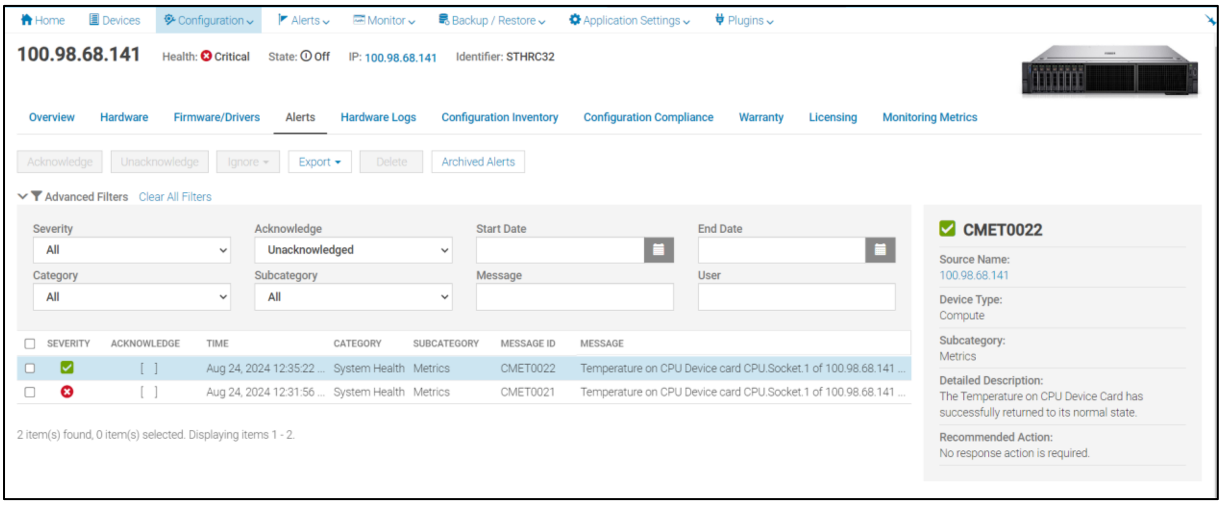


Collected At: Aug 28, 2024 10:01:06 PM

● Upper warning	50
● Upper critical	80

Figure 30 CPU threshold graph

2. View the normal alert on the **Alert Log** page in the **Alerts** tab.



100.98.68.141 Health: ☒ Critical State: Off IP: 100.98.68.141 Identifier: STHRC32

Severity: All
Acknowledge: Unacknowledged
Start Date:
End Date:
Category: All
Subcategory: All
Message:
User:

□	SEVERITY	ACKNOWLEDGE	TIME	CATEGORY	SUBCATEGORY	MESSAGE ID	MESSAGE
□	✓	[ ]	Aug 24, 2024 12:35:22 ...	System Health	Metrics	CMET0022	Temperature on CPU Device card CPU.Socket.1 of 100.98.68.141 ...
□	☒	[ ]	Aug 24, 2024 12:31:56 ...	System Health	Metrics	CMET0021	Temperature on CPU Device card CPU.Socket.1 of 100.98.68.141 ...

2 item(s) found, 0 item(s) selected. Displaying items 1 - 2.

✓ CMET0022

Source Name:
100.98.68.141

Device Type:
Compute

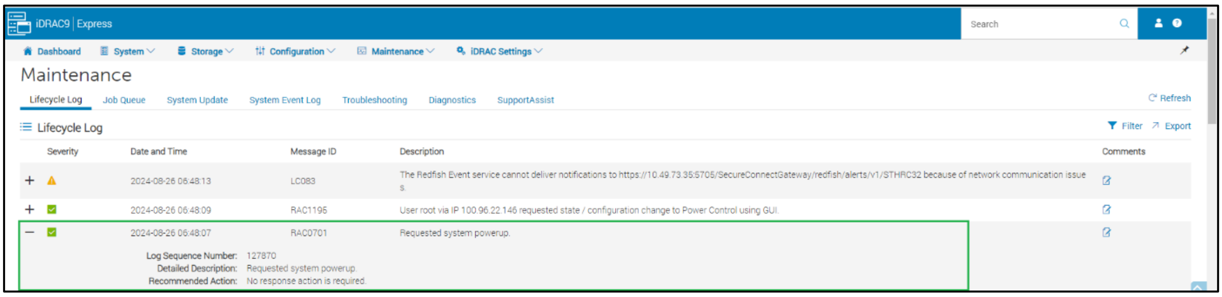
Subcategory:
Metrics

Detailed Description:
The Temperature on CPU Device Card has successfully returned to its normal state.

Recommended Action:
No response action is required.

Figure 31 Alert log page

3. You can log in to the iDRAC web interface for which the normal alert policy is enabled and view the log which shows the power-on message as per the policy action.

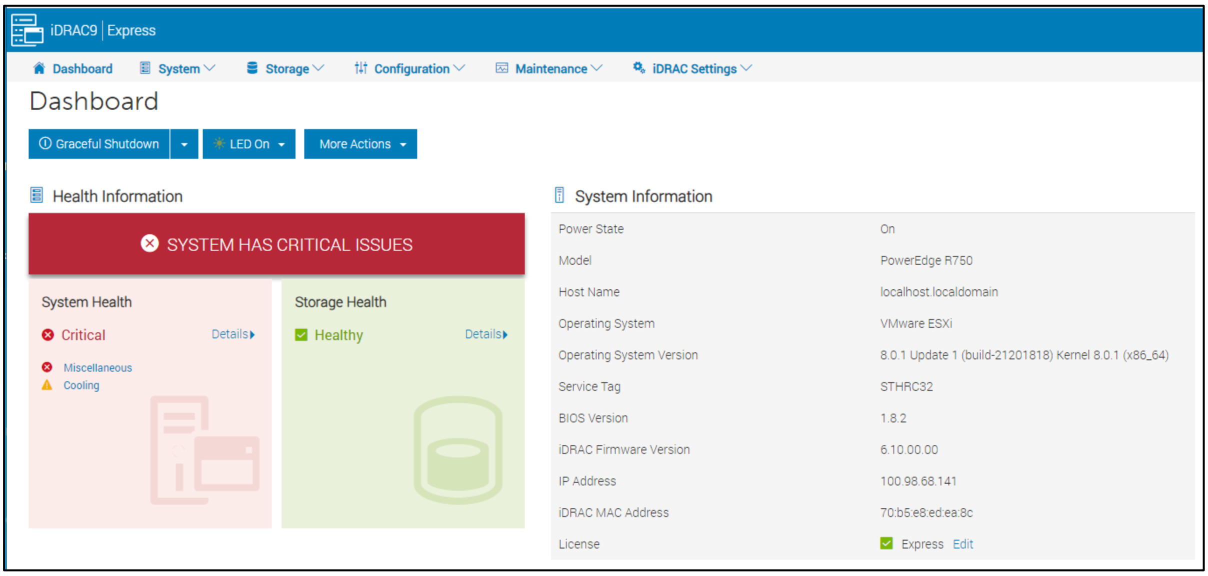


	Severity	Date and Time	Message ID	Description	Comments
+	⚠	2024-08-26 06:48:13	LC083	The Redfish Event service cannot deliver notifications to https://10.49.73.35:5705/SecureConnectGateway/redfish/alerts/v1/STHRC32 because of network communication issue s.	
+	✓	2024-08-26 06:48:09	RAC1195	User root via IP 100.96.22.146 requested state / configuration change to Power Control using GUI.	
–	✓	2024-08-26 06:48:07	RAC0701	Requested system powerup.	

Log Sequence Number: 127870
Detailed Description: Requested system powerup.
Recommended Action: No response action is required.

Figure 32 iDRAC log data after power on

View the system power state (on) on the iDRAC page.



Power State	On
Model	PowerEdge R750
Host Name	localhost.localdomain
Operating System	VMware ESXi
Operating System Version	8.0.1 Update 1 (build-21201818) Kernel 8.0.1 (x86_64)
Service Tag	STHRC32
BIOS Version	1.8.2
iDRAC Firmware Version	6.10.00.00
IP Address	100.98.68.141
iDRAC MAC Address	70:b5:e8:ed:ea:8c
License	✓ Express Edit

Figure 33 iDRAC power state

5 Conclusion

Power Manager plug-in uses the Alert Monitoring feature of OpenManage Enterprise by introducing device and component-level power and temperature threshold violation alerts. It also supports reception of alerts sent by Power Distribution Unit (PDU) and Uninterruptible power supply (UPS) devices. Alert Policy feature in OpenMange Enterprise can be used to execute specific actions in response to these alerts.

6 Appendix

Message ID	Description
CMET0008	Device power has exceeded the configured Critical threshold
CMET0017	Device Temperature has exceeded the configured Critical threshold
CMET0004	Device Power has exceeded the configured Warning threshold
CMET0013	Device Temperature has exceeded the configured Warning threshold
CMET0015	Device Power/Temperature has reached to Normal threshold
CMET0009	GPU Power has exceeded the configured Critical threshold
CMET0018	GPU Temperature has exceeded the configured Critical threshold
CMET0011	GPU Power has exceeded the configured Warning threshold
CMET0020	GPU Temperature has exceeded the configured Warning threshold
CMET0010	GPU Power has reached the configured Normal threshold
CMET0019	GPU Temperature has reached the configured Normal State
CMET0021	CPU Temperature has exceeded the configured Critical threshold
CMET0022	CPU Temperature in Normal State
CMET0023	CPU Temperature in Warning State

7 Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

7.1 Related resources

- Knowledge Base for Dell OpenManage Enterprise HTML
- Dell OpenManage Enterprise Power Manager Version 3.3 User’s Guide PDF HTML
- Dell OpenManage Enterprise Power Manager RESTful API Guide version 3.3 HTML
- Dell OpenManage Enterprise Power Manager 3.3 Release Notes PDF