

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Version 7.3 for Microsoft System Center Operations Manager

User's Guide

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: About Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM.....	6
New features.....	7
What's changed.....	7
Chapter 2: Support Matrix for Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	8
User roles necessary for using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	9
Chapter 3: Installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	10
Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM.....	10
Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack on multiple SCOM Management Servers.....	11
Management features imported into SCOM console after installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	11
Repair installation issues of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	11
Chapter 4: Discover and monitor PowerEdge servers and rack workstations on the SCOM console.....	13
Scalable and detailed editions of monitoring PowerEdge servers and rack workstations.....	13
Discovery and classification of PowerEdge servers and rack workstations	13
Discover PowerEdge servers by using SCOM Agent Management.....	14
Monitoring Dell EMC PowerEdge Servers in the SCOM console.....	14
View options for Dell EMC Server and Rack Workstation monitoring feature.....	14
Chapter 5: Discover and monitor DRACs on the SCOM console.....	18
Introduction to the monitoring features in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for DRACs.....	18
Discovery and classification of DRACs.....	18
Discover and enable DRAC devices.....	19
Monitoring DRACs.....	19
View options for DRAC monitoring feature.....	19
Chapter 6: Supported tasks on the SCOM console.....	22
Run Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature-based tasks on SCOM.....	22
Tasks run on Dell EMC devices by using the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features.....	22
Check connection to the nodes.....	23
View warranty information of PowerEdge servers.....	23
Launch OMSA on monolithic servers using the SCOM console.....	23
Launch iDRAC using the SCOM console.....	24

Launch Remote Desktop on monolithic servers using the SCOM console.....	24
Clear Embedded Server Management (ESM) logs.....	24
Power management-related tasks.....	24
Chapter 7: Generating reports.....	25
View reports about PowerEdge servers on the SCOM console.....	25
Generate Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack reports on the SCOM console.....	25
Chapter 8: Upgrading Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	27
Upgrade to latest version of the OMIMSSC appliance for SCOM.....	27
Upgrade from previous versions of DSMPS.....	27
Chapter 9: Uninstalling Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	29
Uninstall using the Windows Control Panel.....	29
Uninstall using installer file.....	29
Chapter 10: Reference topics.....	30
Monitoring features supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	30
Dell EMC Server and Rack Workstation Monitoring feature using OMSA.....	30
DRAC Monitoring feature.....	33
Configuring the monitoring features by using the Feature Management Dashboard.....	34
Severity levels of discovered devices.....	38
Discovery features supported in the monitoring of PowerEdge servers and rack workstations using OMSA.....	38
Discovery features supported for monitoring DRACs.....	39
Hardware components monitored by different monitoring features.....	39
View options provided by the monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.....	42
Alert views displayed by different monitoring features.....	42
Diagram views displayed by different monitoring features.....	42
State views displayed by different monitoring features.....	46
Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Unit Monitors.....	46
Scalable Edition Unit monitors in the monitoring feature for PowerEdge servers and workstations using OMSA.....	46
Detailed Edition Unit monitors in the monitoring feature for PowerEdge servers and workstations using OMSA.....	47
Unit monitors in the monitoring feature for DRACs.....	49
Event rules used by different monitoring features.....	49
Chapter 11: Troubleshooting.....	51
Data is not displayed on the Feature Management Dashboard.....	51
A task run on the Feature Management Dashboard fails.....	51
Feature Management alerts.....	52
The Management Server (MS) is not functioning, and therefore, tasks associated with it cannot be completed (Health Service of the Feature Management Host Server is nonfunctional).....	52

Chapter 12: Additional resources.....	54
Chapter 13: Accessing support content from the Dell EMC support site.....	55
Chapter 14: Contacting Dell Technologies.....	56
Appendix A: Glossary.....	57
Appendix B: Additional topics.....	58
Identify device and device power status by using identification LEDs.....	58
Migrate from Dell Server Management Pack Suite Version 6.0 for Microsoft SCOM.....	59
Configure SCOM to monitor traps and trap-based unit monitors.....	59
Create Run-As-Account for SNMP monitoring.....	60
Associate multiple Run-As accounts.....	60
Install Web Services Management (WS-Man) and SMASH device template.....	61
Associate Run-As Account task—Dell EMC Server and Rack Workstation Monitoring feature.....	61

About Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM

The Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM enables agent-based discovery and monitoring of PowerEdge servers, rack workstations, and iDRACs through OMSA. The Dell EMC-specific views on the SCOM console is used to observe and analyze the device status in a network.

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM is a self-extracting executable file—*Dell EMC Server Management Pack Suite <Version>_XXX.exe*—where, XXX is the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack version release number. You can download the executable file and the latest documents from the Dell Technologies support site.

CAUTION: You must perform the tasks that are described in this user's guide only if you have firsthand working experience with the supported SCOM console versions and in using Microsoft Windows operating system. Else, it can result in lost or corrupted data.

Monitoring features supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM enables you to discover and monitor the following Dell EMC devices:

- Dell EMC PowerEdge servers—Using the Dell EMC Servers and Rack Workstations Monitoring feature (OMSA agent-based).
 - **NOTE:** Dell EMC Server and Rack Workstation Monitoring feature supports monitoring of PowerEdge servers having Windows Server operating systems.
- Supported Dell Precision Racks
- Integrated Dell Remote Access Controllers—Discovery and monitoring of supported iDRAC devices—12th and 13th generation only. SNMP and PET traps for iDRAC devices is supported by the DRAC monitoring feature.

Comparing the monitoring features offered by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack and OMIMSSC appliance for SCOM

- **Discovery and monitoring features offered by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack**
 - Discovery and monitoring of PowerEdge Servers and Rack Workstations using OMSA (agent-based) and iDRAC devices—12th and 13th generation only.
- **Discovery and monitoring features offered by the OMIMSSC appliance for SCOM**
 - Discovery and monitoring of PowerEdge Servers and Rack Workstations using iDRAC agent-free discovery, Chassis, and Network Switches. For more information about deploying and using the OMIMSSC appliance for SCOM, see the

Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User's Guide on the support site.

Topics:

- [New features](#)

New features

- Support for:
 - Update Rollup 3 for System Center Operations Manager 2019.
 - Update Rollup 10 for System Center Operations Manager 2016.
- Support for the following latest iDRAC9—based PowerEdge servers:
 - PowerEdge R7525, R6525, R7515, R6515
 - PowerEdge R750, R750xa, R650
 - PowerEdge C6525, C6520
 - PowerEdge MX750c
- Support for Version 10.0.1 of Dell EMC OpenManage Server Administrator (OMSA).

What's changed

- **Product name change**
 - The product name is changed to **Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for Microsoft System Center Operations Manager**. In the previous releases, the product name was referred to as **Dell EMC Server Management Pack Suite for Microsoft System Center Operations Manager**.
- **Installer changes**
 - The installation screens display the updated name of the product—**Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for Microsoft System Center Operations Manager**.
 - The monitoring features supported by the product are listed in the installation screens.
- The Server and Rack Workstation monitoring feature using iSM-WMI and its related details and monitoring views are now provided in the *Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) User's Guide* available on the support site.

Support Matrix for Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Before installing and configuring Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack, ensure that the following software and hardware requirements are met.

Table 1. Support Matrix for Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Supported software and hardware	Requirements and versions	
Microsoft System Center— Operations Manager (SCOM)	<p>One of the following SCOM build numbers must be already installed on the management server:</p> <ul style="list-style-type: none"> • SCOM 1807 • SCOM 1801 • SCOM 2012 R2 • SCOM 2016 • SCOM 2019 <p>i NOTE: On systems running the Nano server version of Windows Server 2016 operating system, apply the <i>Update Rollup 1 for Microsoft System Center 2016 - Operations Manager</i> agent package that is provided in the Microsoft knowledge base article KB3190029. For more information, see https://support.microsoft.com/en-us/help/3190029/update-rollup-1. You can upgrade to the latest versions of SCOM from previous versions as per Microsoft guidelines. For information about the supported upgrade scenarios, see the Microsoft System Center documentation.</p>	
Windows requirements for installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack on the Management Server with the SCOM console	<ul style="list-style-type: none"> • Enable the following Windows firewall rules: <ul style="list-style-type: none"> ○ SCOM SNMP Response ○ SCOM SNMP Trap Listener ○ SCOM Ping Response • Windows PowerShell 3.0 or later, if your system is running Windows Server 2012 R2 operating system. 	
Management Server (MS) requirements		
Operating systems	<ul style="list-style-type: none"> • For SCOM 2019, see https://www.docs.microsoft.com/en-us/system-center/scom/?view=sc-om-2019. • For SCOM 2016, see https://www.docs.microsoft.com/en-us/system-center/scom/?view=sc-om-2016. • For SCOM 2012 R2, see https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/hh546785(v=sc.12). 	
Managed System requirements		
Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack features	Supported software and hardware	Requirements and versions
Dell EMC Server and Rack Workstation Monitoring	Dell EMC OpenManage Server Administrator (OMSA)	Versions 10.0.1, 9.4, and 9.3
DRAC Monitoring Feature	iDRAC8 with Lifecycle Controller Modular and Monolithic	Firmware version 2.xx.xx.xx

Table 1. Support Matrix for Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack (continued)

Supported software and hardware	Requirements and versions	
	iDRAC7 Modular and Monolithic	Firmware versions 2.xx.xx.xx and 1.6x.6x
	iDRAC6 Monolithic	Firmware versions 2.92 and 2.85
	iDRAC6 Modular	Firmware versions 3.80 and 3.65

Topics:

- [User roles necessary for using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack](#)

User roles necessary for using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

User must be a member of the following:

- Domain user group
- Local administrator group on the SCOM Management Server
- Operations Manager administrator group

Installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Prerequisites: Before you begin with the installation of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM, ensure that all the software and hardware requirements and user privileges are configured and available. See [Support Matrix for Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack](#) on page 8.

Topics:


- [Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM](#)
- [Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack on multiple SCOM Management Servers](#)
- [Management features imported into SCOM console after installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack](#)
- [Repair installation issues of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack](#)

Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM

Steps

1. From the Dell Technologies support site, download *Dell_EMC_Server_Management_Pack_<version>_XXX.exe*—where XXX is the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack version release number.
2. To extract contents of the self-extractable file, run the EXE file.
3. Launch the *Dell_EMC_Server_Management_Pack_Suite.exe* file from the extracted location. The welcome screen is displayed.
4. Click **Next**. The license agreement is displayed.
5. To continue the installation, read through the license terms and accept.
6. Click **Next**.
7. If you want to change the default location of the installation folder, click **Change > Next**.
8. Click **Install**.
9. On the **Install Shield Wizard Completed** screen, click **Finish**.
By default, the management packs are installed in the location: `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<release>`, where release is the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack version number (For example, 7.3 or 7.2).

Results

 **NOTE:** A log file containing the installation information is generated after the installation of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack. The log file is available in the folder where the EXE file is extracted.

Install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack on multiple SCOM Management Servers

Steps

1. Import the management packs by using the **Dell EMC Feature Management Dashboard** or the **SCOM Import Management Pack** wizard on any of the SCOM Management Server. SCOM automatically distributes the management packs to all the Management Servers.
2. To receive traps, add the Management Server that is used for discovering the Dell EMC devices to the Dell EMC device's trap destination list.
 - NOTE:** Trap destination is automatically configured for the Dell EMC devices that are discovered and monitored through Dell EMC Server and Rack Workstation Monitoring (Licensed) feature. To be able to receive SNMP alerts from devices discovered through the iDRAC access via the Host OS feature, you must install SNMP services on the Managed Node and set the Management Server IP address as the trap destination in the SNMP Services.

Management features imported into SCOM console after installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

The following monitoring features are automatically imported into the SCOM console after you install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack:

- Dell EMC Server and Rack Workstation Monitoring feature—Using OMSA agent-based.
- Dell EMC Feature Management Pack—The Feature Management Dashboard is displayed under **Monitoring > Dell EMC** of the SCOM console.

NOTE: The Dell EMC Server and Rack Workstation Monitoring feature of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack requires the installer to run on all the SCOM Management Servers that are used to monitor the PowerEdge servers.

Repair installation issues of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

About this task

After installing Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack, if you face any installation issues and you are unable to run the application, then use the **Repair** feature available in the installation file to resolve any issues that may have occurred during the installation process.

Steps

1. Run the `Dell_EMG_Server_Management_Pack_Suite.exe` file from the extracted location. The welcome screen is displayed.
2. Click **Next**. The **Program Maintenance** screen is displayed.
3. Select **Repair**, and then click **Next**. The **Ready to Repair the Program** screen is displayed.

4. Click **Install**.

The status bar indicates the installation status. After the installation is completed, the **Installation Completed Successfully** screen is displayed.

5. Click **Finish**.

Example

 **NOTE:** The **Repair** option is not available under **Add/Remove Programs** in the Control Panel.

Discover and monitor PowerEdge servers and rack workstations on the SCOM console

Topics:

- Scalable and detailed editions of monitoring PowerEdge servers and rack workstations
- Discovery and classification of PowerEdge servers and rack workstations
- Discover PowerEdge servers by using SCOM Agent Management
- Monitoring Dell EMC PowerEdge Servers in the SCOM console

Scalable and detailed editions of monitoring PowerEdge servers and rack workstations

The following table describes the environment in which you can use the Scalable and Detailed Edition features.

Table 2. Scalable and detailed editions of PowerEdge servers and rack workstations monitoring feature

Feature	Scalable Edition	Detailed Edition
Dell EMC Server and Rack Workstation Monitoring feature	<ul style="list-style-type: none"> • Inventory and monitoring of component groups. Also, displays the availability of iDRAC. • Reports—Only OpenManage Windows event log report is available. 	<ul style="list-style-type: none"> • Detailed inventory and health monitoring of individual components. • View metrics of memory, processors, network interfaces, sensors, storage controllers, disks, and virtual disks. Also, displays BIOS information. • Reports—Availability of BIOS configuration, firmware and driver version, and RAID configuration reports.

Discovery and classification of PowerEdge servers and rack workstations

Using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack, you can discover and classify Dell EMC PowerEdge Servers (Monolithic, Modular, and sleds) and supported Dell Precision Racks. The following table lists the hardware discovery and grouping that is supported by the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature.

Table 3. Dell EMC hardware discovery and grouping using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Group	Diagram View	Hardware Type
Dell EMC PowerEdge Servers	<ul style="list-style-type: none"> • Dell EMC Monolithic Servers • Dell EMC Modular Servers • Dell EMC Sled Servers 	<ul style="list-style-type: none"> • PowerEdge servers • PowerVault servers
Dell EMC Rack Workstations	Dell EMC Rack Workstation Diagram	Dell EMC Precision Racks

Discover PowerEdge servers by using SCOM Agent Management

About this task

Discover PowerEdge servers in the **Agent Managed** view under the **Administration** section of the SCOM console.

Steps

1. In the left pane of the SCOM console, select **Administration**.
2. In the left pane, click **Discovery Wizard**.
3. In the working pane, select **Windows computers**, and then complete the tasks that are prompted by the **Computer and Device Management Wizard**.

For more information, see the [Microsoft SCOM documentation](#).

NOTE: In a distributed environment, the discovery of devices may not be successful. Ensure all the conditions displayed in the error message are verified, and then discover the devices.

Results

NOTE: The installer automatically imports the Dell EMC Server and Rack Workstation Monitoring management packs into the SCOM console. If the installer fails to install the management packs, then import the management packs using the **Import Management Packs** wizard or the **Dell EMC Feature Management Dashboard** on the SCOM console.

NOTE: Dell EMC PowerEdge Servers that do not have Dell OpenManage Server Administrator (OMSA) installed or are running an unsupported OMSA version are grouped as Dell Unmanaged Devices.

Monitoring Dell EMC PowerEdge Servers in the SCOM console

The **Monitoring** pane of the SCOM console is used to select views that provide complete health information about the discovered Dell EMC PowerEdge Servers. The [Severity Level Indicators](#) helps you to indicate the health of the Dell EMC PowerEdge Servers on the network.

It includes monitoring the health of monolithic and modular servers, and supported Dell Precision Racks and their components, both at regular intervals and on occurrence of events.

View options for Dell EMC Server and Rack Workstation monitoring feature

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack provides the following types of views for monitoring servers and rack workstations by selecting **Monitoring > Dell EMC** on the SCOM console:

- [Alert view in the monitoring feature for PowerEdge servers and rack workstations](#) on page 14
- [Diagram views in the monitoring feature for PowerEdge servers and rack workstations](#) on page 15
- [Performance and power monitoring views in the monitoring feature for PowerEdge servers and rack workstations](#) on page 15
- [State views in the monitoring feature for PowerEdge servers and rack workstations](#) on page 17

Alert view in the monitoring feature for PowerEdge servers and rack workstations

The Alert View is available for managing hardware and storage events from the Dell EMC servers and rack workstations, which are received from OpenManage Server Administrator (OMSA). Link-up and Link-down alerts for events that are received from the Broadcom and Intel Network Interface Cards (NICs) are displayed.

To view the alert views that are displayed by the monitoring feature of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for PowerEdge servers and workstations:

1. On the SCOM console, select **Monitoring**.
2. Expand **Dell EMC > Dell EMC Alerts Views**. The alert views displayed by the monitoring feature for PowerEdge servers and rack workstations are:
 - **Dell EMC Network Interface Alerts Views**—Link-up and Link-down alerts from the discovered NICs.
 - **Dell EMC Server and Rack Workstation Alerts Views**—OMSA alerts from the Dell Server and Rack Workstations.
 - **Dell EMC Rack Workstation Alert Views**
 - **Dell EMC Network Interface Alerts**—Link-up and Link-down alerts from the discovered NICs.
 - **Dell EMC Rack Workstation Alerts**—OMSA alerts from Rack Workstations.
3. Select the required Alert View. In the right pane, alerts that meet the criteria—such as alert severity, resolution state, or alerts that are assigned to you—are displayed.
4. Select an alert to view the details in the **Alert Details** section.

NOTE: By default, informational alerts are disabled. To enable informational alerts, run the **Set Informational Alerts On** task for the Server and Rack Monitoring feature on the **Dell EMC Feature Management Dashboard**.

Diagram views in the monitoring feature for PowerEdge servers and rack workstations

About this task

The Dell EMC Diagram Views offer a hierarchical and graphical representation of all Dell EMC PowerEdge servers and supported rack workstations on the network.

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC > Dell EMC Diagram Views**.
3. Go to the **Dell EMC Diagram Views** folder to view the available diagram views. See [Diagram views displayed by different monitoring features](#) on page 42.
4. Select a required **Dell EMC Diagram View** to view the hierarchical and graphical representation of the selected Dell EMC server or rack workstation in the right pane.
5. Select a component in the diagram to view its details in the **Detail View** section.

Performance and power monitoring views in the monitoring feature for PowerEdge servers and rack workstations

About this task

To view the Dell EMC performance and power monitoring views on the SCOM console:

Steps

1. In the left pane of the SCOM, select **Monitoring**.
2. In the **Monitoring** pane, expand **Dell EMC > Dell EMC Performance and Power Monitoring Views**.

The following Performance and Power Monitoring views are available:

- **Ambient Temperature (Centigrade)**
- **Amperage (Amps)**
- **Dell EMC Performance View**
- **Dell EMC Performance View (iSM)**
- **Dell EMC Server Performance View**
- **Disk Performance - iSM (%)**
- **Energy Consumption (kWh)**
- **Peak Amperage (Amps)**
- **Peak Power (Watts)**

- **Power Consumption (BTU/hr)**
- **Power Consumption (Watts)**

i **NOTE:** Power monitoring is applicable only for Dell EMC PowerEdge Servers with power monitoring capability for a particular attribute. It is enabled only when the detailed edition of Dell EMC Server and Rack Workstation Monitoring feature is present.

i **NOTE:** Disk Performance View - iSM (%) is disabled by default and appears only when the detailed edition of the Dell EMC Server and Rack Workstation Monitoring feature is installed and imported.

3. Select the counters from the individual performance views and select the time range for which the values are required. The data that is collected is represented in a graphical format for each system.

Next steps

A unit monitor monitors the performance counter over two successive cycles to check if it exceeds a threshold value. When the threshold value is exceeded, the Dell EMC PowerEdge Server changes state and generates an alert. This unit monitor is disabled by default. You can override (enable) the threshold values in the **Authoring** pane of the SCOM console. Unit monitors are available under **Dell Windows Server** objects for the Dell EMC Server and Rack Workstation Monitoring feature. To enable the threshold values of unit monitors, see [Enable performance and power monitoring unit monitors](#) on page 16.

To enable the PowerEdge server performance collection rules and for more information about the performance information collection, see [Enable PowerEdge server performance collection rules set on the SCOM console](#) on page 16.

Enable performance and power monitoring unit monitors

Steps

1. In the left pane of the SCOM console, select **Authoring**.
2. Expand **Management Pack Objects > Monitors**.
3. In the **Look for** field, search for **Performance**.
4. Right-click the unit monitor that you want to enable.
5. Select **Overrides > Override the Monitor**, and then select an option based on your requirement.
For example, to override the unit monitors for all objects of class: Dell Windows Server, select **For all objects of class: Dell Windows Server**.
The **Override Properties** screen is displayed.
6. Select **Enabled** and set the Override Value to True.
7. In the **Management Pack** section, select a management pack from the drop-down list.
To create a management pack, click **New** and complete the tasks prompted. For more information about creating management packs, see the Microsoft SCOM documentation.
8. Click **Apply**.

Enable PowerEdge server performance collection rules set on the SCOM console

About this task

By default, the server performance collection rules are disabled. To enable, perform the following actions:

Steps

1. In the left pane of the SCOM console, select **Authoring**.
2. Select **Rules** and in the **Look for** field, search for **Enriched**.
3. Right-click the rule that you want to enable, and then select **Overrides > Override the Monitor > For all objects of class**.

For example, to collect data about network interface of all Dell EMC systems, right-click the following rules:

- Total Transmitted Packets
- Received Bytes
- Total Received Packets
- Transmitted Bytes

4. Select **Enabled** and set the Override Value to True.
5. In the **Management Pack** section, select a management pack from the drop-down list. To create a management pack, click **New**.
6. Click **Apply**.

Results

In the SCOM console, select **Monitoring > Dell EMC > Dell EMC Performance and Power Monitoring Views** to view the performance information collected from Dell EMC PowerEdge servers.

The performance collection rules collect information based on the following parameters:

- Disk Performance (%)
- Ambient Temperature (Centigrade)
- Amperage (Amps)
- Energy Consumption (kWh)
- Peak Amperage (Amps)
- Peak Power (Watts)
- Physical Network Interface
- Power Consumption (BTU/hr)
- Power Consumption (Watts)
- Teamed Network Interface

i **NOTE:** When the Detailed edition of the Server and Rack Workstation Monitoring feature is imported, the disabled Performance (excluding Network Performance) and license-free Disk Performance (%) collection rules are enabled by default.

i **NOTE: Disk Performance (%)**—This view displays the **Remaining Rated Write Endurance** of Solid-State Drives (SSDs) of a PowerEdge server. To view the data, search for the SSD object.

i **NOTE:** Network Statistics, which are disabled by default, are defined only in the Detailed edition of the Dell EMC Server and Rack Workstation Monitoring feature.

State views in the monitoring feature for PowerEdge servers and rack workstations

About this task

The State view is available for viewing the health of Dell EMC devices that are monitored by different monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack. To view the state of a device:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC > Dell EMC State Views**.
Different State views are listed based on the monitoring feature. See [State views displayed by different monitoring features](#) on page 46.
3. To view data about a component, select a component.
Information is displayed in the **Detail View** section.

Results

The health of a component is derived by reviewing the unresolved alerts that are associated with the component. [Severity levels of discovered devices](#) on page 38 explain the various state components with their corresponding severity levels.

Discover and monitor DRACs on the SCOM console

Topics:

- Introduction to the monitoring features in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for DRACs
- Discovery and classification of DRACs
- Discover and enable DRAC devices
- Monitoring DRACs

Introduction to the monitoring features in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for DRACs

About this task

DRAC monitoring feature supports discovery and monitoring for the various generations of iDRAC—iDRAC6, iDRAC7, and iDRAC8 systems using SNMP.

i **NOTE:** The DRAC monitoring feature is deprecated for iDRAC9 and later generation of PowerEdge servers. Dell Technologies recommends that you use the Dell EMC OpenManage Integration with Microsoft System Center—Operations Manager (OMIMSSC) appliance for iDRAC9 systems. For more information about deploying and configuring OMIMSSC, see the latest version of *Dell EMC OpenManage Integration with Microsoft System Center for System Center Operations Manager User's Guide* on the Dell Technologies Support Site.

Discovery and classification of DRACs

About this task

The Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack feature enables you to discover and classify Dell Remote Access Controller (DRAC) and integrated DRAC (iDRAC). The following table lists the details of the hardware discovery and grouping by the Dell DRAC monitoring feature.

Table 4. Discovery and classification of DRACs

Group	Diagram View	Hardware Type
Dell Remote Access Controllers	Remote Access Controller Group	iDRAC modular and iDRAC monolithic instances. i NOTE: DRAC monitoring feature does not support the discovery of iDRAC9-based PowerEdge servers.

Discover and enable DRAC devices

About this task

The DRAC devices must be discovered as network devices under the **Administration** section of the SCOM console. To discover DRAC devices in the SCOM console, do the following:

Steps

1. Log in to the management server as a SCOM administrator.
2. In the left pane, select **Administration**.
3. In the left pane, click **Discovery Wizard**.
4. Select **Network devices**, and then complete the tasks that are prompted by the **Computer and Device Management Wizard**.

For more information, see the [Microsoft SCOM documentation](#).

5. On the **Add a Device Console** screen, enter the IP address that you want to discover.
6. Select the necessary Run As Account from the SNMP V1 or SNMP V2 **Run As Account** drop-down menu.
7. Enable the DRAC monitoring feature by using the **Dell EMC Feature Management Dashboard**.

Results

Scalability recommendation for SCOM

When managing large number of network devices in a distributed setup, use dedicated resource pools of Management Servers for each device type. For more information about the number of devices that are supported in a Management Group, see the Sizing Guide sections in the Microsoft SCOM documentation.

Monitoring DRACs

After you install Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack, you can use the **Monitoring** pane of SCOM to select views that provide complete health information of the discovered Dell DRAC devices. The DRAC monitoring feature discovers and monitors the health of the Dell DRAC devices. It includes monitoring health of the Dell DRAC devices, both at regular intervals and on occurrence of events. The [Severity levels of discovered devices](#) on page 38 indicates the health of the Dell DRAC devices on the network.

NOTE: To monitor the health of DRAC devices, associate the community string Run As account with the SNMP Monitoring Account with the target as the Dell Remote Access Controller class or respective DRAC object (if you have different Run As accounts for different DRAC devices).

View options for DRAC monitoring feature

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack provides the following types of views for monitoring DRACs by selecting **Monitoring > Dell EMC** on the SCOM console:

- [Alert view in the DRAC monitoring feature](#) on page 19
- [Diagram views in the DRAC monitoring feature](#) on page 20
- [State views in the DRAC monitoring feature](#) on page 20

Alert view in the DRAC monitoring feature

The Alert View is available for managing hardware and storage events from Dell EMC DRAC devices. SNMP traps and Platform Event Traps (PET) sent by DRAC devices are displayed by the DRAC monitoring feature.

To view DRAC alerts on the SCOM console:

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC > Dell EMC Alerts Views**. The following alerts are displayed:
 - **PET Traps**—These alerts contain information about PET traps from iDRAC6, iDRAC7, and iDRAC8 devices.

- **Remote Access Alerts**—These alerts contain information about SNMP traps from iDRAC6, iDRAC7, and iDRAC8 devices.

See [Alert views displayed by different monitoring features](#) on page 42.

3. Select the required Alert View. In the right pane, alerts that meet the criteria—such as alert severity, resolution state, or alerts that are assigned to you—are displayed.
4. Select an alert to view the details in the **Alert Details** section.

Diagram views in the DRAC monitoring feature

The Dell EMC Diagram Views offer a hierarchical and graphical representation of all Dell DRAC devices on the network.

To view the diagrams for DRAC monitoring feature on the SCOM console:

1. In the left pane of the SCOM console, select **Monitoring**.
 2. Expand **Dell EMC > Dell EMC Diagram Views**.
 3. In the **Monitoring** pane, select **Dell EMC Diagram Views** folder for the following views:
 - Dell EMC Complete Diagram View
 - Remote Access Controllers Group
- See [Diagram views displayed by different monitoring features](#) on page 42.

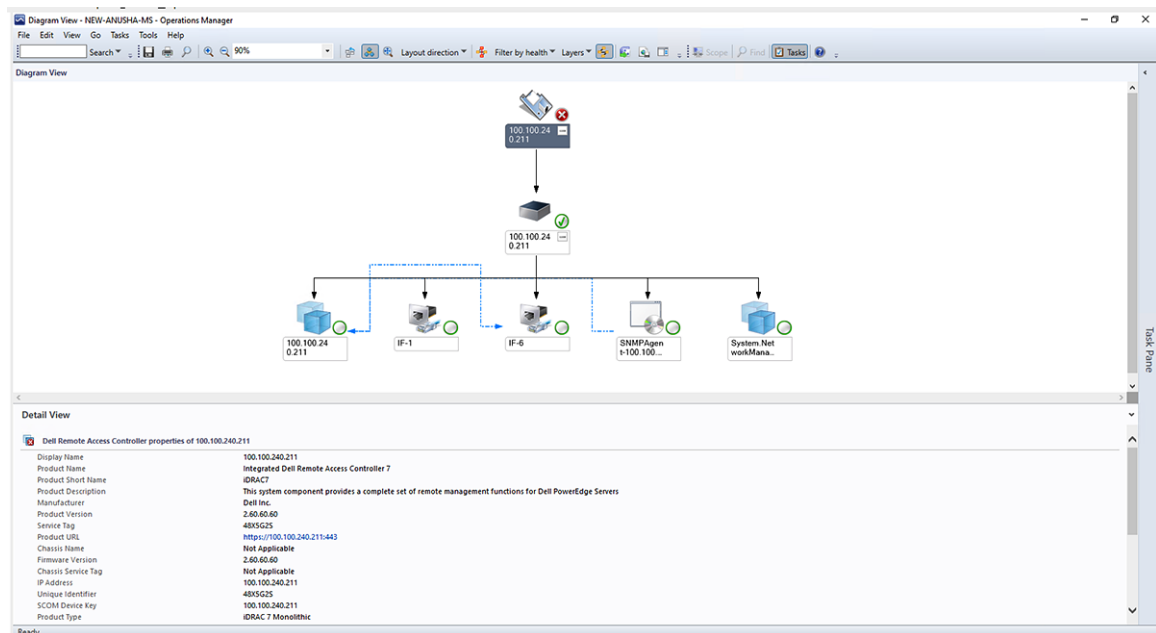


Figure 1. Remote Access Controllers Group Diagram View

4. Select a required **Dell EMC Diagram View** to view the hierarchical and graphical representation of the selected DRAC in the right pane.
5. Select a component in the diagram to view its details in the **Detail View** section.

State views in the DRAC monitoring feature

About this task

The State View is available for viewing the health of Dell EMC DRAC devices that are monitored by different monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack. To view the state of a device:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC > Dell EMC State Views**.

Different State views are listed based on the monitoring feature. See [State views displayed by different monitoring features](#) on page 46.

3. To view data about a component, select a component. Information is displayed in the **Detail View** section.

Results

The health of a component is derived by reviewing the unresolved alerts that are associated with the component. [Severity levels of discovered devices](#) on page 38 explain the various state components with their corresponding severity levels.

Supported tasks on the SCOM console

Topics:


- Run Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature-based tasks on SCOM
- Tasks run on Dell EMC devices by using the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features

Run Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature-based tasks on SCOM

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC**.
3. Expand either **Diagram Views**, **State Views**, or **Alerts Views**.
4. Select the device on which you want to run the task.
A list of tasks you can run by using the monitoring feature that is used by the device is displayed in the **Tasks** pane of the SCOM console.
5. In the **Tasks** pane, click the task that you want to run.
The task is started, and after the task is successfully run, a summary of the task is displayed.

Results

 **NOTE:** Some tasks have prerequisites to be successfully run.

Tasks run on Dell EMC devices by using the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features

When you select a device or a component, the relevant tasks are displayed in the **Tasks** pane of SCOM. This is a list of the tasks that you can run on Dell EMC devices by using different monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.

Table 5. Tasks run on Dell EMC devices by using the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features

Tasks run on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring feature
Check Node Interface	Yes	Yes
Get Warranty Information	-	No

Table 5. Tasks run on Dell EMC devices by using the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features (continued)

Tasks run on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring feature
Launch OpenManage Server Administrator (Monolithic Server)	Yes	Yes
Launch Dell EMC Remote Access Console	Yes	Yes
Launch Remote Desktop (Monolithic Server)	Yes	Yes
iDRAC Hard Reset	No	No
Clear ESM Logs	Yes	No
Power management-related tasks		
Check Power Status	Yes	No
Force Power Off	Yes	No
Power Cycle	Yes	No
Power off Gracefully	Yes	No
Power On	Yes	No
Power Reset	Yes	No
Turn LED Identification On	Yes	No
Turn LED Identification Off	Yes	No

To run the monitoring feature-based tasks on a SCOM console, see [Run Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature-based tasks on SCOM](#) on page 22.

Check connection to the nodes


By running the Check Node Interfaces task, you can check if the selected Dell EMC device or DRAC/iDRAC and its corresponding interfaces are reachable. After the task is successfully run, a summary of the reachability to the server and interface is displayed.

View warranty information of PowerEdge servers

By running the Get Warranty Information task, you can view the warranty status of the Dell EMC device.

Launch OMSA on monolithic servers using the SCOM console

By running the Launch Dell OpenManage Server Administrator task, you can start the Dell OMSA application.

 **NOTE:** The Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack tasks open the remote console when using Internet Explorer.

Launch iDRAC using the SCOM console

By running the Launch Dell EMC Remote Access Console task, you can start the Dell iDRAC application.

Launch Remote Desktop on monolithic servers using the SCOM console

By running the Launch Dell EMC Remote Desktop task, you can launch a Remote Desktop on Dell EMC monolithic servers.

NOTE: You can launch Dell EMC Remote Desktop only if Windows operating system is installed, and Remote Desktop is manually enabled on the managed node.

Clear Embedded Server Management (ESM) logs

The Server Administrator Embedded Server Management (ESM) log, also referred to as the hardware log, maintains a list of all system events that are generated by the hardware, such as Error-Correcting Code (ECC), system reset and boot, and probe threshold changes. You can refer to this log when hardware errors appear or when the system is not functioning properly.

To run the Clear ESM Logs task, do the following:

1. In the left pane, click **Monitoring**.
2. Expand **Dell EMC**.
3. Expand either **Diagram Views**, **State Views**, or **Alerts Views**.
4. Select the device on which you want to run the task. A list of tasks you can run by using the monitoring feature that is used by the device is displayed in the **Tasks** pane of the SCOM console.
5. In the **Tasks** pane, click **Dell EMC Windows Server Tasks > Clear ESM Logs**. The **Run Tasks** window is displayed.
6. Click **Run**. The ESM logs of the selected device is deleted.

NOTE: When you run the Clear ESM Logs task, on the task execution screen, only the result of the task initiating is displayed. For example, the task execution screen may show a success result even if the ESM logs are not cleared. This means that the Clear ESM Logs task initiation was successful.

Power management-related tasks

- Check power status of Dell EMC PowerEdge servers and Rack Workstations—You can run this task only on servers that are monitored by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack using OMSA. By running the Check Power Status task, you can check the power status and manage power control tasks by using the IPMI Shell.
- Power off PowerEdge server shutting down the operating system—By running the Force Power Off task, you can power off the PowerEdge server without shutting down the operating system.
- Power cycle a PowerEdge server—By running the Power Cycle task, you can power off the PowerEdge server, and then power on again after a delay.
- Gracefully power off a PowerEdge server—By running the Power Off Gracefully task, you can shut down the operating system, and then power off the PowerEdge server.
- Power on a PowerEdge server—By running the Power On task, you can power on the PowerEdge server of if it is in powered-off state.
- Reset the PowerEdge server power—By running the Power Reset task, you can power on the PowerEdge server of if it is in powered-off state.
- Identify an OMSA-based server by enabling the identification LED—By running the Turn LED Identification On task, you can enable the feature to identify a server by using a blinking LED. Similarly, by running the Turn LED Identification Off task, the feature to identify a server by using a blinking LED is disabled.

NOTE: To enable Advanced Power Control, install BMU in the default path. If BMU is not installed in the default path, create a console task. For more information about creating a console task, see [Identify device and device power status by using identification LEDs](#).

Generating reports

About this task

The reporting feature of the SCOM console enables you to create reports for Dell EMC OpenManage Windows Event Log, Dell server BIOS, firmware, and RAID configuration.

NOTE:


- Dell EMC Server and Rack Workstation Monitoring feature supports only object-level reporting.
- Dell server BIOS, firmware, and RAID configuration reports are available only in the Detailed edition.

Topics:

- [View reports about PowerEdge servers on the SCOM console](#)

View reports about PowerEdge servers on the SCOM console

Steps

1. On the SCOM console, select **Reporting**.
 2. Select:
 - a. **Dell Windows Server (Scalable Edition)** for the OpenManage Windows Event Log reports.
 - b. **Dell Windows Server (Detail Edition)** for BIOS configuration, firmware and driver versions, and RAID configuration reports.
-  **NOTE:** You can also access **Reporting** from the Diagram View or State View by clicking the server instance. The option for **Dell Reports** is available in the **Tasks** pane under the Dell System instance reports along with the default SCOM reports.

Generate Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack reports on the SCOM console

Steps

1. On the SCOM console, select **Reporting**.
2. In the working pane, based on the report that you want to generate, perform one of the following actions:
 - a. For OpenManage Windows Event Log report: Select **Dell Windows Server (Scalable Edition)** and select **OpenManage Windows Event Log**.
 - b. For BIOS configuration report: Select **Dell Windows Server (Detail Edition)** and select **BIOS Configuration**.
 - c. For firmware and driver report: Select **Dell Windows Server (Detail Edition)** and select **Firmware and Driver Versions**.
 - d. For RAID configuration report: Select **Dell Windows Server (Detail Edition)** and select **RAID Configuration**.
3. In the **Tasks** pane, click **Open**.
4. Select the duration for which you want the report to be generated.
5. Click **Add Object**.
6. Search for the following objects of class and click **Add: Dell Windows Server**.
The object is displayed in the **Select object** pane.
7. Select the required properties.
8. Click **Run**.

Results

The selected report is generated.

Upgrading Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

If you are using Dell EMC Server Management Pack Suite (DSMPS) version 7.2 then you can either upgrade to:

- Latest version of the OMIMSSC appliance for SCOM.
- Latest version of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack (using an installer).

Topics:

- [Upgrade to latest version of the OMIMSSC appliance for SCOM](#)
- [Upgrade from previous versions of DSMPS](#)

Upgrade to latest version of the OMIMSSC appliance for SCOM

While upgrading to the latest version of OMIMSSC appliance, do the following:

1. Set up the OMIMSSC appliance by deploying the VHD or OVA file on a Hyper-V or ESXi VM.
2. Enroll the Management Server with the OMIMSSC appliance. Wait for few minutes until the Dell EMC management packs are upgraded.
 - NOTE:** To plan for the number of Dell EMC Alert Relay Servers (previously known as Proxy Management Servers) that are required, see the *Scalability with OpenManage Integration with Microsoft System Center for System Center Operations Manager* technical white paper on the support site.
3. Open the Dell EMC OpenManage Integration Dashboard. Select **Monitoring** and click the link corresponding to the device type and perform the **Synchronize with MSSC** operation to synchronize the devices that are discovered in the SCOM console. For example, to synchronize the SMASH devices that are discovered in SCOM:
 - a. Go to the **Server View** in the Dell EMC OpenManage Integration Dashboard.
 - b. Click **Synchronize with MSSC**.

On the Dell EMC OpenManage Integration Dashboard, click **Sync with SCOM MS** to synchronize the Alert Relay Server information with the OMIMSSC appliance

CAUTION: Ensure to add the required number of Alert Relay Servers when you want to scale to large number of devices.


NOTE: Performance metrics that are generated from Dell EMC Servers and Rack Workstation Monitoring feature, which is discovered through the WS-Man protocol in the 7.0 views, are not retained.


Upgrade from previous versions of DSMPS

NOTE: The feature to upgrade DSMPS version 6.3 to DSMPS version 7.1 and later is not supported.

The installer detects the features that are installed from DSMPS version 7.0, and automatically upgrades the DSMPS to version 7.1 and later.

NOTE: The installer may display a message prompting a restart of the MS after the upgrade is completed. Ignore the message as restart is not required.

 **NOTE:** The alerts generated for PowerEdge servers and Rack Workstations will be acknowledged.

 **NOTE:** Low performance metrics will be retained after the upgrade.

Uninstalling Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

About this task

You can uninstall Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack by using:

- The Windows Control Panel.
- The **Remove** option in the installer file.

You can remove the Dell EMC management packs by de-enrolling one or more SCOM Management Servers.

Topics:

- [Uninstall using the Windows Control Panel](#)
- [Uninstall using installer file](#)

Uninstall using the Windows Control Panel

Steps

1. Click **Start > Control Panel > Uninstall a program**.
2. Right-click **Dell EMC Windows Server Agent-based and iDRAC 7/8 SNMP Management Pack** and click **Uninstall**.
3. Complete the uninstallation process by following the on-screen instructions.

Uninstall using installer file

Steps

1. From the location where the downloaded Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack installation file is extracted, run the `Dell EMC Server Management Pack Suite.exe` file. The **Welcome** screen is displayed.
2. Click **Next**.
3. Select **Remove**, and then select **Next**. The **Remove the Program** screen is displayed.
4. Click **Remove**.

Results

Uninstallation of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack removes the Dell EMC management packs that are imported in the SCOM console. For more information about removing management packs from SCOM, see the respective Microsoft documentation.

Reference topics

Topics:

- Monitoring features supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack
- Severity levels of discovered devices
- Discovery features supported in the monitoring of PowerEdge servers and rack workstations using OMSA
- Discovery features supported for monitoring DRACs
- Hardware components monitored by different monitoring features
- View options provided by the monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack
- Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Unit Monitors
- Event rules used by different monitoring features

Monitoring features supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

The topics in this section describe the monitoring features that are supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM.

Dell EMC Server and Rack Workstation Monitoring feature using OMSA

Dell EMC Servers and Rack Workstation Monitoring feature supports the discovery and monitoring of the following devices that are installed with the supported Windows operating system, using OpenManage Server Administrator (OMSA):

- PowerEdge Modular and PowerEdge Monolithic servers
- PowerVault servers
- Hardware monitoring of Dell EMC-branded or Dell EMC OEM Ready servers
- Dell Precision Racks

Inventory and monitoring of these devices is performed through the OpenManage Server Administrator (OMSA) application that is installed on the servers—which is a license-free monitoring feature.

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack automatically imports the scalable version of the Dell EMC Server and Rack Workstation Monitoring feature into SCOM.

Management packs necessary for using the Server and Rack Workstation Monitoring feature

After the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed successfully, the required Dell EMC management packs are imported and should appear in the **Administration** pane of the SCOM console.

Management packs' names and library location for monitoring PowerEdge servers and rack workstations

Table 6. Management Packs for the Server and Rack Workstation Monitoring feature

Feature	Default location of Management Packs	Management Packs
Dell EMC Server and Rack Workstation Monitoring	<p>Library: %PROGRAMFILES%\Dell Management Packs\Server Mgmt\<release>\Library</release></p> <p>Scalable and detailed Management Packs: %PROGRAMFILES%\Dell Management Packs\Server Mgmt\<release>\Server Monitoring</release></p>	<p>Library</p> <ul style="list-style-type: none"> Dell.Connections.HardwareLibrary.mp Dell.OperationsLibrary.Server.mp <p>Scalable feature</p> <ul style="list-style-type: none"> For Dell EMC Servers or Rack Workstations discovered using OMSA: <ul style="list-style-type: none"> Dell.Model.Server.mp Dell.WindowsServer.Scalable.mp Dell.View.Server.mp (Optional) Dell.WindowsServer.InformationAlertsOn.mp <p>i NOTE: Import Dell.WindowsServer.InformationAlertsOn.mp only if you want to receive Informational Alerts.</p> <p>Detailed feature</p> <ul style="list-style-type: none"> Dell.WindowsServer.Detailed.mp and all scalable management packs.

System configuration required for using the Server and Rack Workstation Monitoring feature

Management Server (MS) requirements for using the Server and Rack Workstation Monitoring feature

Operating systems supported by Microsoft SCOM Management Servers:

- For SCOM 2019, see <https://docs.microsoft.com/en-us/system-center/scom/welcome?view=sc-om-2019>.
- For SCOM 1807, see <https://docs.microsoft.com/en-us/system-center/scom/whats-new-in-om?view=sc-om-1807>.
- For SCOM 1801, see <https://docs.microsoft.com/en-us/system-center/scom/whats-new-in-om?view=sc-om-1801>.
- For SCOM 2016, see <https://docs.microsoft.com/en-us/system-center/scom/release-build-versions-2016?view=sc-om-2016>.

Software requirements for Microsoft SCOM Management Server:

- (Optional) DRAC tools from OpenManage Server Administrator (Server Administrator)—To inventory and monitor Dell EMC Server and Rack Workstation's iDRAC and its NIC.
- (Optional) Baseboard Management Controller (BMC) Management Utility—To run the Remote Power Control tasks or the LED Identification Control tasks on Dell-managed systems.

i **NOTE:** Access DRAC tools, OpenManage Server Administrator (Server Administrator), and BMC Management Utility from Dell Systems Management Tools and Documentation media, or download it from Dell Technologies support site.

Management Server Action Account privileges (MSAA)

- Start the DRAC discovery and corresponding DRAC console—Administrator or Power user.
- Clear ESM log data—Administrator or Power user. Alternatively, if the MSAA has normal user privileges, operators can, instead of selecting Use the predefined Run as Account, enter task credentials with Power User (or higher) privileges to run the Clear ESM Logs task.

Managed System requirements for using the Server and Rack Workstation Monitoring feature

Install any supported OpenManage Server Administrator versions (including the Server Administrator Storage Management Service) on the managed system.

- If you want to upgrade or uninstall OMSA on the managed system, the Alerts View of the managed system may display the following error: `Script or Executable failed to run.`

- If the managed system is not a Management Server then switch the system to the Maintenance Mode until the upgrade or uninstall completes. If the managed system is the Management Server, you may manually close the alerts after the upgrade or uninstall is complete.

NOTE: On systems using OMSA 7.2 DRAC tools, it is recommended to upgrade to OMSA 7.4 DRAC tools or later.

NOTE: For more information about the supported operating systems for the managed system, see the *OpenManage Server Administrator Installation Guide* on the support site.

Feature management tasks for monitoring PowerEdge servers and rack workstations

After Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed, the Dell EMC Server and Rack Workstation Monitoring feature is auto-imported into SCOM and its related tasks are available in the Feature Management tasks section. The following table lists the Server and Rack Workstations Monitoring feature tasks available on the **Dell EMC Feature Management Dashboard**.

NOTE: In the event log, ignore the errors pertaining to reimporting of existing management packs under the error logs. These errors occur when Dell EMC Feature Management Dashboard reimports all the dependent management packs that are already imported while importing a monitoring feature.

NOTE: Wait for a task to complete (view the state update change in the dashboard) before starting another task using the Dell EMC Feature Management Dashboard.

Table 7. Feature management tasks of the Dell EMC Server and Rack Workstations Monitoring feature in DSMPS

Tasks	Description
Enable Agent Proxying	Enables the agent proxy.
Set as Preferred Monitoring Method	Enables the Dell EMC Server and Rack Workstation Monitoring feature as the preferred monitoring method for your Dell EMC Server and Rack Workstations, when the Server and Rack Workstations in the setup are monitored through both; Dell EMC Server and Rack Workstations Monitoring feature and Dell Technologies Server and Rack Workstations Monitoring (Licensed) feature.
Set to Scalable Feature	If the Detailed feature is running on the system, the Dell EMC Feature Management Dashboard switches from the Detailed to the Scalable version. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set to Detailed Feature	If the Scalable feature is running on the system, the Dell EMC Feature Management Dashboard switches from the Scalable to the Detailed version. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set Informational Alerts On	Informational alerts are turned on when the Dell EMC Server and Rack Workstations Scalable monitoring is in use.
Set Informational Alerts Off	Informational alerts are turned off when the Dell EMC Server and Rack Workstations Scalable monitoring is in use.
Refresh Dashboard	Updates the Dell EMC Feature Management Dashboard . NOTE: The Refresh dashboard task may not update the dashboard immediately; it might take a few minutes to update the dashboard contents.
Refresh Node Count	Updates the node count of servers monitored using this feature.

Table 7. Feature management tasks of the Dell EMC Server and Rack Workstations Monitoring feature in DSMPS (continued)

Tasks	Description
Remove Monitoring Feature	Removes the Dell EMC Server and Rack Workstations Monitoring feature.

DRAC Monitoring feature

The DRAC Monitoring feature supports discovery and monitoring for the various generations of iDRAC—iDRAC6, iDRAC7, and iDRAC8 systems by using SNMP.

NOTE: The DRAC Monitoring feature is deprecated for iDRAC9 and above systems. Recommendation is to use the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature for iDRAC9 systems available in the OMIMSSC appliance for SCOM.

Management packs necessary for using the DRAC Monitoring feature

Table 8. Management packs for the DRAC monitoring feature in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Feature	Default location of Management Packs	Required Management Packs
DRAC Monitoring	<p>Library: %PROGRAMFILES%\Dell Management Packs\Server Mgmt Suite\<release>\Library</release></p> <p>Management Packs: %PROGRAMFILES%\Dell Management Packs\Server Mgmt Suite\<release>\Remote Access Monitoring</release></p>	<p>Library</p> <ul style="list-style-type: none"> • Dell.Connections.HardwareLibrary.mp • Dell.OperationsLibrary.Common.mp <p>Management Packs</p> <ul style="list-style-type: none"> • Dell.DRAC.OM07.mp • Dell.DRAC.OM12.mp—SCOM 2012 or later. • Dell.Model.DRAC.mp • Dell.OperationsLibrary.DRAC.mp • Dell.View.DRAC.mp

Configuration prerequisites required for using the DRAC Monitoring feature

For using the DRAC monitoring feature, you must configure the firewall to enable the SNMP ports.

DRAC monitoring requirement

To monitor the health of DRAC devices, associate the community string Run As account with the SNMP Monitoring Account with the target as Dell Remote Access Controller class or respective DRAC object (if you have different Run As accounts for different DRAC devices).

Feature management tasks for DRAC Monitoring feature

The following table lists the DRAC monitoring tasks available in the Dell EMC Feature Management Dashboard. Some tasks that are listed in the Feature Management tasks table appear only after you have imported the DRAC monitoring feature.

NOTE: In the event log, ignore the errors pertaining to reimporting of existing management packs under the error logs. These errors occur when Dell EMC Feature Management Dashboard reimports all the dependent management packs that are already imported while importing a monitoring feature.

NOTE: Wait for a task to complete (view the state update change in the dashboard) before starting another task using the Dell EMC Feature Management Dashboard.

Table 9. Feature management tasks of the DRAC Monitoring feature

Tasks	Description
Import DRAC Monitoring Feature	Imports and enables the DRAC monitoring feature in SCOM.
Refresh Dashboard	Updates the Dell EMC Feature Management Dashboard . <i>i</i> NOTE: The Refresh Dashboard task may not update the dashboard immediately; it might take a few minutes to update the dashboard contents.
Refresh Node Count	Updates the node count.

Configuring the monitoring features by using the Feature Management Dashboard

The **Dell EMC Feature Management Dashboard** provide options to configure monitoring features using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack to monitor Dell EMC PowerEdge servers, Dell EMC Precision Racks, and Dell Remote Access Controllers (DRACs). You can import, upgrade, and remove the monitoring features using the Dell EMC Feature Management dashboard.

Import monitoring features using the Dell EMC Feature Management Dashboard

About this task

The **Dell EMC Feature Management Dashboard** enables you to view the available Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features and then configure them automatically for importing, upgrading, and removing the Dell EMC management packs required by a feature. In a distributed setup (including distributed resource pool in SCOM 2012), the Management Server, where Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed first, is selected to host all the feature-based management activities.

To import the monitoring features:

Steps

1. Start the SCOM console.
2. In the left pane, select **Monitoring**.
3. Expand **Dell EMC > Dell EMC Feature Management Dashboard**.

On the **Dell Technologies Feature Management Dashboard** page, you can view the list of Dell EMC monitoring features installed, the version currently in use, the version you can upgrade to, the level of monitoring, total nodes used by the current license, and the licenses required, if any.

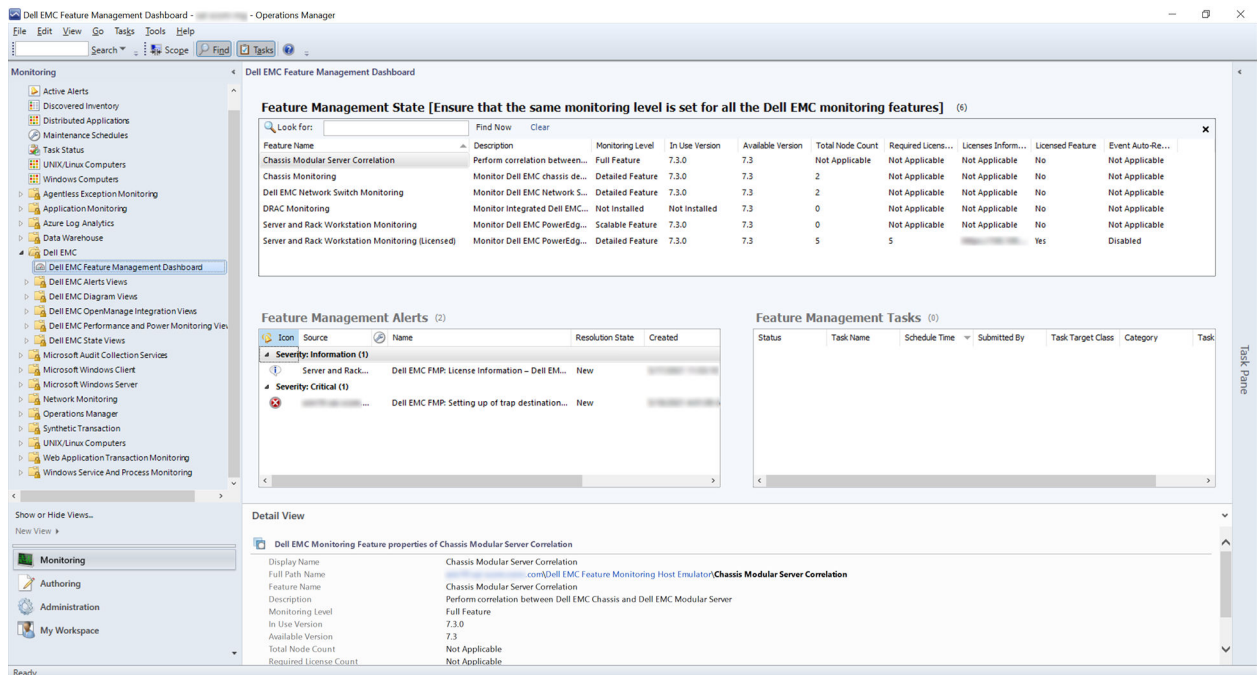


Figure 2. Dell EMC Feature Management Dashboard

4. Select the monitoring feature that you want to install.
5. In the **Tasks** pane, expand **Dell EMC Monitoring Feature Tasks**.
6. Click the task to import a feature.
7. On the **Run Task** screen, select **Use the predefined Run As Account**.
8. Click **Run**.
9. After the task is successfully completed, click **Close**.

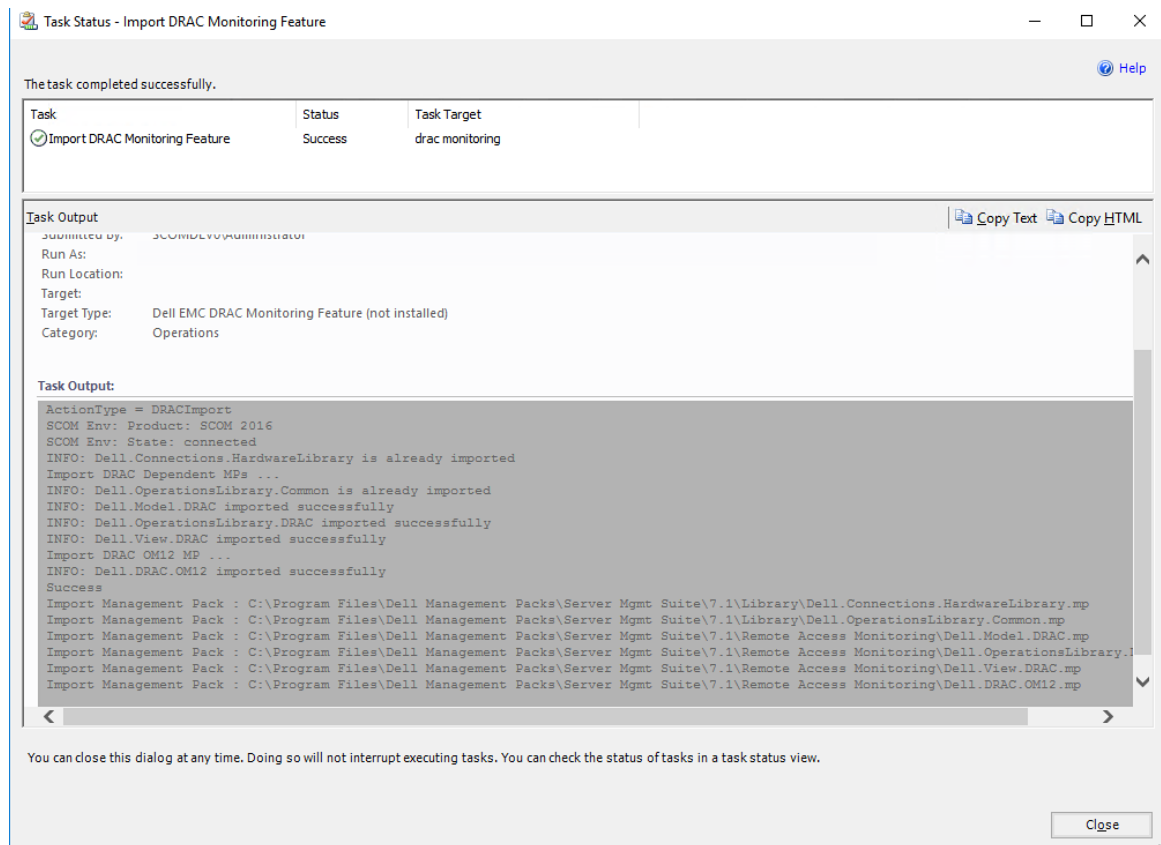


Figure 3. Task status of Import Monitoring Feature

10. Repeat steps 3 through 8 for each monitoring feature you want to enable.

Results

NOTE: Before running another task by using the **Dell Technologies Feature Management Dashboard**, wait for the current tasks to complete.

Upgrade monitoring features using the Dell EMC Feature Management Dashboard

About this task

To ensure that you take advantages of the latest monitoring features by using Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack, you must upgrade the monitoring features, whenever they are released. To upgrade monitoring features by using the Feature Management Dashboard, do the following:

Steps

1. Start the SCOM console.
2. Select **Monitoring**.
3. Expand **Dell EMC > Dell EMC Feature Management Dashboard**.
4. Select the monitoring feature that you want to upgrade.
5. In the **Tasks** pane, expand **Dell EMC Monitoring Feature Tasks** and select the upgrade task.
6. On the **Run Task** upgrade screen, select **Use the predefined Run As Account**.
7. Click **Run**.

CAUTION: If there are any dependencies or associations that have to be overridden, which results in data loss, the task cannot be successfully run and an appropriate message is displayed. To continue to run the task, click **Override**, and set the **AutoResolve Warnings/Errors override** to **True**.

8. After the task is complete, click **Close**.

Results

During the process of upgrading, all overrides—any customization to discovery, unit monitors, and rules from previous versions of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack (DSMPS)—are carried over to the DSMPS version 7.1 and later.

Customizing monitoring features using the Feature Management Dashboard for scalable and detailed editions

Table 10. Customizing Monitoring Features using Dell EMC Feature Management Dashboard—Scalable and Detailed editions

Features	Scalable Edition	Detailed Edition
Dell EMC Server and Rack Workstation Monitoring	Inventory and health monitoring at server and component group level.	Detailed inventory and monitoring of the following components: memory, processors, sensors, network interfaces, storage controllers, disks, and volumes. BIOS information is also displayed.
DRAC Monitoring	<ul style="list-style-type: none"> iDRAC inventory iDRAC health monitoring 	Not Applicable.

Remove monitoring features using the Dell EMC Feature Management Dashboard

About this task

To remove or disable the monitoring features, use the **Dell EMC Feature Management Dashboard**. Before removing any of the monitoring features, close or resolve all open alerts. While removing a monitoring feature, the **Dell EMC Feature Management Dashboard** exports all override references as backup in the installation folder. However, custom group information and override instance level information cannot be reused in the future.

To remove the monitoring features:


Steps

1. Start the SCOM console and select **Monitoring**.
2. In the **Monitoring** pane, expand **Dell EMC > Dell EMC Feature Management Dashboard**. The **Dell EMC Feature Management Dashboard** pane displays the list of monitoring features currently available on the SCOM console.
3. Select the monitoring feature that you want to remove.
4. Under the **Tasks** pane, expand **Dell EMC Monitoring Feature Tasks**.
5. To remove the monitoring feature, click **Remove Feature**. For example, to remove **Dell EMC Servers and Rack Workstations Monitoring** feature, click **Remove Monitoring Feature** in the **Tasks** pane.
6. On the **Run Task—Remove Feature** screen, click **Use the predefined Run As Account**.
7. Click **Run**.

CAUTION: If there are any dependencies or associations that have to be overridden, which result in data loss, the task cannot be successfully run. To continue to run the task, click **Override**, and set the **AutoResolve Warnings/ Errors override** to **True**.

8. After the task is complete, click **Close**.

Results

-  **NOTE:** Running the **Remove Monitoring Feature** task in **Dell EMC Feature Management Dashboard** may fail if there are overrides that are referenced to custom group or instances. In such a case, ensure to remove the overrides that are associated to custom group or instances.

Import management packs to the SCOM console

About this task






To effectively use Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for device monitoring and management purposes, you must import the latest Dell EMC management packs to SCOM, whenever they are released. To import the Dell EMC management packs for SCOM, do the following:

Steps

1. Start the SCOM console.
2. In the left pane, select **Administration**.
3. Click **Management Packs** and select **Import Management Packs** from the **Administration Overview**.
4. On the **Select Management Packs** screen, click **Add > Add from disk**.
5. Enter the location details or go to the location where you have installed Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack.
If you had chosen to install in the default directory, the Dell EMC management packs are available in: `C:\Program Files\Server Mgmt Suite\Dell Management Packs\<release>`.
6. Select the Dell EMC management pack that you want to import and click **Open**.
The **Import Management Packs** screen is displayed, and the Dell EMC management packs are listed in the **Import List**.
7. Click **Install**.

Severity levels of discovered devices

The symbols that indicate the severity levels of the discovered Dell EMC devices on the SCOM console:

-  —Normal/OK—The component is working as expected.
-  —Critical/Failure/Error—The component has either failed or a failure is imminent. The component requires immediate attention and may must be replaced. Data loss may have occurred.
-  —Warning/Noncritical—A probe or other monitoring device has detected a reading for the component that is greater than or lesser than the acceptable level. The component may still be functioning, but it could fail. The component may also be functioning in an impaired state.
-  —The health status is not applicable for the specific component.
-  —The service is unavailable.

Discovery features supported in the monitoring of PowerEdge servers and rack workstations using OMSA

- Dell EMC PowerEdge Servers discovery—Classifies the Dell EMC PowerEdge Servers and populates the attributes.
- Dell EMC PowerEdge Server Network Interface discovery—Discovers the network interface at group level of the Dell EMC PowerEdge Server.

- Dell EMC PowerEdge Server Hardware Components discovery—Discovers hardware components at a group level (such as sensors, processor, memory, and power supply).
- Dell EMC OpenManage Software Services discovery—Discovers the objects for OMSA Windows services.
- Dell EMC PowerEdge Server Detailed BIOS discovery—Discovers BIOS objects for each Dell EMC PowerEdge Server (Detailed edition only).
- Dell EMC PowerEdge Server Detailed Memory discovery—Discovers memory instances for the Dell EMC PowerEdge Server (Detailed edition only).
- Dell EMC PowerEdge Server Detailed Power Supply discovery—Discovers power supply instances for the Dell EMC PowerEdge Server (Detailed edition only).
- Dell EMC PowerEdge Server Detailed Processor discovery—Discovers processor instances for the Dell EMC PowerEdge Server (Detailed edition only).
- Dell EMC PowerEdge Server Detailed Storage discovery—Discovers the complete storage hierarchy for the Dell EMC PowerEdge Server (Detailed edition only).
- Dell Windows Server Detailed Sensor discovery—Discovers sensor instances for Dell EMC PowerEdge Server (Detailed edition only).
- Dell Windows Server Detailed Network Interfaces discovery module—Discovers the physical and teamed network interface instances of the Dell EMC PowerEdge Server (Detailed edition only).
- Dell Windows Server Network Interfaces Group discovery module—Discovers the Network Interfaces group.
- Dell EMC Rack Workstation Group discovery—Discovers the Dell EMC Rack Workstation group.
- Dell Unmanaged Server Group discovery—Discovers Dell EMC PowerEdge Servers that are not being monitored either due to the absence of Dell instrumentation, an unsupported OMSA version, or has an instrumentation version lower than the required version.

Discovery features supported for monitoring DRACs

iDRAC Discovery—Discovers all supported Integrated Dell Remote Access Controllers.

Dell Integrated Remote Access Modular Discovery—Discovers the Chassis Name and Chassis Service Tag of Dell Integrated Remote Access Controllers for Modular systems.

- iDRAC6 Modular Discovery—Discovers the iDRAC6 (Modular) group.
- iDRAC6 Monolithic Discovery—Discovers the iDRAC6 (Monolithic) group.
- iDRAC7 Modular Discovery—Discovers the iDRAC7 (Modular) group.
- iDRAC7 Monolithic Discovery—Discovers the iDRAC7 (Monolithic) group.
- iDRAC8 Modular Discovery—Discovers the iDRAC8 (Modular) group.
- iDRAC8 Monolithic Discovery—Discovers the iDRAC8 (Monolithic) group.
- Dell Remote Access Group Discovery—Discovers the Dell Remote Access group and populates iDRAC.
- Dell Integrated Remote Access Monolithic Group Discovery—Discovers the Dell Integrated Remote Access Monolithic group and iDRAC (Monolithic).
- Dell Integrated Remote Access Modular Group Discovery—Discovers and populates the iDRAC (Modular) group.

Hardware components monitored by different monitoring features

Table 11. Monitored hardware components by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features

Monitored hardware components	Server and Rack Workstation monitoring feature using OMSA	
	Scalable edition	Detailed edition
Battery Sensor	No	Yes
Battery Sensor Group	No	Yes
BIOS Config Unit	No	No
BIOS Unit	-	-
Chassis Intrusion Sensor	No	Yes

Table 11. Monitored hardware components by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features (continued)

Monitored hardware components	Server and Rack Workstation monitoring feature using OMSA	
	Scalable edition	Detailed edition
Current Sensor	No	Yes
Current Sensor Group	No	Yes
Fan Sensor	No	Yes
Fan Sensor Group	No	Yes
Host NIC	-	-
Host NIC Group	-	-
iDRAC	Yes	Yes
iDRAC License	-	-
iDRAC License Group	-	-
iDRAC Network Interface	-	-
Intrusion Sensor	-	-
Intrusion Sensor Group	-	-
Memory	Yes	Yes
Memory Group	-	-
Memory Unit	No	Yes
Network Interfaces	-	-
Network Interfaces Group	Yes	Yes
Network Interfaces Physical Group	No	Yes
Network Interfaces Teamed Group	No	Yes
OpenManage Software Services	Yes	Yes
PCIeSSD Backplane	-	-
PCIeSSD Extender	-	-
PCIeSSD Physical Disk	-	-
Physical Network Interface Instance	No	Yes
Network Interfaces Teamed Group	-	-
Power Supplies	Yes	Yes
Power Supply Group	-	-
Power Supply Unit	No	Yes
Processor Group	-	-
Processor Unit	No	Yes
Processors	Yes	Yes
SD Card Group	-	-
SD Card	-	-
Sensors	Yes	Yes
Sensors Group	-	-
Storage	Yes	Yes

Table 11. Monitored hardware components by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features (continued)

Monitored hardware components	Server and Rack Workstation monitoring feature using OMSA	
	Scalable edition	Detailed edition
Storage Connector Internal/external/direct attached physical disk group	-	-
Storage Connector Internal/external/direct attached physical disk instance	-	-
Storage Controller	Yes	Yes
Storage Controller Battery Group	-	-
Storage Controller Battery	-	-
Storage Controller Connector Unit	No	Yes
Storage Controller Enclosure Fan Sensor	-	-
Storage Controller Enclosure Fan Sensor Group	-	-
Storage Controller Enclosure Instance	-	-
Storage Controller Enclosure Unit	No	Yes
Storage Controller Physical Disk Group	No	Yes
Storage Controller Physical Disk Unit	No	Yes
Storage Controller Sensors	No	Yes
Storage Controller Virtual Disk Group	No	Yes
Storage Enclosure EMM Unit	No	Yes
Storage Enclosure Physical Disk Group	No	Yes
Storage Enclosure Power Supply Group	No	Yes
Storage Enclosure Power Supply	-	-
Storage Enclosure Sensors	No	Yes
Storage Enclosure Temperature Sensor Group	-	-
Storage Enclosure Temperature Sensors	-	-
Storage Group	-	-
Storage Virtual Disk	-	-
Storage Controller Virtual Disk Group	-	-
Teamed Network Interface Unit	No	Yes
Temperature Sensor	-	-
Temperature Sensor Group	-	-
Voltage Sensor	No	Yes
Voltage Sensor Group	No	Yes

View options provided by the monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

Table 12. View options provided by the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features

View types	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring
Alert View	Yes	Yes
Diagram View	Yes	Yes
Performance and Power Monitoring View	Yes	No
State View	Yes	Yes

Alert views displayed by different monitoring features

Table 13. Alert views displayed by different monitoring features

Alert View Type displayed on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring
Dell EMC Network Interface Alerts Views	Yes	No
Dell EMC Server and Rack Workstation Alerts Views	Yes	No
Dell EMC Network Interface Alerts	Yes	No
Dell EMC Rack Workstation Alerts	Yes	No
PET Traps	No	Yes
Remote Access Alerts	No	Yes

Diagram views displayed by different monitoring features

Table 14. Diagram views displayed by different monitoring features

Diagram View Type displayed on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring
Complete Diagram View	Yes	Yes
Rack Workstation Diagram View	Yes	No
Modular Server Diagram View	Yes	No

Table 14. Diagram views displayed by different monitoring features (continued)

Diagram View Type displayed on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring features	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring
Monolithic Server Diagram View	Yes	No
Sled Server Diagram View	Yes	No
Unit Diagram View	Yes	No
Remote Access Controller Group Diagram View	No	Yes

Complete Diagram View supported by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

The Dell EMC Complete Diagram View displays a graphical representation of all Dell EMC devices that are monitored in the SCOM console. You can expand and verify the status of individual devices and their components in the diagram.

A Complete Diagram view displayed by the monitoring features in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack has information about the following:

- Dell EMC Modular and Monolithic servers
- Dell EMC Sled Group
- Dell EMC Rack Workstations Group
- Dell EMC Rack Workstations (Monitoring feature using iSM-WMI)
- Remote Access Controllers
- Dell EMC unmanaged systems

Rack Workstation Diagram View supported

The Dell EMC Rack Workstation Diagram Views provides a graphical representation of all supported Dell EMC Rack Workstations and enables you to expand and verify the status of individual devices and their components in the diagram. Select a Rack Workstation in the diagram to view its details in the **Detail View** section.

Component data displayed by the Modular and Monolithic Systems Diagram Views

The Dell EMC Modular Systems Diagram View and Dell EMC Monolithic Servers Diagram View displays information about the following components:

Table 15. Component data displayed by the Modular and Monolithic Systems Diagram Views

Component data displayed by the Modular and Monolithic Diagram Views	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature
	Server and Rack Workstation monitoring feature using OMSA
Physical network interfaces	No
Memory	No
PSU	No
Sensors	No
Processors	No
Storage Components	No
BIOS (Inventory only)	No

Table 15. Component data displayed by the Modular and Monolithic Systems Diagram Views (continued)

Component data displayed by the Modular and Monolithic Diagram Views	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature
	Server and Rack Workstation monitoring feature using OMSA
BIOS	Yes
iDRAC NIC	No
Host NIC	No
SD Card	No
Network Interfaces Group	Yes
License	No
Memory Group	Yes
PSU Group	Yes
Sensor Group	Yes
Processor Group	Yes
Storage Component Group	Yes
Host NIC Group	Yes
iDRAC	Yes
iDRAC License Group	Yes
PCIe/SSD Group	No
SD Card Group	Yes

Supported Modular Systems Diagram View

The Modular Systems Diagram View offers a graphical representation of all Dell EMC modular systems and enables you to expand and verify the status of individual devices and their components in the diagram.

Supported Monolithic Servers Diagram View

The Dell EMC Monolithic Servers Diagram View offers a graphical representation of all Monolithic systems and enables you to expand and verify the status of individual devices and their components in the diagram.

Supported Sled Servers Diagram View

The Dell EMC Sled Servers Diagram View offers a graphical representation of all Sled servers and enables you to expand and verify the status of individual devices and their components in the diagram. Select a Sled server in the diagram to view its details in the **Detail View** section.

Supported PowerEdge server Unit Diagram View

Select a Dell EMC PowerEdge Server from the Dell EMC Modular System View or Dell EMC Monolithic Servers Diagram Views, to view the diagram specific to that particular system. System-specific diagrams illustrate and indicate the status of the components that are supported by the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature.

Supported Remote Access Controllers Group Diagram view

The Remote Access Controllers Group diagram view offers a graphical representation of all iDRAC6, iDRAC7, and iDRAC8 devices. Select a component in the diagram to view its details in the **Detail View** section.

Storage controller component hierarchy

To view the status and health of components such as hard drives, connectors, VDs, controllers, sensors, and enclosures, expand the **Storage** component in any Dell EMC system instance Diagram View.

Network interfaces component hierarchy

The Dell EMC Network Interfaces group is created only when an Intel or Broadcom network interface card is present and enabled on the Dell EMC PowerEdge server. Network interfaces are grouped under **Physical Interfaces** and **Teamed Interfaces**. If you disable a network interface, the network interfaces group will be removed from management in the next discovery cycle. A reference relationship is created between a Teamed network interface and its associated Physical network interfaces. You can view the reference relationship only when you enable the **Enable Correlation** attribute of **Dell EMC Windows Server Physical and Teamed Relationship Discovery**. For more information, see [Enable correlation between Windows-based server physical and teamed interfaces in PowerEdge servers monitored using OMSA](#) on page 45.

Enable correlation between Windows-based server physical and teamed interfaces in PowerEdge servers monitored using OMSA

Steps

1. Start the SCOM console.
2. In the left pane, select **Authoring**.
3. In the left pane, select **Management Pack Objects**, and then double-click **Object Discoveries**.
4. In the working pane, search for **Dell Windows Server Physical and Teamed Relationship Discovery Rule**.
5. Right-click, and then click **Overrides > Override the Object Discovery → For all objects of class: Teamed Network Interface instance (Enriched)**.
6. In the **Override Properties** dialog box:
 - a. In the **Enabled Correlation** row, set the Override Value to True.
 - b. Click **OK**.

Results

The status roll-up of network interfaces on the Diagram view is displayed only up to the Network Interfaces group level. For example, if the remaining components of the server are normal and only one or more of the network interfaces are in critical or noncritical state, the health state of the server is indicated as Normal, but the Network Interfaces group status is indicated as Critical or Warning.

Enable the server rollup health status in PowerEdge servers monitored using OMSA

About this task

For the status roll-up to be displayed at the server level, enable the **Network Interfaces Group to Dell Server Health Roll up** dependency monitor by doing the following:

Steps

1. Start the SCOM console.
2. In the left pane, select **Authoring**.
3. In the pane, click **Management Pack Objects > Monitors**.
4. In the working pane, search for **Network Interfaces Group** to search for the server you want to enable the functionality on.

5. A list of server types on which you can enable the feature is listed. For example, Dell Windows Server.
6. Under Dell Windows Server, expand **Entity Health > Availability**.
7. Right-click **Network Interfaces Group to Dell Server Health Roll up**, and click **Overrides > Override the Monitor > For all objects of class: Dell Windows Server**.
8. In the **Override Properties** dialog box:
 - a. In the **Enabled** row, set the Override Value to True.
 - b. In the **Management Pack** section, select a management pack from the drop-down list.
9. Click **Apply**.

Results

The server rollup health status is enabled on PowerEdge servers that are monitored by that specific monitoring feature.

State views displayed by different monitoring features

Table 16. State views displayed by different monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack

State View Type displayed on the SCOM console	Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack monitoring feature	
	Server and Rack Workstation monitoring feature using OMSA	DRAC monitoring
Servers and Rack Workstation State View	Yes	No
Managed Rack Workstation State View	Yes	No
FM Servers State View	Yes	No
Sled Servers State View	Yes	No
DRAC State View	No	Yes

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Unit Monitors

A unit monitor monitors the performance counter over two successive cycles to check if it exceeds a threshold value. When the threshold value is exceeded, the Dell EMC PowerEdge Server changes state and generates an alert. This unit monitor is disabled by default. You can override (enable) the threshold values in the **Authoring** pane of the SCOM console. Unit monitors are available under Dell Windows Server objects for the Dell EMC Server and Rack Workstation Monitoring feature. To enable the threshold values of unit monitors, see [Enable performance and power monitoring unit monitors](#) on page 16. Dell Unit monitors assess the various conditions that can occur in monitored objects. The result of this assessment determines the health state of a target.

The Dell unit monitors are:

- Event Monitor—Triggered by the event that the Dell instrumentation logs in the Windows event log indicating the health of the corresponding object.
- Periodic Monitor—Triggered by a periodic poll that is configured as Interval Seconds.

Scalable Edition Unit monitors in the monitoring feature for PowerEdge servers and workstations using OMSA

All the following unit monitors provided by the monitoring feature using OMSA are of **Periodic** type:

Memory

- Dell EMC Server Memory Status

- Dell EMC Server Memory Redundancy Status

OpenManage Software Services

- Dell EMC Server Management (DSM) Connection Service Availability Status
- DSM Data Manager Availability Status
- DSM Event Manager Availability Status
- DSM Shared Service Availability Status
- DSM Storage Service Availability Status
- Windows Management Instrumentation (WMI) Service Availability Status

Power Supplies

- Dell EMC Server Power Supplies Status

Processors

- Dell EMC Server Processors Status

Sensors

- Dell EMC Server Battery Status
- Dell EMC Server Current Status
- Dell EMC Server Fans Status
- Dell EMC Server Intrusion Sensor Status
- Dell EMC Server Temperature Sensor Status
- Dell EMC Server Voltage Sensor Status

Storage Controller

- Storage Controller Status

Network Interfaces Group (Basic)

- Global Network Interfaces (Basic) Connection Status

Network Interfaces Group (Enriched)

- Global Enriched Network Interfaces Status
- Global Network Interfaces (Basic) Connection Status

iDRAC

- Dell Server iDRAC Network Interface Monitor

Dell OM Performance

- Ambient Temperature Average Threshold AlertMonitor
- Amperage Average Threshold AlertMonitor
- EnergyConsumption Average Threshold AlertMonitor
- PowerConsumption (BTU/hr) Average Threshold
- PowerConsumption (Watts) Average Threshold AlertMonitor
- Dell OM Server Unsupported Unit Monitor

Detailed Edition Unit monitors in the monitoring feature for PowerEdge servers and workstations using OMSA

All the following unit monitors provided by the monitoring feature using OMSA are of **Periodic** type:

Memory Unit

- Detailed Memory Event Monitor
- Detailed Memory Unit Monitor

Power Supplies Unit

- Detailed Power Supply

Processor Unit

- Detailed Processor

Storage Controller Connector Unit

- Controller Connector Event Monitor
- Controller Connector Unit Monitor

Storage Controller EMM Unit

- Enclosure EMM Event Monitor
- Enclosure EMM Unit Monitor

Storage Controller Enclosure Unit

- Controller Enclosure Event Monitor
- Controller Enclosure Unit Monitor

Storage Controller Physical Disk Unit

- Controller Physical Disk Event Monitor
- Controller Physical Disk Unit Monitor
- Enclosure Physical Disk Event Monitor
- Enclosure Physical Disk Unit Monitor

Storage Controller Power Supply Unit

- Enclosure Power Supply Event Monitor
- Enclosure Power Supply Unit Monitor

Storage Controller Sensors

- Controller Sensor Event Unit Monitor
- Controller Sensor Unit Monitor

Storage Controller Virtual Disk Group

Storage Controller Virtual Disk Unit

- Controller Virtual Disk Event Monitor
- Controller Virtual Disk Unit Monitor

Storage Enclosure Physical Disk Group

Storage Enclosure Sensors

- Enclosure Fan Event Unit Monitor
- Enclosure Fan Unit Monitor
- Enclosure Temperature Event Monitor
- Enclosure Temperature Unit Monitor

Physical Network Interface Unit (Basic)

- Connection Status

Physical Network Interface Unit (Enriched)

- Administrative Status
- Connection Status
- Link Status
- Operational Status

Teamed Network Interface Unit (Basic)

- Teamed Network Interface (Basic) Availability Status

Teamed Network Interface Unit (Enriched)

- Teamed Network Interface Unit (Enriched) Administrative Status
- Teamed Network Interface Unit (Enriched) Connection Status
- Teamed Network Interface Unit (Enriched) Link Status
- Teamed Network Interface Unit (Enriched) Operational Status
- Teamed Network Interface Unit (Enriched) Redundancy Status

Fan Sensor

- Fan Sensor Unit Monitor

Current Sensor

- Current Sensor Unit Monitor

Voltage Sensor

- Voltage Sensor Unit Monitor

Battery Sensor

- Battery Sensor Unit Monitor

Chassis Intrusion Sensor

- Chassis Intrusion Sensor Unit Monitor

Unit monitors in the monitoring feature for DRACs

All the following unit monitors provided for DRAC monitoring are of **Periodic** type:

- iDRAC6 Modular
 - Dell Remote Access Status
- iDRAC6 Monolithic
 - Dell Remote Access Status
- iDRAC7 Modular
 - **NOTE:** For iDRAC7 modular and monolithic servers, the Dell RAC periodic-based and Dell RAC triggered-based unit monitors are disabled.
 - Dell Remote Access Status
 - Controller Global Status
 - Controller Global Storage Status
- iDRAC7 Monolithic
 - Dell Remote Access Status
 - Controller Global Status
 - Controller Global Storage Status
- iDRAC8 Modular
 - **NOTE:** For iDRAC8 modular and monolithic servers, the Dell RAC periodic-based and Dell RAC triggered-based unit monitors are disabled.
 - Dell Remote Access Status
 - Controller Global Status
 - Controller Global Storage Status
- iDRAC8 Monolithic
 - Dell Remote Access Status
 - Controller Global Status
 - Controller Global Storage Status

Event rules used by different monitoring features

The data center administrators using the SCOM console may want to know about the rules and monitors running on a system. The event rules that are used by different monitoring features of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack provide information the relevant event rules information to the administrators.

Event rules processed by the monitoring feature for PowerEdge servers and workstations using OMSA

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack processes rules from OMSA and OMSA Storage Management events.

Server Administrator

All informational, warning, and critical events of OMSA have corresponding event processing rule. Each of these rules is processed based on the following criteria:

- Source Name = "Server Administrator"
- Event ID = Actual event ID of the Server Administrator instrumentation event
- Data Provider = Windows System Event Log

Storage Management


All informational, warning, and critical events for the Server Administrator Storage Management Service have a corresponding event processing rule. Each of these rules is processed based on the following criteria:

- Source Name = "Server Administrator"
- Event ID = Actual event ID of the Server Administrator Storage Management Service event
- Data Provider = Windows system event log

Event rules processed by the monitoring feature for DRACs

All informational, warning, and critical SNMP traps for the DRAC devices have a corresponding SNMP trap rule. Each of these rules are processed based on the following criteria:

- Source Name = "DRAC/CMC name or IP"
- OID = Actual trap ID of the DRAC /CMC SNMP trap event
- Data Provider = SNMP trap

 **NOTE:** Informational alerts are turned off by default. To receive these alerts, import informational alerts management pack.

Troubleshooting

Topics:

- Data is not displayed on the Feature Management Dashboard
- A task run on the Feature Management Dashboard fails
- Feature Management alerts
- The Management Server (MS) is not functioning, and therefore, tasks associated with it cannot be completed (Health Service of the Feature Management Host Server is nonfunctional)

Data is not displayed on the Feature Management Dashboard

About this task

In a distributed setup, the SCOM Management Server, where the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed first, is selected to host all feature management activities such as discoveries, alerts, and tasks. The SCOM Management Server on which the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed first populates the Feature Management Dashboard. However, if you have manually imported the Feature Monitoring management pack without running the installer on the SCOM Management Server, the Feature Management Pack host is not selected. Therefore, data is not displayed on the Feature Management Dashboard.

To populate the Feature Management Dashboard:


Steps

1. In the SCOM console, click **Authoring**.
2. In the **Authoring** section, expand **Management Pack Objects**.
3. Click **Object Discoveries**.
4. In the **Look for** box, search for **Dell Feature Management Host Discovery**.
5. Right-click **Dell Feature Management Host Discovery**, and then select **Overrides > Override the Object Discovery > For all objects of class: Dell Feature Management Host Discovery**.
6. To run the feature management activities, select **FmpHostFqdn**.
7. Set the override value to the FQDN of the SCOM Management Server.

A task run on the Feature Management Dashboard fails

About this task

Performing upgrade task on the Feature Management Dashboard can result in data loss. For example, if there are any dependencies or associations on the monitoring feature being modified then upgrade task fails by displaying a message.

 **CAUTION: Overriding task parameters may result in management pack or operational data loss.**

To resolve this issue, do the following:

Steps

1. Start the SCOM console and click **Monitoring**.
2. In the **Monitoring** pane, browse to **Dell EMC > Feature Management Dashboard**.

The Feature Management Dashboard displays a list of management packs present in SCOM and the management pack version to which you can upgrade.

3. Select the monitoring feature.
4. Under **Tasks**, expand **Dell Monitoring Feature Tasks**.
5. Click the upgrade monitoring task.
6. On the **Run Task — Upgrade Monitoring Feature** screen, click **Override**.
The Override Task parameters are displayed.
7. From the drop-down menu in the **New Value** column, set the AutoResolve Warnings/Errors property True.
8. Click **Override**.
9. To run the task, click **Run**.

Feature Management alerts

Table 17. Feature Management alerts

Alert Text	Alert State	Cause	Resolution
Dell FMP: Dell Device Helper Utility is either not present or incompatible with the Dell EMC Server and Rack Monitoring (Licensed) Management Pack.	Critical	<ul style="list-style-type: none"> • The required Dell Device Helper Utility version was not found, or the Dell Device Helper Utility is corrupted. • A version later than the required Dell Device Helper Utility version was detected. • A version earlier than the required Dell Device Helper Utility version was detected. 	Run the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack installer on the SCOM Management Server. Use the Repair option in the installer. See Repair installation issues of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack on page 11.

The Management Server (MS) is not functioning, and therefore, tasks associated with it cannot be completed (Health Service of the Feature Management Host Server is nonfunctional)

About this task

In a distributed setup, the SCOM Management Server, where the Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack is installed first, is selected to host all feature management activities such as discoveries, alerts and tasks. If the selected Management Server has stopped functioning, the executed Feature Management task fails, and Dell EMC Feature Management Dashboard is not populated. If such a selected Management Server is corrupt or health service is not obtained, decommission the Management Server to remove stale objects. For more information, see [https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/hh456439\(v=sc.12\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/system-center/system-center-2012-R2/hh456439(v=sc.12)?redirectedfrom=MSDN).

To populate the Dell EMC Feature Management Dashboard:

Steps

1. In the SCOM console, click **Authoring**.
2. In the **Authoring** section, expand **Management Pack Objects**.
3. Click **Object Discoveries**.
4. In the **Look for** box, search for **Dell Feature Management Host Discovery**.

5. Right-click **Dell Feature Management Host Discovery**, and then select **Overrides > Override the Object Discovery > For all objects of class: Dell Feature Management Host Discovery**.
6. Select **FmpHostFqdn**, and then set the override value to FQDN of the SCOM Management Server where the feature management activities have to run.

Additional resources

Table 18. Additional resources

Document	Description	Availability
Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Release Notes	Provides information about new features, known issues, and workaround in Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM.	<ol style="list-style-type: none"> 1. Go to Dell.com/esmmanuals. 2. Select OpenManage Integration for Microsoft System Center Operations Manager (SCOM), and then select the required application version. 3. Select the DOCUMENTATION tab to access these documents.
Dell EMC OpenManage Integration with Microsoft System Center for System Center Operations Manager User's Guide	Provides information about deploying, configuring, using, and troubleshooting the OMIMSSC appliance.	
Dell EMC OpenManage Integration with Microsoft System Center for System Center Operations Manager Release Notes	Provides information about new features, known issues, and workaround in the OMIMSSC appliance for SCOM.	
Scalability with OpenManage Integration with Microsoft System Center for System Center Operations Manager technical white paper	Provides information to scale up your monitoring capabilities by adding Dell EMC Alert Relay Servers in to your OMIMSSC environment.	

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.


- Direct links:
 - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—<https://www.dell.com/esmmanuals>
 - For Dell EMC Virtualization Solutions—www.dell.com/virtualizationsolutions
 - For Dell EMC OpenManage—<https://www.dell.com/openmanagemanuals>
 - For iDRAC—<https://www.dell.com/idracmanuals>
 - For Dell EMC OpenManage Connections Enterprise Systems Management—<https://www.dell.com/OMConnectionsEnterpriseSystemsManagement>
 - For Dell EMC Serviceability Tools—<https://www.dell.com/serviceabilitytools>
- Dell EMC support site:
 1. Go to <https://www.dell.com/support>.
 2. Click **Browse all products**.
 3. From the **All products** page, click **Software**, and then click the required link.
 4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.

Contacting Dell Technologies

About this task

Dell Technologies provides several online and telephone-based support and service options. Availability varies by country or region and product, and some services may not be available in your area.

 **NOTE:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell Technologies product catalog.

To contact Dell Technologies for sales, technical support, or customer service issues:

Steps

1. Go to Dell.com/support.
2. At the bottom right of the page, select preferred country or region from the list.
3. Click **Contact Us** and select the appropriate support link.

Glossary

Table 19. Terms used in this guide

Term	Description
AMSRP	All Management Server Resource Pool
CMC/ OME-M	Dell EMC Chassis Management Controller/ OpenManage Enterprise—Modular
DRAC/ iDRAC	Dell Remote Access Controller/ integrated Dell Remote Access Controller of Dell EMC PowerEdge server, Dell branded OEM servers, and Dell OEM—ready servers, unless otherwise specified.
Dell EMC Servers and Rack Workstation monitoring	This is a license-free monitoring feature that is offered by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack to discover and monitor PowerEdge servers, PowerVault Monolithic and Modular systems, Dell EMC branded or Dell EMC OEM Ready servers, and supported Dell Precision Racks running the supported Windows operating system by using the supported OpenManage Server Administrator (OMSA) in a data center.
FMD	Dell EMC Feature Management Dashboard
MS	Management Server
MP	Management Pack
OMIMSSC	Dell EMC OpenManage Integration for Microsoft System Center—Operations Manager
SCOM	Microsoft System Center for Operations Manager.
VM	Virtual Machine

Additional topics

Topics:

- Identify device and device power status by using identification LEDs
- Migrate from Dell Server Management Pack Suite Version 6.0 for Microsoft SCOM
- Configure SCOM to monitor traps and trap-based unit monitors
- Create Run-As-Account for SNMP monitoring
- Associate multiple Run-As accounts
- Install Web Services Management (WS-Man) and SMASH device template
- Associate Run-As Account task—Dell EMC Server and Rack Workstation Monitoring feature

Identify device and device power status by using identification LEDs

About this task

Advanced power control and LED identification tasks use the default BMC credentials and installation path (C:\Program Files\Dell\SysMgt\bmc). If the systems deviate from the default BMC credentials and installation path, install BMU 2.0 or later the management server and create new console tasks.

- NOTE:** For the following steps, create a task and set the password in plain text. If BMC is not installed on the management server, the SCOM console may indicate an error with the entire command in a dialog box, and then reveal the password. If you export the created override management pack containing this task to a drive:
- Open the exported management pack in a common text editor.
 - View the password in plain text in the **Authoring** section of the SCOM console.

- NOTE:** Create a task only if necessary and consider the security aspects before you proceed.

To create a task for managing the status of LED to identify the status of a device power:

Steps

1. On the SCOM console, in the left pane, click **Authoring**.
2. Under **Management Pack Objects**, right-click **Tasks**, and then select **Create a New Task**.
3. In the **Select a Task Type** dialog box, do the following:
 - a. In the **Select the type of task to create** section, select **Command line**.
 - b. Select a destination management pack.
 - c. Click **Next**.
 - d. Enter a task name and its description.
To select a task target, click **Select**, and then select from the **Select Items to Target** dialog box. In this case, select Dell Windows Server—For Server and Rack Workstation Monitoring feature.
 - e. Click **Next**.
The **Command Line** screen is displayed.
 - f. In the **Application** box, enter the ipmitool.exe application path (the path where BMU was installed on the management server).
For example, C:\Program Files\Dell\SysMgt\bmc\ipmitool.exe. For the two LED identification tasks, the application path is C:\Program Files\Dell\SysMgt\bmc\ipmish.exe (default BMU path may differ based on the operating system language).
4. For power control tasks, in the **Parameters** field, enter the command-line parameters in the following format:
 - Enter **-I lanplus -H**, and then choose the **Remote Access IP with IPMI capability** from the drop-down menu.

- Enter `-U <username> -P <password> -k <kgkey> <IPMI Task String>`
- Replace `<IPMI Task String>` with one of the following options:
 - `power status` (for Check Power Status task)
 - `power on` (for Power On task)
 - `power soft` (for Power Off Gracefully task)
 - `power off` (for Force Power Off task)
 - `power cycle` (for Power Cycle task)
 - `power reset` (for Power Reset task)
 - `identify on` (for LED Identification On task)
 - `identify off` (for LED Identification Off task)

For example: `-I lanplus -H Target/Property[Type="Dell.WindowsServer.Server"]/RemoteAccessIP$ -U root -P<password> -k <kgkey> power status`

- For LED on or off tasks, enter the CLI parameters in the following format:
 - Enter `-ip` and select **Remote Access IP with IPMI capability** from the drop-down menu.
 - Enter `-u <username> -p <password> -k <kgkey> <IPMI task string>`.
- Click **Create**.
Perform these actions for each new BMC task.

Migrate from Dell Server Management Pack Suite Version 6.0 for Microsoft SCOM

Until Dell Server Management Pack Suite Version 6.0 for SCOM, Dell Connections License Manager (DCLM) was required to manage licenses. For Dell Server Management Pack Suite Version 6.1 and later, you do not require DCLM. There is no longer a license-count enforcement post DCLM being removed. You can continue to manage the PowerEdge servers using Server and Rack Workstation Monitoring (Licensed) feature for SCOM even after reaching or exceeding the limit of the number of licenses purchased from Dell Technologies. The Checking License Usage section presents the steps to help you determine the number of nodes being managed to ensure that you have the appropriate number of license entitlements from Dell Inc. Purchase additional licenses if the number of nodes you are managing exceeds the number of licenses you have purchased.

Licenses that you have purchased for Dell Server Management Pack Suite Version 6.0 for SCOM are still applicable to Dell Server Management Pack Suite Version 6.1 and later for SCOM. Therefore, after a product upgrade, the earlier license is still valid, and you can still manage servers based on the permissible count mentioned in the previously purchased license.


Configure SCOM to monitor traps and trap-based unit monitors


About this task

To monitor traps and trap-based unit monitors in SCOM, do the following:

Steps

- Start the SCOM console and select **Administration**.
- In the **Administration** pane, browse to **Run As Configuration > Profiles**.
- From the list of available profiles, right-click **SNMP Monitoring Account** and click **Properties**.
The **Introduction** screen is displayed.
- Click **Next**.
The **Specify the Run As profile's general properties** screen is displayed.
- Click **Next**.
The **Run As Accounts** screen is displayed.
- Click **Add**.
- To discover devices, from the **Run-As Account** drop-down menu, select the community string.


 **NOTE:** If a Run-As-Account community string is not available then create one. See [Create Run-As-Account for SNMP monitoring](#).

 **NOTE:** If you are using multiple Run-As accounts to discover devices, associate each device with its associated Run-As account. For more information, see [Associate Multiple Run As Accounts](#).

8. Click **OK**.
9. After completing tasks prompted by the wizard, click **Close**.


Create Run-As-Account for SNMP monitoring

Steps

1. Start the SCOM console and select **Administration**.
2. In the **Administration** pane, click **Run As Configuration > Accounts**.
3. Right-click **Accounts** and click **Create Run As Account**.
The **Introduction** screen is displayed.
 **NOTE:** For more information about Run As Account for Network Monitoring, see the [Microsoft documentation](#).
4. Click **Next**.
The **General Properties** screen is displayed.
5. Select a community string from the **Run As Account type** drop-down menu.
6. In the **Display name** box, enter the community string name and click **Next**.
7. In the **Community string** box, enter the community string, and then click **Next**.
The **Distribution Security** screen is displayed.
8. Select the **Less secure - I want the credentials to be distributed automatically to all managed computers** option, and then click **Create**.
9. After completing tasks prompted by the wizard, click **Close**.
10. Under **This Run As Account will be used to manage the following objects**, select **All targeted objects** to associate the Run As Account to all Dell EMC devices.
11. Click **OK**.

Associate multiple Run-As accounts

Steps

1. Complete steps 1–6 in [Configuring Operations Manager to monitor Traps and Trap-Based Unit Monitors](#).
2. On the **Add a Run As Account** screen, select the **A selected class, group, or object** option.
3. Click **Select > Class**.
The **Class Search** screen is displayed.
 **NOTE:** You can also associate the community string Run As Account with Object and Group. For more information, see the Microsoft documentation for SCOM at www.docs.microsoft.com.
4. In the **Filter by (optional)** box, enter the class name. Based on the type of device, enter **Dell EMC Server**, **Dell CMC/OME-M**, or **Dell EMC DRAC/MC**.
5. Click **Search**.
6. Under **Available items**, select the class you want to add.
7. Click **OK**.
8. On the **Add Run As account** screen, click **OK**.
9. For each class type you want to manage, repeat steps 2–8.
10. Click **Save**.
11. After completing tasks prompted by the wizard, click **Close**.


Install Web Services Management (WS-Man) and SMASH device template

Steps

1. From www.microsoft.com/en-in/download/confirmation.aspx?id=29266, download the following SMASH Library MPB file to a temporary location: `WS-ManagementAndSMASHDeviceDiscoveryTemplate.msi`.
2. To copy the SMASH Library MPB file to the user- or default location, run the MSI file.
3. Start the SCOM console.
4. In the left pane, select **Administration**.
5. Select **Management Packs**, and then select **Import Management Packs** in the working pane.
6. Select **Add > Add from disk**.
7. Enter the location details or browse the location where you downloaded the Microsoft SMASH Library MPB file.
8. Select the MPB file and click **Open**.
The **Import Management Packs** screen is displayed with the template in the **Import list**.
9. Click **Install**.

Associate Run-As Account task—Dell EMC Server and Rack Workstation Monitoring feature

Associate Run-As Account task associates the Run-As Account used for SMASH discovery with all the Dell Server objects that are required for health monitoring. This task is available as an option for performing object-level association.

 **WARNING: Perform the Associate Run-As Account task only if necessary. This task affects the configuration of all Dell Server objects. Dell Server Run-As Account Association unit monitor automatically performs the object-level association.**