Dell EMC OpenManage Integration Version 7.3 with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM)

User's Guide

D&LL Technologies

Notes, cautions, and warnings

(i) **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.**

Contents

About Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM)

Microsoft System Center—Operations Manager (SCOM) enables you to monitor devices and applications in your data center. Dell EMC provides management packs on the OpenManage Integration with Microsoft System Center (OMIMSSC) appliance for SCOM, by using which administrators can manage their Microsoft and Dell EMC devices by using a single interface: The Microsoft System Center—Operations Manager (SCOM) console. The Dell EMC OMIMSSC appliance integrates with Microsoft SCOM to discover, inventory, monitor health, monitor performance metrics, and monitor alerts of PowerEdge servers and rack workstations, Modular Infrastructure (including PowerEdge MX7000), and network switches. The OMIMSSC appliance offers the agent-free monitoring of Dell EMC Servers and Rack Workstations—through iDRAC or iSM management pack, Dell EMC Chassis, and Dell EMC Networking Switches.

OMIMSSC is a VM that is hosted on one of the following:

- Hyper-V using a VHD file.
- VMware ESXi using an OVA file.

OMIMSSC is an appliance-based solution available in a ZIP file package. There are two supported file formats of the appliance that can be extracted from the following ZIP packages:

- OMIMSSC_<version>_SCOM.vhd_<revision>.zip, where version is the release version of the OMIMSSC appliance and revision is the build revision number, can be extracted to a VHD file format.
- OMIMSSC_<version>_SCOM.ova_<revision>.zip, where version is the release version of the OMIMSSC appliance and revision is the build revision number, can be extracted to an OVA file format.

Both the above compressed packages contain:

- VHD file or OVA file.
- Documentation folder containing the readme.txt file.

The Dell EMC OMIMSSC appliance is based on CentOS and interacts with the Dell EMC devices. The supported protocols for communication with the devices are:

- Web Services-Management (WS-Man)
- Simple Network Management Protocol (SNMP)
- Redfish

Topics:

- OMIMSSC architecture overview
- Key features of OMIMSSC for SCOM
- Advantages of the OMIMSSC appliance for SCOM
- Compare the features offered by OMIMSSC appliance for SCOM against Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM
- New features in this release

OMIMSSC architecture overview
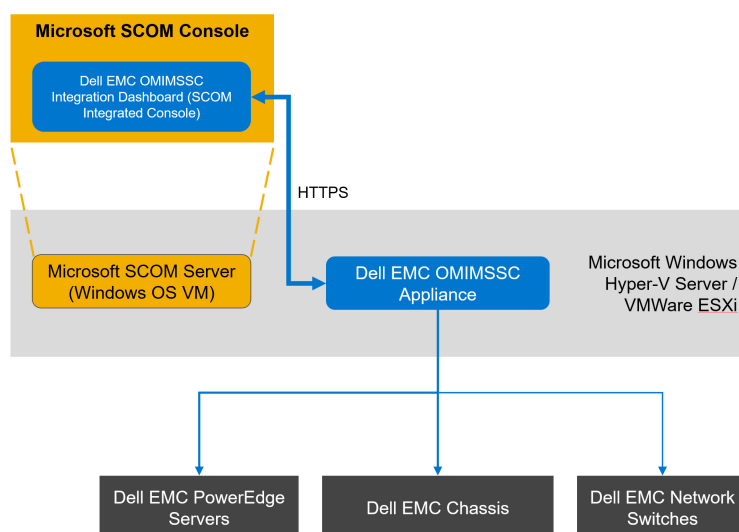
Figure 1. Architecture of the OMIMSSC appliance

Key features of OMIMSSC for SCOM

Table 1. Key features with descriptions of OMIMSSC for SCOM

Features	Description
License center	Manage OMIMSSC licenses from the OMIMSSC Admin Portal.
Dell EMC Servers and Rack Workstation (Licensed) monitoring feature	Support for the following by using the **Dell EMC OpenManage Integration Dashboard** on the SCOM console: • License-based discovery and monitoring of iDRAC9-based PowerEdge Servers, 12th generation, and 13th generation PowerEdge Servers, PowerVault servers, supported Dell Precision Racks, hardware monitoring of Dell EMC branded or Dell EMC OEM Ready servers and Dell EMC Microsoft Storage Spaces Direct Ready nodes through: ○ iDRAC using WS-MAN ○ iDRAC access using Host operating system ○ iSM using Windows Management Instrumentation (WMI) • Discovery and monitoring of iDRAC9-based PowerEdge Servers, 12th generation, and 13th generation PowerEdge Servers, PowerVault servers, supported Dell Precision Racks, hardware monitoring of Dell EMC branded or Dell EMC OEM Ready servers and Dell EMC Microsoft Storage Spaces Direct Ready nodes using iDRAC. • Discovery and monitoring of iDRAC9-based PowerEdge Servers, 12th generation, and 13th generation PowerEdge Servers using iSM. For the complete list of supported servers, see **Supported platforms** in the **iDRAC Service Module Installation Guide** on the support site. • SNMP traps for devices that are discovered through WS-Man of Servers and Rack Workstation Monitoring (Licensed) feature.

Table 1. Key features with descriptions of OMIMSSC for SCOM (continued)

Features	Description
Dell EMC Chassis monitoring feature	Support for the following by using the **Dell EMC OpenManage Integration Dashboard** on the SCOM console: ● Discovery and monitoring of Dell EMC Chassis, and Dell OEM Ready chassis devices. ● Discovery of server modules and chassis slot summary for CMC chassis. ● SNMP traps for Chassis devices.
Dell EMC Network Switch monitoring feature	Support for the following by using the **Dell EMC OpenManage Integration Dashboard** on the SCOM console: ● Discovery and monitoring of Dell EMC Network Switches devices. ● SNMP traps for Dell EMC Network Switch devices.

DRAC monitoring feature is deprecated for iDRAC9-based PowerEdge servers. Dell Technologies recommends using the agent-free Dell EMC Servers and Rack Workstation (Licensed) monitoring feature to monitor iDRAC9-based PowerEdge servers.

Advantages of the OMIMSSC appliance for SCOM

● Simplifies data center operations by integrating OMIMSSC with the SCOM console.
● Uses agent-free monitoring architecture for PowerEdge servers.
● Simplifies device monitoring by using a management dashboard.
● Reduces operations cost, increase effectiveness, and enable administrators to perform value-added tasks.
● Scaling up the monitoring capabilities by configuring Dell EMC Alert Relay Servers (previously known as Proxy Management Servers) in the SCOM Management Group.
● Can be deployed on either Hyper-V or ESXi by using VHD or OVA file formats.

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

Table 2. Compare the features offered by OMIMSSC appliance

Features	Offered by OMIMSSC appliance for SCOM	Offered by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM (previously known as Dell EMC Server Management Pack Suite for SCOM)
Solution offered	OMIMSSC is an integration with SCOM, a solution that offers the agent-free monitoring of Dell EMC devices including PowerEdge servers, chassis, and network switches.	Offers the agent-based monitoring solution for Dell EMC PowerEdge servers.
Discovery and monitoring features	Agent-free discovery and monitoring of the following platforms: ● PowerEdge Servers and Rack Workstations ● PowerEdge Modular Infrastructure ● Network Switches	Discovery and monitoring of servers and rack workstations using software-based agent (OMSA).

Table 2. Compare the features offered by OMIMSSC appliance (continued)

Features	Offered by OMIMSSC appliance for SCOM	Offered by Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for SCOM (previously known as Dell EMC Server Management Pack Suite for SCOM)
Licensed features	OMIMSSC appliance has license for Dell EMC server and rack workstation monitoring feature using iDRAC agent- free and iSM.	None. Offers the agent-based monitoring solution for Dell EMC PowerEdge servers and rack workstations.
License-free features	• Dell EMC Chassis monitoring feature • Dell EMC Chassis modular servers monitoring feature • Dell EMC Chassis and modular servers correlation feature • Dell EMC Network Switch monitoring feature	• Dell EMC server and rack workstation monitoring feature using OMSA • Dell Remote Access Controllers (DRAC) monitoring feature
Necessity of Dell EMC Alert Relay Servers (previously known as Proxy Management Servers)	Does the OMIMSSC appliance require Alert Relay Servers—Yes. For more information about configuring and onboarding Dell EMC Alert Relay Servers before discovering Dell EMC devices, see Setting up Dell EMC Alert Relay Servers.	Does Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager require Alert Relay Servers—Not applicable.
Supported number of nodes	600 and above, in multiples of 1,000 devices. For more information about configuring Alert Relay Servers, see the **Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM)** technical white paper on the support site.	Maximum of 600 devices.

For more information about Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager, see the **Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager User's Guide** on the support site.

New features in this release

- For a seamless onboarding of the OMIMSSC appliance for agent-free monitoring:
  - Wizard-based enhancement to enroll SCOM Management Group and Dell EMC Alert Relay Servers (previously known as Proxy Management Servers) with the OMIMSSC appliance.
  - Dell EMC Alert Relay Server Installer to onboard and configure the Dell EMC Alert Relay Servers to discover and monitor multiple Dell EMC devices by scaling up the monitoring capabilities on the SCOM console.
  - For seamless alert reception capabilities, the SNMP Monitoring Profile on the SCOM console is automatically associated with the Dell EMC Hardware class after the enrollment of SCOM Management Group.
- An option to create, edit, and delete Windows Credential profiles on the OMIMSSC Admin Portal.
- Using online (linux.dell.com/repo/omimssc-scom/latest) or offline custom repositories, you can update to the latest OMIMSSC appliance version wherein the imported Dell EMC Management Packs, appliance kernel RPMs, and application RPMs are automatically updated.
- SCOM Console administrators receive recommendations to install or update the OMIMSSC Appliance and agent-free management packs for supported PowerEdge servers, AX nodes, and S2D Ready Nodes on the **Updates and Recommendations** page.
- Support for:
  - System Center Operations Manager 2022.
  - 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 R250, R350, T150, T350
  - PowerEdge R450, R550, R750xs, R650xs, T550
  - PowerEdge R7525, R6525, R7515, R6515
  - PowerEdge R750, R650

- ○ PowerEdge R750xa
- ○ PowerEdge C6525
- ○ PowerEdge C6520
- ○ PowerEdge MX750c
- ○ PowerEdge XR12, XR11
● Support for the following latest SmartFabric OS10-based Network Switches: MX5108N, MX9116N, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148FE-ON, S4148T-ON, S4148U-ON, S4248FB-ON, S4248FBL-ON, S5148F-ON, S5212F-ON, S5224F-ON, S5232F, S5248F-ON, S5296F-ON, S6010-ON, Z9264F-ON.
● Support for the following AX nodes:
  - ○ AX-7525
  - ○ AX-740xd
  - ○ AX-6515
  - ○ AX-640
● Support for the following Dell EMC Microsoft Storage Spaces Direct Ready Nodes:
  - ○ Storage Spaces Direct R740xd Ready Node
  - ○ Storage Spaces Direct R740xd2 Ready Node
  - ○ Storage Spaces Direct R640 Ready Node
  - ○ Storage Spaces Direct R440 Ready Node
● Security enhancements:
  - ○ For secure HTTP access (HTTPS), the OMIMSSC appliance supports Certificate Authority (CA) or Enterprise CA signed certificates.
  - ○ As part of ongoing security enhancements, various security-related improvements are implemented in this release.

Purchase and manage OMIMSSC license

The Dell EMC Server and Rack Workstation Monitoring (Licensed) feature in OMIMSSC is licensed. Licenses must be purchased based on the number of nodes that you want to monitor. A node is a server which is monitored by using the iDRAC IP (agent-free, using WS-Man) or iSM (agent-based, using WMI).

Topics:

- OMIMSSC license types
- OMIMSSC licensed features
- OMIMSSC license-free features
- Purchase OMIMSSC license
- Importing licenses in the OMIMSSC Admin Portal
- Check the usage of your OMIMSSC license on the SCOM console

OMIMSSC license types

- Evaluation license—A trial version of the license that supports up to five nodes. By default, the OMIMSSC appliance is provided with the Evaluation License to discover and monitor up to five nodes.
- Production license—Purchase based on the number of nodes you want to be monitored by OMIMSSC. For more information about purchasing licenses, see Purchase OMIMSSC license.

ⓘ **NOTE:** Both evaluation and production licenses are node-based licenses and are specific to the generation of PowerEdge Servers (such as 13th generation or iDRAC9 based). After a server is retired, you cannot reuse the license associated with the server on other nodes—of same or other generations of PowerEdge servers, and you must purchase new licenses from Dell Technologies.

OMIMSSC licensed features

OMIMSSC appliance has license for the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature using iDRAC agent-free and iSM.

OMIMSSC license-free features

- Dell EMC Chassis monitoring feature
- Dell EMC Chassis modular server monitoring feature
- Dell EMC Chassis and modular servers correlation feature
- Dell EMC Network switch monitoring feature

Purchase OMIMSSC license

To leverage the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature functionalities, you must purchase licenses (based on the required number of managed nodes) from Dell Technologies. The order confirmation and license are sent to the email address that you have specified in **My Account—Dell**. The purchased licenses are also downloadable from the Dell Digital Locker portal at dell.com/software-and-subscriptions. If you are unable to download your licenses, email Dell Technologies Customer Support by going to dell.com/support/incidents-online/en-in/ContactUs/Dynamic.

The licenses are also governed by the same license terms as the product End-User License Agreement (EULA). You can get the latest updated license terms at dell.com/learn/us/en/uscorp1/terms?s=corp. For further queries, contact Dell Technologies Sales and Support.

Importing licenses in the OMIMSSC Admin Portal

After purchasing the licenses, you can import them into the OMIMSSC Admin Portal.

1. Log in to the OMIMSSC Admin Portal.
2. Expand the left pane and select **License Center**.
3. On the **Licensing Center** page, click **Import** and select the XML file to be imported.

The **License Summary** section lists the total number of licensed nodes, nodes that are in use, and nodes that are available to be discovered. The details of the licenses with their Entitlement ID, Product ID, and Total Capacity are listed under the **Managing Licenses** section.

Check the usage of your OMIMSSC license on the SCOM console

To view the PowerEdge servers that are managed by Dell EMC Server and Rack Workstation Monitoring (Licensed) feature for SCOM:

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

   (i) **NOTE:** The number of nodes that are consumed is displayed in the **Total Node Count** column.

Port information and communication matrix for OMIMSSC appliance

To connect the OMIMSSC appliance with the applications and devices that must be monitored by OMIMSSC, you must ensure that certain ports, protocols, and communication networks are available and enabled on OMIMSSC and the SCOM Management Servers.

Table 3. Port information for OMIMSSC appliance

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
HTTP Server	80	TCP	In	OMIMSSC Admin Portal	OMIMSSC appliance	Used for redirection from HTTP to HTTPS while loading OMIMSSC Admin Portal.
Inventory or health update to SCOM	111	TCP	In	SCOM management server	OMIMSSC appliance	Appliance permits NFS share to share the inventory details to management packs.
UI operations from the SCOM view	443	TCP	In	SCOM management server	OMIMSSC appliance	UI operations using OMIMSSC dashboard which is started from the SCOM console.
NFS Share	2049	TCP/ UDP	In	SCOM management server	NFS	NFS share that is used by OMIMSSC appliance to the managed nodes and systems that are used in enrollment and device health monitoring flow.
NFS Share	4003	TCP/ UDP	In	SCOM management server	OMIMSSC appliance	Used for mountd service.
DNS Client	53	TCP	Out	OMIMSSC appliance	DNS Server	Connectivity to DNS Server for resolving the host names.
Dynamic network configuration	67 and 68	UDP	Out	OMIMSSC appliance	DHCP Server	To get network details such as IP, Gateway, Netmask, DNS, and DHCP.
Internet	80	TCP	Out	OMIMSSC appliance	Dell Online Data Access	To connect to the Service Pack Update repository of OMIMSSC appliance for SCOM.
SNMP	161	UDP	Out	OMIMSSC appliance	Managed Nodes (iDRAC, CMC, or network devices)	To connect to the Managed Node for collecting inventory and health information.
HTTPS Server	443	TCP	Out	OMIMSSC appliance	Managed Nodes (iDRAC, CMC, or network devices)	Uses WS-Man, Redfish, or SNMP.
Windows Network Share	445/139	SMB	Out	OMIMSSC appliance	Windows Network Share	Used to back up and restore files of OMIMSSC appliance settings and data

Table 3. Port information for OMIMSSC appliance (continued)

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
PowerShell Connectivity between Appliance and Managed System Host OS	5985 and 5986	TCP	Out	OMIMSSC Appliance	SCOM Management Server	• Windows event is created using Remote PowerShell. • Dell EMC Management Pack Rules monitor the events and updates the SCOM DB.

Table 4. Port information for SCOM Management Servers and Dell EMC Alert Relay Servers

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
SNMP traps	162	UDP	In	iDRAC, CMC, network devices	All SCOM Management Servers and Dell EMC Alert Relay Servers	• OMIMSSC distributes the total devices to all the Alert Relay Servers. • Alert Relay Servers receive the alert and converts to Windows events .
Health or metrics update to SCOM	5985 and 5986	TCP	In	OMIMSSC appliance	All SCOM Management Servers	PowerShell commands are started from the appliance.
Inventory or health update to SCOM	111 and 2049	TCP and UDP	Out	All SCOM Management Servers	OMIMSSC appliance	Appliance permits NFS share to share the inventory details with management packs.
UI operations	443	TCP	Out	All SCOM Management Servers	OMIMSSC appliance	UI operations using OMIMSSC dashboard which is started from the SCOM console.

Table 5. Port information for Dell EMC devices (iDRAC, CMC, OME-Modular, or network switch)

Communication purpose	Port number	Protocols	Direction	Source	Destination	Description
SNMP traps	162	UDP	Out	iDRAC, CMC, or network devices	All SCOM Management Servers and Dell EMC Alert Relay Servers	• OMIMSSC distributes the total devices to all Alert Relay Servers. • Alert Relay Servers receive the alert and converts to Windows events.
Health, metrics, or inventory collection from devices	443	TCP	In	OMIMSSC Appliance	iDRAC, CMC, or network devices	Uses WS-Man, Redfish, or SNMP.

Support Matrix

Before you begin to deploy and configure the OMIMSSC appliance for SCOM, ensure that the following software and hardware requirements are met.

Table 6. Support Matrix

Supported software and hardware	Requirements and versions
Microsoft System Center—Operations Manager (SCOM)	One of the following SCOM build numbers must be already installed on the SCOM Management Servers: ● SCOM 2022 ● SCOM 2019—Update Rollup 3 ● SCOM 2019—Update Rollup 2 ● SCOM 2016—Update Rollup 10 ● SCOM 2012 R2—Update Rollup 14 ⓘ **NOTE:** Ensure that the SCOM build number in use is supported by Microsoft. See the Microsoft product and service life cycle information of the respective SCOM build number for details on the support dates. ⓘ **NOTE:** On systems running the Nano server version of Windows Server 2016 operating system, apply the **Update Rollup 1 for Microsoft System Center 2016 - Operations Manager** agent package that is provided in the Microsoft knowledge base article KB3190029. For more information, see support.microsoft.com/en-us/topic/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.
Microsoft Hyper-V Manager	● On Windows Server 2022: Microsoft Corporation Version: 10.0.20348 ● On Windows Server 2019: Microsoft Corporation Version: 10.0.17763.1 ● On Windows Server 2016: Microsoft Corporation Version: 10.0.14393.0 ● On Windows Server 2012 R2: Microsoft Corporation Version: 6.3.9600.16384
VMware ESXi	7.0 Update 2, 7.0 Update 1, 6.7 Update 3, and 6.5
Web browsers	To start the OMIMSSC Admin Portal, you must use one of the following web browsers: ● Microsoft Internet Explorer 11 or later ● Mozilla Firefox 30 or later ● Google Chrome 23 or later ● Microsoft Edge

Windows requirements for deploying OMIMSSC on the Management Server with the SCOM console	● Enable the following Windows firewall rules:
	  ○ 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.

RAM for the OMIMSSC appliance	Minimum of 8 GB
Processor cores for the OMIMSSC appliance	4 The CPU cores are configured by default when the OMIMSSC appliance is deployed by using the OVA format. When using the VHD format, you must configure the CPU cores for the VM during the deployment process.

Table 6. Support Matrix (continued)

Supported software and hardware	Requirements and versions
Hard drive on the system where the OMIMSSC appliance VM gets deployed.	Minimum of 40 GB

Management Server (MS) requirements

Operating systems	• For SCOM 2022, see microsoft.com/en-us/system-center/scom/?view=scom-2022. • For SCOM 2019, see microsoft.com/en-us/system-center/scom/?view=scom-2019. • For SCOM 2016, see microsoft.com/en-us/system-center/scom/?view=scom-2016. • For SCOM 2012 R2, see microsoft.com/en-us/previous-versions/system-center/system-center-2012-r2/hh546785(v=sc.12). The Chassis Detailed and Scalable editions are supported only on SCOM 2022, SCOM 2019, SCOM 2016, and SCOM 2012 R2.

Managed system requirements

OMIMSSC features	Supported software and hardware	Requirements and versions
Dell EMC Server and Rack Workstation Monitoring (Licensed)	iDRAC9-based PowerEdge servers with Lifecycle Controller	Firmware version 4.40.40.00 and earlier versions
	iDRAC8-based PowerEdge 13th generation servers with Lifecycle Controller	Firmware version 2.xx.xx.xx
	iDRAC7-based PowerEdge 12th generation servers	Firmware version 1.6x.6x and 2.xx.xx.xx
iDRAC Service Module (iSM) Monitoring Feature	iSM for iDRAC9-based and 13th generation of PowerEdge servers	4.0.1, 3.5.1, and 3.4.0
Dell EMC Chassis Monitoring Feature	Dell EMC PowerEdge FX2/FX2s	Firmware versions 2.21 and 2.20
	Dell EMC PowerEdge VRTX	Firmware versions 3.21 and 3.20
	Dell EMC PowerEdge M1000e	Firmware versions 6.21 and 6.20
OpenManage Enterprise—Modular Monitoring Feature	Dell EMC PowerEdge MX7000	Firmware versions 1.10.20 and 1.10.10
DRAC Monitoring Feature	iDRAC8 with Lifecycle Controller Modular and Monolithic	Firmware version 2.xx.xx.xx
	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
Dell EMC Network Switch Monitoring Feature	N Series of network switches	Firmware versions 6.6.xx.xx and 6.5.xx.xx
	M, S, and Z Series of network switches	Firmware versions 10.xx.xx.xx, 9.14.xx.xx, and 9.13.xx.xx

Chassis Modular Server Correlation Feature

The Chassis Modular Server Correlation feature is used for correlation of Chassis slots with its Modular blades. Modular blades could be discovered either through the Server and Rack Workstation Monitoring feature or the Server and Rack Workstation Monitoring (Licensed) feature. For the supported Dell EMC Chassis, iDRAC, iSM, and OMSA versions, see the respective supported firmware versions section.

ⓘ **NOTE:** OMIMSSC supports the enrollment of one SCOM Management Group through the enrollment of any of the SCOM Management Servers within the group.

ⓘ **NOTE:** For Gateway Servers, iDRAC should be reachable from the OMIMSSC appliance to discover devices.

Topics:

- User roles necessary for using OMIMSSC appliance for SCOM

User roles necessary for using OMIMSSC appliance for SCOM

- Create a Windows Credential Profile user account.
- The user must be a member of the following:
  - Domain user group.
  - Local administrator group on the SCOM Management Servers and Alert Relay Servers.
  - Operations Manager administrator group.

Deploy and configure the OMIMSSC appliance for SCOM

To monitor Dell EMC devices and other monitoring applications in your data center, you can use Microsoft System Center—Operations Manager (SCOM) as a common interface by integrating with the OMIMSSC appliance. As an administrator, you must deploy and configure OMIMSSC, and then enroll the associated SCOM Management Servers.

High level deployment process of the OMIMSSC appliance:

- Deploy OMIMSSC on Hyper-V or ESXi.
- Log in first time as administrator using the OMIMSSC Command Line Interface (CLI).
- Configure OMIMSSC VM after first login.
- Enroll SCOM Management Server(s) and Dell EMC Alert Relay Servers with OMIMSSC appliance for SCOM.

(i) **NOTE:** To successfully enroll SCOM Management Servers with OMIMSSC and to install the Dell EMC management packs:

- During deployment of OMIMSSC, ensure that you enable Synchronize guest time with host option on the VM.
- While configuring OMIMSSC VM network settings, under IPv4 CONFIGURATION, if you assign a Static IP address, enter the IP address and save the changes. Re-open the Configure Network option on the CLI and change the hostname. See Configure OMIMSSC VM network settings.

Deploy on Microsoft Hyper-V by using a VHD file

Deploy OMIMSSC

Deploy on VMware ESXi by using an OVA file
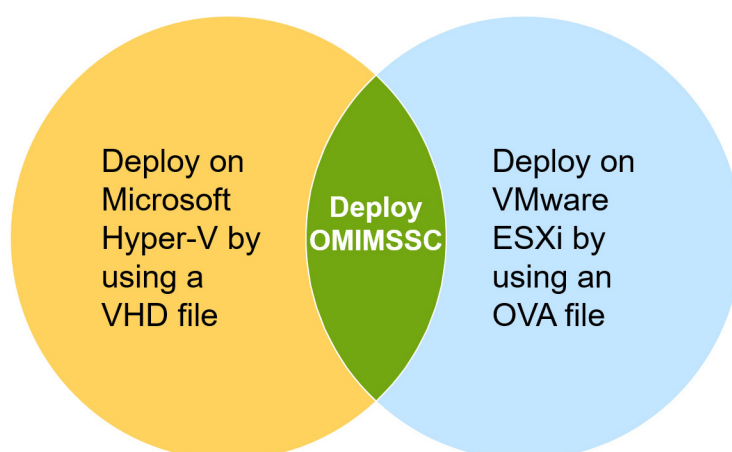
Figure 2. Deploy OMIMSSC appliance for SCOM

Before you begin to deploy the OMIMSSC appliance for SCOM, Dell Technologies recommends that you read:

- The **Support Matrix** section to know about the supported hardware and software requirements.
- The latest OMIMSSC Release Notes available on the support site for information about the new features, limitations, and known issues in OMIMSSC.

Topics:

Download OMIMSSC from the support site

Steps

1. Download the OMIMSSC ZIP file from the Dell Technologies Support Site.

   ⓘ **NOTE:** If you are unable to download your license keys, contact Dell Technologies Support. Locate the regional Dell Technologies Support phone number for your product.

2. Extract the VHD or OVA file to set up the OMIMSSC appliance.

   ⓘ **NOTE:** Before extracting the VHD file, ensure that a minimum of 60 GB disk space is available on the system where you want to deploy the OMIMSSC appliance.

Before deploying the OMIMSSC appliance for SCOM

Before deploying OMIMSSC by using either Hyper-V or ESXi methods, ensure that:

- Virtual switch or VM network is enabled within the network of the Management Group to communicate with the OMIMSSC appliance and the Management Server.
- The recommended memory space is available for VM on either Hyper-V or ESXi host. See the *Support Matrix* section.

Choose one of the following methods to deploy the OMIMSSC appliance:

- If you are using Hyper-V, then deploy a VM by using a VHD file. See Deploy and configure OMIMSSC on Hyper-V.
- If you are using VMware ESXi, then deploy a VM by using an OVA file. See Deploy and configure OMIMSSC 7.2 on ESXi.

You can set up an NTP server to synchronize the time between Hyper-V host or ESXi host and a SCOM Management Server.

Deploy and configure OMIMSSC on Hyper-V

About this task

You can deploy OMIMSSC on Hyper-V by using the Hyper-V Manager UI.

Prerequisites:

- Ensure that the software and hardware requirements are met and the necessary user roles are configured. See the *Support Matrix* section.
- Required OMIMSSC ZIP file is downloaded from the support site, and the VHD file is extracted for deployment. See Download OMIMSSC from the support site.
- Ensure that the guidelines in Before deploying OMIMSSC on Hyper-V or ESXi are followed.

To deploy OMIMSSC on Hyper-V, do the following:

Steps

1. In Hyper-V Manager, from the **Actions** menu, select **New** > **Virtual Machine**.

   The **New Virtual Machine Wizard** wizard is displayed.

   a. In the **Before You Begin** section, read through the instructions and click **Next**.

   b. In the **Specify Name and Location** section, enter a name for the VM, and then click **Next**.

   If you want to save the VM in a different location, select the **Store the virtual machine in a different location** check box. Click **Browse**, and then select a new location.

   c. In the **Specify Generation** section, select **Generation 1**, and then click **Next**.

   d. In the **Assign Memory** section, assign the disk space for the newly created VM. For example, select 8,192 MB.

   e. In the **Configure Networking** section, from the **Connection** drop-down menu, select the network that you want to use for the new VM.

   f. Click **Next**.

   g. In the **Connect Virtual Hard Disk** section, select **Use an existing virtual hard disk**.

   h. Navigate to the location where the OMIMSSC VHD file is saved, and then select the file.

   i. In the **Summary** section, confirm the data that you have provided, and then click **Finish**.

2. Set the number of virtual processors count value to 4, because by default, the processor count is set to 1. To set the processor count:
   a. In the list of VMs, right-click **OMIMSSC**, and then select **Settings**.
   b. In the **Settings** dialog box, in the left pane, select **Processor**.
   c. In the **Number of virtual processors** box, enter or select 4.
   d. Click **OK**.
3. To enable the **Time synchronization option** on the VM hosted on Hyper-V, do the following:
   a. Select the VM hosted on Hyper-V.
   b. Right-click the VM and select **Settings**.
   c. Click **Management** > **Integration Services** > **Time Synchronization**.
      The Hyper-V and SCOM Management Server times are synced.

Ensure that OMIMSSC appliance is hosted on Hyper-V

About this task

After deploying OMIMSSC on Hyper-V, to ensure that the OMIMSSC is hosted on the Hyper-V with the required configurations, do the following:

Steps

1. Right-click the OMIMSSC appliance VM and click **Settings**.
2. Ensure that the memory space and processor count are as recommended.
   a. Else, assign the memory in Startup RAM and click **Apply**.
3. Ensure that the processor count is as recommended.
   a. Else, specify the number of processors counts in **Number of Virtual processors count** under **Processors**.
4. Click **IDE Controller:IDE Controller 0** > **Hard Drive**, and then ensure that the **Virtual hard disk** field is indicating to the OMIMSSC file.
   a. Else, click **Browse**, and select the OMIMSSC extracted file.
   b. Click **Apply**.
5. Ensure that the virtual switch is connected to a physical NIC.
   a. Else, configure the NIC, and select the appropriate NIC from the **Virtual Switch** drop-down menu.
   b. Click **Apply**.
6. From the **Hyper-V Manager** menu, right-click the appliance VM and perform the following tasks:
   a. Click **Connect**, and then click **Start**.

   If the newly created VM with the selected VD of appliance fails to boot with any kernel panic exception, edit the VM settings. And, then enable the dynamic memory option for the VM.

Deploy and configure OMIMSSC on ESXi

About this task

Before deploying OMIMSSC by using ESXi, ensure that you extract the OVA file from the compressed ZIP file to a local drive. To deploy OMIMSSC on ESXi, do the following:

Steps

1. Start ESXi by using the IP address.
   The **VMware ESXI** login page is displayed.
2. Enter the username and password, and then click **Log in**.
3. In the left pane, select **Virtual Machines**.
4. To create a VM, select **Create / Register VM**.

   The **New virtual machine** wizard is displayed.

   a. In the **Select creation type** section, select **Deploy a virtual machine from an OVF or OVA file**.
   b. Click **Next**.

c. In the **Select OVF and VMDK files** section, enter a name for the VM that you want to create.

d. Select **Click to select files or drag/drop**.

e. Double-click the **OMIMSSC_xx.ova file**. The OVA management pack is uploaded to the installation process.

f. Click **Next**.

g. In the **Select storage** section, select the storage or datastore where you want to store the configuration and VD files.

h. Click **Next**.

i. In the **Deployment options** section, select the required network mappings.
   - By default, the disk provisioning feature is selected as **Thin**.
   - The option to automatically power on the VM is enabled.

j. Click **Next**.

k. In the **Ready to complete** section, verify the setting that you have specified, and then click **Finish**.

   The VM creation process is started. You can view the status in the **Recent tasks** pane.

5. Enable the Synchronize guest time with host option on the VM hosted on ESXi:

a. Select the VM and click **Edit options**.

b. Select **VM options**.

c. Select **VMware Tools** > **Time** > **Synchronize guest time with host**.

Configure the OMIMSSC appliance

About this task

After deploying the OMIMSSC appliance, log in to OMIMSSC as an administrator for the first time by doing the following:

Steps

1. In the list of VMs, right-click **OMIMSSC**, and then select **Connect**.

   By default, the VM is in powered off mode.

2. In the menu bar, click the **Start** symbol.

3. Before you try to log in, wait for five minutes so that all services are started.

4. At the CLI, enter the following:
   - localhost login=**admin**
   - Enter new Admin password=Enter a secure and strong password.
   - Please confirm new Admin password=Reenter the same password.

   ⓘ **NOTE:** Dell Technologies recommends configuring and using strong passwords to authenticate appliance admin user and the OMIMSSC Dashboard login page.

5. Press Enter.
   The Command Line Interface (CLI) is displayed.
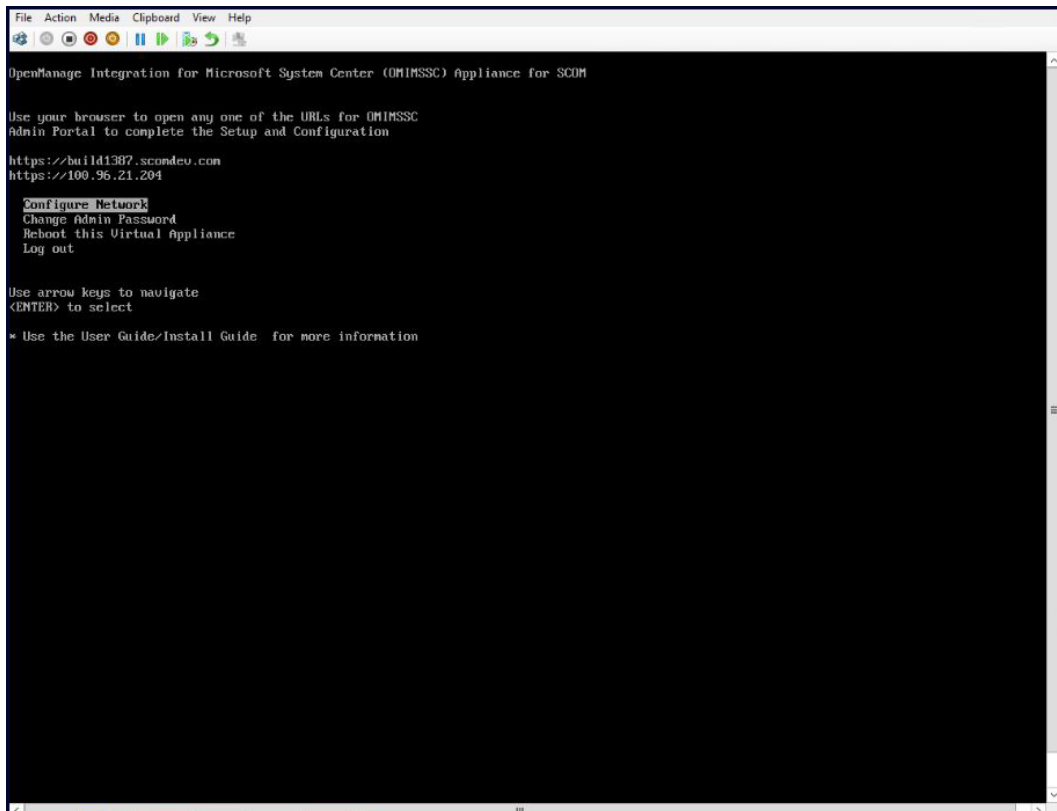
Figure 3. OMIMSSC Command Line Interface

Configure OMIMSSC VM network settings

About this task

After first logging in to OMIMSSC, to configure the OMIMSSC network setting with the SCOM Management Server, do the following:

Steps

1. On the CLI, select **Configure Network**, press Enter.
2. In the **Network Manager** section, do the following:
   a. Select **Edit a connection** and press Enter.
      i. Select the Ethernet connection—eth0, and then select **Edit**.
      ii. Press Enter.
   b. To provide an IPv4 address, select **IPv4 CONFIGURATION** and choose one of the following:
      - Automatic assignment: By default, **Automatic** is selected and a DHCP-assigned IPv4 address is automatically populated.
      - Manual assignment: Change the option to **Manual** and enter a Static IPv4 address.

      Press Enter.

   c. In DNS servers, enter the DNS IP address, and then press Enter.
   d. Select **Back** to return to the CLI, and then select **Configure Network** and press Enter.
   e. Select **Set system hostname** and press Enter.
   f. In the **Hostname** box, enter the FQDN of the host system, and then press **OK**.

      For example, **HostName.DomainName.com**.

   g. When prompted for a confirmation, press **Enter**.
3. From the CLI, note down the Admin portal URL of the newly deployed OMIMSSC appliance.

   (i) **NOTE:** Ensure that the SCOM Management Server is reachable from the OMIMSSC appliance.

> (i) **NOTE:** A hostname:
> - Can have alphanumeric characters (a–z and 0–9), hyphen (-), and a period (.).
> - Must not start with a hyphen or period.
> - Must not include other special characters such as an underscore (_).

> (i) **NOTE:** You can change the IP address of the OMIMSSC appliance by selecting the **Device configuration** option.
> - Do not change the hostname of the appliance after this point.
> - You can choose to use a static IP or a dynamic IP while configuring the appliance network settings. However, ensure that the IP address does not change while using the OMIMSSC appliance to discover and monitor devices on SCOM console.

4. Select **Quit**, and then press Enter.

OMIMSSC and SCOM interfaces for enrollment and device management

For the OMIMSSC appliance for SCOM, based on the type of device management tasks you perform, monitoring operations must be performed on the following:

- **OMIMSSC Admin Portal**—Accessed through a supported web browser, allows you to log in as an OMIMSSC administrator to enroll a SCOM Management Group with OMIMSSC appliance, modify Windows credential profiles, edit enrollment settings to change the monitoring scope, de-enroll a SCOM Management Group, backup and restore OMIMSSC appliance settings and data, view all jobs started in Dell EMC OMIMSSC by various users, view license details, console details, and to upgrade Dell EMC OMIMSSC appliance for SCOM.
- **SCOM console**—The SCOM console provides the Dell EMC state views, alert views, diagram views, and performance metrics views to view the discovered objects in the console.
- **Dell EMC OpenManage Integration Dashboard**—Appears as a view under the Dell EMC folder in the **Monitoring** pane of the SCOM console. Use this page for Dell EMC device discovery, monitoring, and performance monitoring. For example, tasks that are related to starting OpenManage Integration Dashboard from the SCOM console, discovering Dell EMC devices—PowerEdge Servers, Rack Workstations, Chassis, and Network Switches, managing device credential profiles, and managing jobs.

> (i) **NOTE:** Configure these settings on Internet Explorer (provided Internet Explorer is the default web browser) before accessing the OMIMSSC Admin Portal or Dell EMC OpenManage Integration Dashboard on the SCOM console:
> - Go to **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced** and enter the IP address and FQDN of the OMIMSSC appliance to include in the Local Intranet zone.
> - Go to **Internet Options** > **Advanced** > **Security** and clear the **Do not save encrypted pages to disk** option.

Log in to the OMIMSSC Admin Portal

About this task

> (i) **NOTE:** On Internet Explorer, configure these settings before accessing the OMIMSSC Admin Portal:
> - Go to **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced** and enter the IP address and FQDN of the OMIMSSC appliance to include in the Local Intranet zone.
> - Go to **Internet Options** > **Advanced** > **Security** and clear the **Do not save encrypted pages to disk** option.

To log in to the OMIMSSC Admin Portal:

Steps

1. Open the supported web browser and enter the OMIMSSC IP address.
   To get the OMIMSSC IP address or URL details, see Configure OMIMSSC VM network settings.
2. On the **Login** page of OMIMSSC Admin Portal, enter the OMIMSSC admin password.
   The OMIMSSC admin password is set while configuring the OMIMSSC appliance. See Configure the OMIMSSC appliance.
3. Click **Log In**.

The Dell EMC OpenManage Integration for Microsoft System Center-Admin Portal page is displayed.
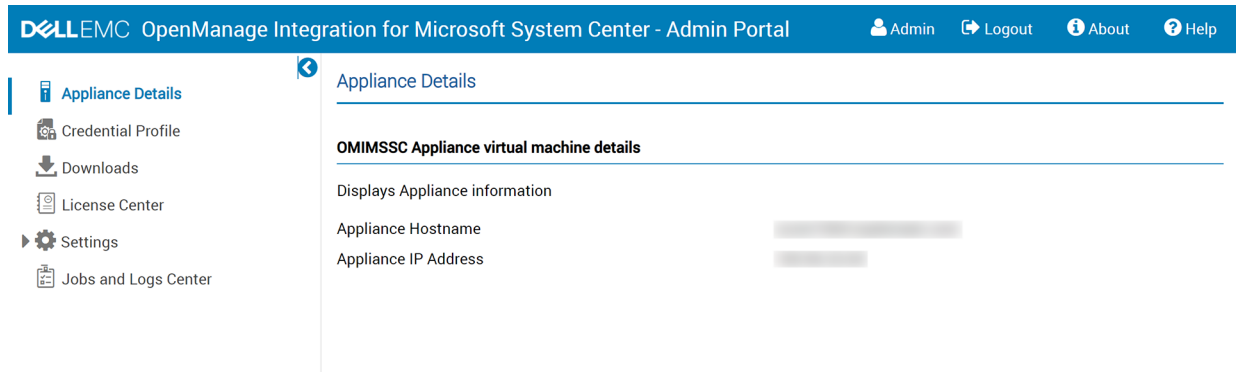
Figure 4. OMIMSSC Admin Portal

View the current version, hostname, and IP address of the OMIMSSC appliance

Steps

1. Log in to the OMIMSSC Admin Portal as an OMIMSSC administrator.
2. To view the OMIMSSC appliance version, in the upper right corner, click **About**.
   The deployed build and version of the OMIMSSC appliance for SCOM is displayed.
3. On the Admin Portal, expand the left pane and click **Appliance Details**.
   The appliance hostname and IP address are displayed in the working pane.

Enrolling (registering) SCOM Management Group with OMIMSSC appliance for SCOM

After deploying the OMIMSSC appliance for SCOM and configuring its network properties with the SCOM Management Server, you must enroll the SCOM Management Server(s) with the OMIMSSC appliance. During the enrollment, the following activities are performed:

- All prerequisites are configured on the Management Servers.
- The Dell EMC management packs are copied to the Management Servers, and then imported to the SCOM console.

After the enrollment job is complete, you can discover and monitor Dell EMC devices on the SCOM console using OMIMSSC for SCOM.If there are multiple SCOM Management Servers within a SCOM Management Group, all Management Servers within the group are enrolled with the OMIMSCC appliance. If a SCOM Management Server is added or deleted from All Management Server Resource Pool (AMSRP), you must synchronize the SCOM console data that are enrolled with OMIMSSC. See Synchronize details of Management Servers and Dell EMC Alert Relay.

Scalability with OMIMSSC appliance for SCOM

When you add more devices to scale up your infrastructure, you can seamlessly scale up your monitoring capabilities by adding Dell EMC Alert Relay Servers (previously known as Proxy Management Servers) in to your SCOM environment. Dell EMC Alert Relay Servers enables you to offload the monitoring, performance metrics, and SNMP alerts' workflows from the Management Server, and thus helps in scaling up the number of devices being monitored within a SCOM Management Group. Discover Alert Relay Server as an Agent-Managed Windows system in the SCOM console.

Ensure that SCOM Management Servers and Dell EMC Alert Relay Servers are in the same domain.

On each of the identified systems, download and install the **Dell EMC Alert Relay Server Installer** from the **Downloads** page on the OMIMSSC Admin Portal. To configure and onboard Alert Relay Servers, see Setting up Dell EMC Alert Relay Servers. For more information about scalability with OMIMSSC appliance for SCOM, see the **Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) technical white paper** on the support site.

Topics:

- Create Windows Credential Profile
- Enroll SCOM Management Group and Dell EMC Alert Relay Servers with OMIMSSC for SCOM
- Modify enrollment settings
- Configuring and onboarding Dell EMC Alert Relay Servers

Create Windows Credential Profile

About this task

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of a user. Each credential profile contains a username and password for a single user account. A Windows Credential Profile is used to enroll SCOM Management Group with the OMIMSSC appliance for SCOM and to back up and restore OMIMSSC appliance data from a Windows Network Share path.

To create a Windows credential profile:

Steps

1. On a supported web browser, provide the OMIMSSC appliance IP address and log in as an OMIMSSC ADMIN user.
   The **Dell EMC OpenManage Integration for Microsoft Windows Center—Admin Portal** page is displayed.
2. To expand the left pane, click the **>** icon, and then select **Credential Profile**.
3. In the working pane, click **Create**, and then enter or select the following data:
   a. By default, **Windows Credential Profile** is selected from the **Credential Profile Type** drop-down menu.

b. Enter a name and description for the profile.

c. Under the **Credentials** section, enter the user credentials of a user who will enroll SCOM Management Server(s) with OMIMSSC or access a Windows Network Share Path to back up and restore OMIMSSC appliance data.

   The user must be a domain user with local administrative privileges on all the Management Servers in the Management Group and must be added to the Operations Manager Administrator role.

d. Enter domain name of the SCOM Management Group.

4. Click **Finish**.

Results

The new Windows Credential Profile is successfully created, and then listed on the **Credential Profiles** page.

Modify Windows Credential Profile

Steps

1. On the OMIMSSC Admin Portal, to expand the left pane, click the **>** icon, and then select **Credential Profile**.
2. Select the Windows Credential Profile that you want to edit, and then click **Edit**.
3. Modify the settings and click **Finish**.

Delete Windows Credential Profile

About this task

ⓘ **NOTE:** A Windows Credential Profile being used in a enrollment or edit enrollment job cannot be deleted.

Steps

1. On the OMIMSSC Admin Portal, to expand the left pane, click the **>** icon, and then select **Credential Profile**.
2. Select the Windows Credential Profile that you want to delete, and then click **Delete**.
3. On the **Delete Credential Profiles** page, click **Yes** to provide your confirmation to delete the Windows Credential Profile.

Enroll SCOM Management Group and Dell EMC Alert Relay Servers with OMIMSSC for SCOM

Prerequisites

Enable Remote PowerShell on all SCOM Management Servers.

Steps

1. On a supported web browser, enter the IP address of the OMIMSSC appliance and log in as an OMIMSSC ADMIN user.
   You must use the OMIMSSC ADMIN user credentials set during the configuration of OMIMSSC appliance for SCOM. See Configure the OMIMSSC appliance.
2. To expand the left pane, click the **>** icon, and then select **Settings** > **Console Enrollment**.
3. In the working pane, click **Enroll**.
4. In the **Introduction to Onboarding OMIMSSC for SCOM** dialog box, an overview of enrollment process of the SCOM Management Server(s) with OMIMSSC appliance for SCOM, the steps that are involved in setting up the Dell EMC Alert Relay Servers, and to discover devices using OMIMSSC for SCOM are provided. Read the information and click **Next**.
5. To enroll Management Group with the OMIMSSC appliance for SCOM:
   a. Enter a name for the enrollment.
   b. In the **SCOM MS FQDN** box, enter the FQDN of a SCOM Management Server in the SCOM Management Group.
   c. From the **Credentials** drop-down menu, select a Windows credential profile with local administrative privileges on the SCOM Management Server and Operations Manager administrative privileges.

      To create a credential profile, see Create Windows type credential profile for enrolling a SCOM console.

d. To verify the connection between OMIMSSC appliance and SCOM Management Server, click **Test Connection**. If the test connection is successful, the following message is displayed: `Test connection is successful.`

e. To receive alerts from the discovered Dell EMC devices on the SCOM console, enter the SNMP community name for SNMP v1 or v2 .

The DellEMC_OMIMSSC_SNMP_RunAsAccount is created and is associated with the SNMP Monitoring Account Profile on the SCOM console. This RunAsAccount is targeted for all Dell EMC Hardware devices. To change the target device objects, wait for the enrollment job to complete, and then open the SCOM console and select **Administration** > **Run As Configuration** > **Profiles** > **SNMP Monitoring Account**. Select **DellEMC_OMIMSSC_SNMP_RunAsAccount** and click **Edit** to change associated class.

f. Under **Monitoring scope**, select the device types that you want to monitor using the OMIMSSC appliance for SCOM.

(i) **NOTE:** At least one of the device types must be selected under **Monitoring scope** to proceed with the enrollment job.

g. Under **Monitoring mode**, select either **Scalable** or **Detailed** mode for device monitoring using OMIMMSC for SCOM.

In the Scalable mode, you can view basic device and component group-level inventory and health monitoring metrics. And, in the Detailed mode, you can view detailed device and component-level inventory (such as memory, processors, and storage controllers) and health monitoring metrics (such as power and temperature).

Using the Detailed mode of monitoring, up to 300 devices can be monitored. When the number of monitored devices exceeds the maximum limit, OMIMSSC automatically changes the monitoring mode to Scalable.

h. Click **Next**.

i. Click **Apply** to start the enrollment job.
The enrollment sub-tasks are executed, and the status of each sub-task is listed. The time taken to complete the subtasks is 30 to 40 minutes and depends on the existing load of the SCOM servers. To view the status of the enrollment job and the associated logs, click **Settings** > **Jobs and Logs**. The enrollment job is listed, and to view the subtasks, expand the enrollment job. The **Progress Status** column displays the progress of the enrollment job.

If any of the sub-tasks are unsuccessful, under **Jobs and Logs** > **History**, expand the enrollment job to view the status of subtasks and the associated logs. You can also see the Troubleshooting section to resolve the issues.

j. Click **Next**.

6. To configure and onboard Dell EMC Alert Relay Servers:
   a. Discover Alert Relay Server as an Agent-Managed Windows system on the SCOM console.
   b. Download and install the **Dell EMC Alert Relay Server Installer** from the OMIMSSC Admin Portal on each of the Agent-Managed Windows system to be used as Alert Relay Servers. For more information about installing and configuring Dell EMC Alert Relay Servers, see Setting up Dell EMC Alert Relay Servers.
   c. On the SCOM console, after the Alert Relay Servers are listed under the Dell EMC Alert Relay Server State View, synchronize the Alert Relay Servers details with the OMIMSSC appliance by navigating to **Monitoring** > **Dell EMC** > **Dell EMC OpenManage Integration Views** > **Dell EMC OpenManage Integration Dashboard**. On the **Overview** page, select **Sync with SCOM MS**.

7. Click **Finish**.

Results

The Management Server with the SCOM console is successfully enrolled to the OMIMSSC appliance and listed on the **Console Enrollment** page.

● It may take 15 to 20 minutes for all the OMIMSSC—related management packs to get imported into the SCOM console. Event ID 71 is generated. See the enrollment job logs under **Jobs and Logs** > **History** for information about the configuration changes.

● During the enrollment process, all the Dell EMC management packs are copied from the OMIMSSC appliance to the SCOM Management Server and are saved in the folder: `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<version>`. Based on the devices selected for monitoring, the required management packs are imported into the SCOM console.

● The following prerequisites are automatically configured by the OMIMSSC appliance:
  ○ On the SCOM Management Servers—
    ▪ The client for NFS feature on the Windows server is enabled.
    ▪ The persistence version store maximum value is set to 131072.
  ○ On the Dell EMC Alert Relay Servers—
    ▪ Registry entries "HKLM:\\SOFTWARE\\Dell\\Dell Server Management Pack Suites" are set.
    ▪ The WinRM rule is added to firewall.
    ▪ The WinRM client and server authentication are enabled.

- To troubleshoot any issues during or after the enrollment, see Troubleshooting.

If there are multiple SCOM Management Servers within the SCOM Management Group, this process enrolls all the SCOM Management Servers within that SCOM Management Group. If a SCOM Management Server is added or deleted from All Management Server Resource Pool (AMSRP), synchronize the SCOM console data that are enrolled with OMIMSSC. See Synchronize details of Management Servers and Dell EMC Alert Relay.

ⓘ **NOTE:** Informational event (event ID 71) is generated in the Windows Event Viewer under **Windows Logs** > **Application**. This event contains information about the prerequisites which get configured on the SCOM Management Servers.

The **Dell EMC OpenManage Integration Dashboard** link is displayed under the **Monitoring** > **Dell EMC** > **Dell EMC OpenManage Integration Views** pane of the SCOM console. You can now start discovering and monitoring your devices by using the Dell EMC OpenManage Integration Dashboard or through the SCOM console.

⚠ **WARNING: Before you try to enroll SCOM Management Servers (in a SCOM Management Group) to a different OMIMSSC appliance for SCOM, ensure that you de-enroll them from the current appliance. For more information about de-enrolling the Management Servers from OMIMSSC appliance for SCOM, see De-enroll (Deregister) SCOM Management Server(s) enrolled to OMIMSSC for SCOM.**

Modify enrollment settings

About this task

You can edit the enrollment settings using the **Edit** option on the **Console Enrollment** page.

You can use the edit enrollment option to:

- Change the Windows Credential Profile.
- Update the SNMP v1 or v2 Community Name.
- Change the monitoring scope and mode of the devices that you want to monitor on the SCOM console.
- Re-run the enrollment job when any of the sub tasks of the enrollment job is unable to complete.

ⓘ **NOTE:** On the **Console Enrollment** page, the **Edit** option to modify the enrollment settings is disabled when an enrollment, de-enrollment, or force de-enrollment job is in progress. Wait for these jobs to complete before editing the enrollment settings.

Steps

1. On a web browser, enter the IP address of the OMIMSSC appliance and log in as an OMIMSSC ADMIN user.
2. To expand the left pane, click the **>** icon, and then select **Settings** > **Console Enrollment**.
3. In the working pane, select the enrollment and click **Edit**.
   The **Edit Enrollment Settings** page is displayed.
4. You can edit the following settings:
   a. Name of the enrollment.
   b. In the **SCOM MS FQDN** box, enter an FQDN of the new SCOM Management Server to be enrolled with the OMIMSSC appliance.

      This new FQDN is listed as a new entry on the **Console Enrollment** page.
   c. From the **Credentials** drop-down menu, you can select a different Windows Credential profile with local administrative privileges on the SCOM Management Server and Operations Manager administrative privileges.

      To create a credential profile, see Create Windows type credential profile for enrolling a SCOM console.
   d. To verify the connection between OMIMSSC appliance and SCOM Management Server, click **Test Connection**.
      If the test connection is successful, the following message is displayed: Test connection is successful.
   e. The SNMP community name for SNMP v1 or v2.

      A Run As account, named DellEMC_OMIMSSC_SNMP_RunAsAccount, is created and gets associated with the SNMP Monitoring Account Profile on the SCOM console. This is used to receive alerts from the discovered Dell EMC devices on SCOM console.
   f. Under **Monitoring scope**, you can change the device types that you want to monitor using the OMIMSSC appliance for SCOM.

      ⓘ **NOTE:** At least one of the device types must be selected under **Monitoring scope** to proceed with the enrollment job.

g. Under **Monitoring mode**, select either **Scalable** or **Detailed** mode of device monitoring using OMIMMSC for SCOM. If the number of monitored Dell EMC devices exceeds 300, then you can select only Scalable mode of monitoring.

h. Click **Next**.
    The **Edit Enrollment Settings - Apply Changes** page is displayed.

i. Click **Apply** to start the edit enrollment job.
    The sub tasks in the edit enrollment job are started and the status of each sub task is listed. Wait for 20 to 40 minutes until the sub tasks of the edit enrollment job are completed.

    To view the status of the job that is created and the logs that are associated with the edit enrollment job, select **Jobs and Logs**, and then select the **Running Jobs** tab. The edit enrollment job is listed and to view the sub tasks, expand the edit enrollment job. The **Progress Status** column displays the progress of the enrollment job.

    If any of the sub tasks are unsuccessful, under **Jobs and Logs** > **History**, expand the edit enrollment job to view the status of sub tasks and the associated logs. You can also see the Troubleshooting section in the user's guide to resolve the issues.

j. Click **Next**.

Results

After the edit enrollment job completes successfully, the SCOM Management Servers are listed on the **Console Enrollment** page.

Based on the current enrollment settings changes and the previous enrollment configurations, OMIMSSC configures the prerequisites on the SCOM Management Server accordingly. The Dell EMC management packs are either deleted or imported into the SCOM console depending on the device monitoring scope and mode that is selected during the edit enrollment job.

Configuring and onboarding Dell EMC Alert Relay Servers

The Dell EMC OpenManage Integration with Microsoft Windows System Center (OMIMSSC) appliance for System Center Operations Manager (SCOM) provides an option to configure Dell EMC Alert Relay Servers (previously known as Proxy Management Servers). When you want to scale up your infrastructure by including more devices, you can seamlessly scale up your monitoring capabilities by adding Alert Relay Servers in to your OMIMSSC environment.

Alert Relay Servers system requirements

The following are the minimum software and hardware requirements of a Windows VM on the managed node to host Alert Relay Servers.

- Supported operating system on the managed node for:
  - SCOM 2022, see the **Server operating system** section at microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2022.
  - SCOM 2019, see the **Server operating system** section at microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2019.
  - SCOM 2016, see the **Server operating system** section at microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2016.
  - SCOM 2012 R2, see the **Server operating system** section at microsoft.com/en-us/previous-versions/system-center/system-center-2012-r2/hh546785(v=sc.12).
- CPU Cores—8
- RAM—32 GB

Prerequisites for setting up Alert Relay Servers for scaling up the number of monitored devices

- Ensure that you are a domain user with local administrator privileges on the Management Server and you are assigned the Operations Manager administrator role to install and configure Alert Relay Servers in the SCOM Management Group.
- SCOM agent must be installed on the Windows VM to be used as a Dell EMC Alert Relay Server.
- Ensure that Alert Relay Servers is discovered as an agent-based system on the SCOM console.

- Apply Microsoft public hotfix— microsoft.com/en-us/topic/system-center-operations-manager-snmp-modules on each of the SCOM server and all Alert Relay Servers in the Scalability setup. On the Alert Relay Server, locate **SnmpModules.dll** in `C:\Program Files\Microsoft Monitoring Agent\Agent\SnmpModules.dll`.

(i) **NOTE:** Ensure that Alert Relay Server is hosted on a Management Server that is part of the All Management Servers Resource Pool (AMSRP).

Discover Alert Relay Servers on the SCOM console

Steps

1. In the left pane of the SCOM console, select **Administration** and click **Discovery Wizard**.
2. Select **Windows computers** and click **Next**.
3. Select **Advanced discovery** and from the **Management Server** drop-down menu, select a Management Server in the Management Group, and then click **Next**.
4. Select **Browse for, or type-in computer names** and click **Browse**.

   Provide the Alert Relay Server details to be discovered on the SCOM console.
5. Click **Discover**.

Results

After the Dell EMC Alert Relay Server is discovered, it is listed on the SCOM console under **Administration** > **Device Management** > **Agent Managed**.

Download and install Dell EMC Alert Relay Server Installer from the OMIMSSC Admin Portal

Steps

1. On a web browser, provide the OMIMSSC appliance IP address and log in as an OMIMSSC ADMIN.

   Use the OMIMSSC ADMIN user credentials set during the configuration of OMIMSSC appliance for SCOM. See the **Configure the OMIMSSC appliance** section in the **Dell EMC OpenManage Integration with Microsoft System Center for System Center Operations Manager User's Guide** on the Dell Technologies support site.
2. On the OMIMSSC Admin Portal, to expand the left pane, click the **>** icon, and then select **Downloads**.
3. Click **Dell EMC Alert Relay Server Installer**.

   Save the installer on each of the Alert Relay Server in the SCOM Management Group.
4. Double-click the **DellEMCAlertRelayServerInstaller.msi** file and click **Next**.
5. Read the license agreement and to accept the license terms, select **I accept the terms in the license agreement**, and then click **Next**.
6. Click **Install**.

Results

(i) **NOTE:** It is recommended that you do not delete the Dell EMC Alert Relay Server Installer from the downloaded location. You can uninstall Dell EMC Alert Relay Server Installer only using the downloaded MSI file.

Configuration changes performed by Dell EMC Alert Relay Server Installer

The following configurations are set after the Dell EMC Alert Relay Server Installer is installed on the Alert Relay Servers:

- Logs are created under `C:\Users\<admin>\AppData\Local\Temp\Dell EMC.OMIMSSC.Configuration`.
- Event ID 72 is generated in the Windows Event Viewer under **Windows Logs** > **Application**. The Alert Relay Server-related configurations are listed under the **General** tab.
- Registry entries are created under **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Dell** > **DSMPS**.

- Health services-related registry entries are updated under **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **HealthService** > **Parameters**.
    - Persistence Version Store Maximum Registry Path is set to 131072.
    - Maximum Global Pending Data Count Registry is set to 20408.
    - State Queue Items Registry is set to 20480.
    - Persistence checkpoint Depth Maximum Registry is set to 20971520.
    - Microsoft Monitoring Agent Health Services are started.
- (i) **NOTE:** For more information about registry key settings, see microsoft.com/en-us/archive/blogs.

During the enrollment of SCOM Management Servers with OMIMSSC appliance for SCOM, the following Dell EMC management packs for Alert Relay Servers are automatically imported to the SCOM console: **Dell EMC Alert Relay Server Model** and **Dell EMC Alert Relay Server View**.

Monitoring views of Dell EMC Alert Relay Servers

Steps

1. In the left pane of the SCOM console, select **Monitoring**, and then expand:
    a. **Dell EMC** > **Dell EMC Diagram Views** > **Dell EMC Alert Relay Server Diagram View** to view a hierarchical and graphical representation of Alert Relay Servers on the network.
    b. **Dell EMC** > **Dell EMC State Views** > **Dell EMC Alert Relay Server State View** to view the status of Alert Relay Servers managed by SCOM on the network.
2. To view more information, select an Alert Relay Server in the list.
   The details of Alert Relay Servers are displayed in the **Detail View** section.

Synchronize Alert Relay Servers with OMIMSSC appliance for SCOM

Steps

1. In the left pane of the SCOM console, select **Monitoring** and expand **Dell EMC OpenManage Integration Views** > **Dell EMC OpenManage Integration Dashboard**.
2. Log in to OMIMSSC by using the local administrative privileges of the Management Server.
3. On the home page, scroll down to the **Synchronized SCOM Management Servers and Dell EMC Alert Relay Servers** section and click **Sync with SCOM MS**.
4. After the sync task is complete, the Alert Relay Servers count is updated. Click **View Alert Relay Servers** to view the discovered Alert Relay Servers.

Next steps

Wait for 15 minutes for the OMIMSSC appliance to be updated with new Alert Relay Server information, and then continue to perform discovery of Dell EMC devices.

Repair Dell EMC Alert Relay Server Installer installation errors

Steps

1. From the downloaded location, double-click the **DellEMCAlertRelayServerInstaller.msi** file and click **Next**.
2. Select **Repair**, and then click **Next**.
3. Click **Install**.

Results

During the repair of the Dell EMC Alert Relay Server Installer, note that:
- Installation logs are not removed from the `C:\Users\<admin>\AppData\Local\Temp\Dell EMC.OMIMSSC.Configuration` location.

- Registry entries under **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **HealthService** > **Parameters** are restored to the previous values.

ⓘ **NOTE:** After repairing the Dell EMC Alert Relay Server Installer, if required, you must manually update the values of the registry entries.

Next steps

If repairing the Dell EMC Alert Relay Server Installer fails or if any installation issue persists, then you can manually restore the registry settings using the registry backup that is created by the Dell EMC Alert Relay Server Installer and install Dell EMC Alert Relay Server Installer using the configuration scripts available in the `C:\Program Files\Dell Management Packs\Automation` location.

Uninstall Dell EMC Alert Relay Server Installer

About this task

⚠ **WARNING: Uninstalling the Dell EMC Alert Relay Server Installer stops the monitoring of Dell EMC devices that are associated with the respective Alert Relay Server. Therefore, ensure that correct number of Alert Relay Servers are available to continue monitoring the Dell EMC devices on the SCOM console.**

ⓘ **NOTE:**
- Before uninstalling the Dell EMC Alert Relay Server Installer, close the `C:\Program Files\Dell Management Packs` folder to ensure that all the associated Alert Relay Server files are successfully removed.
- The Dell EMC Alert Relay Server Installer cannot be uninstalled using the Windows Control Panel.

Steps

1. [Optional] If the Dell EMC Alert Relay Server Installer is deleted from the system, access the Dell EMC OMIMSSC Admin Portal, and then select **Downloads** in the left pane and download the installer.
2. From the downloaded location, double-click the **DellEMCAlertRelayServerInstaller.msi** file and click **Next**.
3. Select **Remove**, and then click **Next**.
4. Click **Remove** and to confirm uninstalling Dell EMC Alert Relay Server Installer, click **Yes**.
5. Click **Finish**.

Results

ⓘ **NOTE:** When you uninstall the Dell EMC Alert Relay Server Installer, logs are not removed from the system.

After the Dell EMC Alert Relay Server Installer is successfully uninstalled, the Alert Relay Servers will no longer be listed under **Administration** > **Device Management** > **Device Management** > **Agent Managed**. The corresponding Dell EMC Alert Relay Server Diagram View and Dell EMC Alert Relay Server State View will not be displayed. Event ID 74 is generated in the Windows Event Viewer with details related to the registry updates performed during the uninstallation.

When you select **Dell EMC OpenManage Integration Dashboard** > **Sync with SCOM MS**, a warning message is displayed informing you that all the associated devices with the Alert Relay Server will no longer be monitored and will be removed from the SCOM console. The devices must be rediscovered to be monitored on the SCOM console by the OMIMSSC appliance.

Other tasks you can perform on the OMIMSSC Admin Portal

The following sections provide details on the other tasks that you can perform on the OMIMSSC Admin Portal.

Topics:

* OMIMSSC SSL Certificates
* Jobs and logs in OMIMSSC Admin Portal and OpenManage Integration Dashboard
* Downloading OMIMSSC appliance troubleshooting logs

OMIMSSC SSL Certificates

Dell EMC OMIMSSC appliance for SCOM uses certificates for secure HTTP access (HTTPS). By default, OMIMSSC installs and uses the self-signed certificate for the HTTPS secure transactions. For stronger security, it is recommended to use the Certificate Authority (CA) signed or custom certificates. The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server. The self-signed certificate cannot be used for authentication.

The Dell EMC OMIMSSC appliance uses the OpenSSL API to create the Certificate Signing Request (CSR). The RSA encryption standard with a 2048–bit key length is used. The CSR generated by OMIMSSC gets a digitally signed certificate from a trusted certification authority. The OMIMSSC uses the digital certificate to enable HTTPS on the web server for secure communication.

You can use the following types of certificates for OMIMSSC authentication:

* A self-signed certificate: OMIMSSC generates self-signed certificates when the hostname of the appliance changes.
* A signed certificate by a trusted Certificate Authority (CA) vendor.

(i) **NOTE:** Consider company policies when creating certificates.

Generate a Certificate Signing Request (CSR)

Generating a new CSR prevents certificates that were created with the previously generated CSR from being uploaded to the appliance. To generate a CSR, do the following:

1. On the OMIMSSC Admin Portal, expand the left pane and select **Settings** > **Security**.
2. On the **OMIMSSC SSL Certificates** page, click **Generate Certificate Signing Request**.
3. In the **Generate Certificate Signing Request** dialog box, enter the details such as Distinguished Name, Primary Subject Alternate Name, business name, department name, locality, state, country or region, and email address.
4. Click **Generate**.
5. Click **Download**, and then save the resulting CSR to an accessible location.

(i) **NOTE:** In Internet Explorer, you must enable the option to allow file downloads. For more details, see Unable to download Certificate Signing Request using Internet Explorer.

Upload a CA-signed certificate

Ensure that the certificate uses the PEM format.

You can use the HTTPS certificates for secure communication between the OMIMSSC appliance and host systems or OMIMSSC. To establish secure communication, send the CSR certificate to a certificate signing authority, and then upload the signed certificate using the OMIMSSC Admin Portal.

1. On the OMIMSSC Admin Portal, expand the left pane and select **Settings** > **Security**.
2. On the **OMIMSSC SSL Certificates** page, click **Upload Certificate**.
3. Select **Browse**, and select the certificate.

4. Click **Upload**.

(i) **NOTE:** While the certificate is being uploaded, the OMIMSSC appliance may be unresponsive for a few minutes and the services are restarted. After the task is completed, it is recommended to close all existing browser sessions of OMIMSSC Admin Portal and Dell EMC OpenManage Integration Dashboard on the SCOM console. Log in again to the OMIMSSC Admin Portal to view the uploaded certificate.

Restore default certificate

1. On the OMIMSSC Admin Portal, expand the left pane and select **Settings** > **Security**.
2. On the **OMIMSSC SSL Certificates** page, click **Restore Default Certificate**.
3. To confirm, click **Yes**.

(i) **NOTE:** While the certificate is being restored, the OMIMSSC appliance may be unresponsive for a few minutes, and the services restart. After the task completes, clear the browser cache, close the existing browser sessions of OMIMSSC Admin Portal and Dell EMC OpenManage Integration Dashboard on the SCOM console. Log in again to the OMIMSSC Admin Portal.

Jobs and logs in OMIMSSC Admin Portal and OpenManage Integration Dashboard

You can view all information about the tasks initiated in OMIMSSC along with a job's progress status, and its sub task by using the **Jobs and Logs** page. Also, you can filter and view jobs for a category. You can view the jobs from the OMIMSSC Admin Portal and OpenManage Integration dashboard.

Job names are provided by users or are system generated, and the sub tasks are named after the IP address of the managed server. Expand the sub task to view the activity logs for that job. There are four categories of jobs.

- **Running**—Lists jobs that are either currently running or are in-progress state.
- **History**—Lists jobs run in the past along with its job status.
- **Scheduled**—Lists jobs scheduled for a future date and time. Also, you can cancel the scheduled jobs.
- **Generic Logs**—Lists OMIMSSC appliance-specific, common log messages that are not specific to a sub task, and other activities for every user specifying the username and console FQDN.
  - **Appliance logs**—Displays all OMIMSSC appliance-specific log messages such as enrolling Management Server with OMIMSSC and restarting OMIMSSC. Available only in the OMIMSSC Admin Portal.
  - **Generic logs**—Displays all log messages that are common across jobs that are listed in the Running, History, and the Scheduled tabs. These logs are specific to a console and a user.

The various states of jobs defined in OMIMSSC are:

- **Canceled**—The job either manually canceled by you or when OMIMSSC restarts.
- **Successful**—The job is successfully completed.
- **Failed**— The job could not be successfully run.
- **In Progress**—The job is running.
- **Scheduled**—The job has been scheduled for a future time.
- **Waiting**—The job is in a queue to start running.
- **Recurring**—The job will repeatedly run after a fixed interval of time.

(i) **NOTE:** If multiple jobs are submitted at the same time to the same server, the jobs fails. Therefore, ensure that you schedule jobs at different times.

View OMIMSSC jobs and logs

About this task

By using the OMIMSSC Admin Portal or the OpenManage Integration Dashboard (can be viewed on the SCOM console itself), you can view the status of different types of jobs—running, schedules, and completed (history). To view the job status:

Steps

1. Log in to the OMIMSSC Admin Portal or Dell EMC OpenManage Integration Dashboard.
2. In the left pane, click **Jobs and Log Center**.
3. To view a specific category of job, such as Running, Scheduled, and History, click the respective tab.
   A list of jobs under the selected category is displayed. Jobs are classified based on the devices monitored by OMIMSSC.
4. To view information about jobs running on a device, expand the job name. Expand further to view the log messages for that job.
5. (Optional) To view jobs of different categories, use the filters. You can also view its status in **Status** column.
6. To view the job-related generic log messages, select the **Generic logs** tab and expand **Generic logs**.
7. On the OMIMSSC Admin Portal, to view the appliance specific log messages, select the **Generic logs** tab and expand **Appliance logs**.
   The **Appliance logs** option is not available on the Dell EMC OpenManage Integration Dashboard.

Downloading OMIMSSC appliance troubleshooting logs

About this task

The OMIMSSC appliance provides an option to download a ZIP file with detailed log information about the completed activities using the OMIMSSC appliance.

(i) **NOTE:** The downloaded troubleshooting bundle will not carry logs collected from SCOM Management Servers and Dell EMC Alert Relay Servers.

To download the troubleshooting bundle:

Steps

1. On the OMIMSSC Admin Portal, expand the left pane and select **Settings** > **Logs**.
2. Click **Download Troubleshooting Bundle**.

Results

To view the logs, extract the downloaded file and select the required log file containing the details specific to that category.

Manage OMIMSSC from the SCOM console

The key feature of the OMIMSSC appliance is that it enables you to monitor and manage your Dell EMC devices by using the SCOM console as a single common interface. To manage devices by using the SCOM console, you must import and deploy specific Dell EMC management packs from OMIMSSC to the SCOM console.

Topics:

Access Dell EMC OpenManage Integration Dashboard by using the SCOM console

About this task

To discover and manage your Dell EMC devices, you can log in to the Dell EMC OpenManage Integration Dashboard by using the SCOM console. If the current IP address of OMIMSSC is changed, you can Override the current OMIMSSC IP address using the new IP address.

(i) **NOTE:** On Internet Explorer, configure these settings before accessing the Dell EMC OpenManage Integration Dashboard on the SCOM console:

*   Go to **Internet Options** > **Security** > **Local Intranet** > **Sites** > **Advanced** and enter:
    *   The IP address and FQDN of the OMIMSSC appliance.
    *   Links—`about:security_Microsoft.EnterpriseManagement.Monitoring.Console.exe`, `about:internet`, and `about:blank` to include in the Local Intranet zone.
*   Go to **Internet Options** > **Advanced** > **Security** and clear the **Do not save encrypted pages to disk** option.

To log in to the Dell EMC OpenManage Integration Dashboard from SCOM console:

Steps

1. In the left pane of the SCOM console, select **Monitoring**, and expand **Dell EMC** > **Dell EMC OpenManage Integration Views**.
2. Select **Dell EMC OpenManage Integration Dashboard**.
3. In the working pane, log in with the local administrator credentials of the SCOM Management Server.
    The **Overview** page of Dell EMC OpenManage Integration Dashboard is displayed.
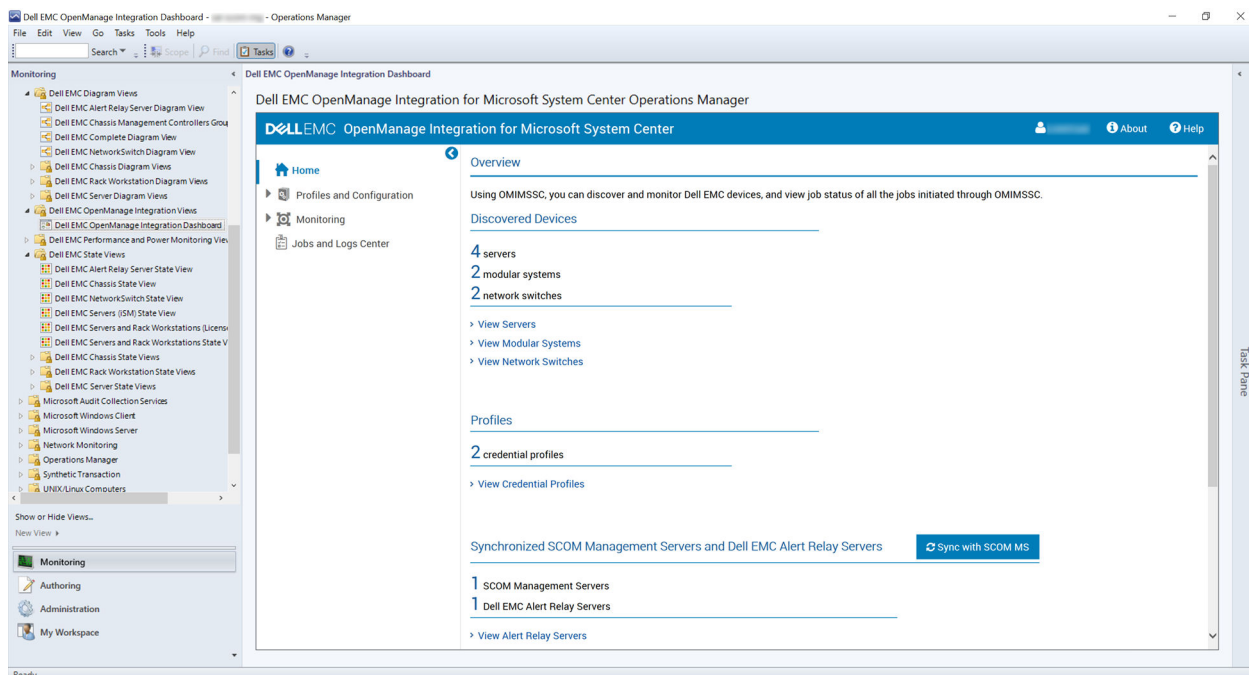
Figure 5. Dell EMC OpenManage Integration Dashboard—Overview page

Override the current OMIMSSC IP address using the new IP address

Steps

1. In the left pane of the SCOM console, select **Authoring** and expand **Management Pack Objects** > **Monitors**.
2. In the **Look for** field, search for `Appliance` and scroll down to **Management Server** > **Dell EMC SDK Override Appliance IP** .
3. Under **Dell EMC Appliance IP**, change the override value to a new IP address.
4. Save the overwritten information to **Dell EMC SDK Appliance IP override** management pack.

Create Device Credential Profile

About this task

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of a user. Each credential profile contains a username and password for a single user account. OMIMSSC uses Device Credential Profiles which consists of the credentials, SNMP community string, HTTPS port number, and SNMP port number fields which are used to access an iDRAC console, Chassis Management Controller, OpenManage Enterprise-Modular, or a network switch management console. The fields that are displayed vary based on the selected protocol. For example, HTTP provides username, password, and port number options.

ⓘ **NOTE:** A Device Credential Profile is used for discovery of a server, a modular system, or a network switch.

To create a Device Credential Profile from Dell EMC OpenManage Integration Dashboard:

Steps

1. In the left pane of SCOM, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC OpenManage Integration Dashboard**.
3. Log in to the Dell EMC OpenManage Integration Dashboard.
4. Expand the left pane and select **Profiles and Configuration** > **Credential Profile**.
   The available credential profiles are listed in the working pane.

5. Click **Create**.
6. In the **Credential Profile** dialog box, enter or select the following data:
   a. From the **Credential Profile Type** drop-down menu, select **Device Credential Profile**.
   b. Enter a name and description for the new credential profile.
7. To create a device credential profile for:
   - PowerEdge servers, chassis, and modular systems :
     a. Select HTTP as the protocol.
     b. Enter the credentials.
     c. If necessary, change the WS-Man or Rest port number.
   - Network switches:
     a. Select SNMP as the protocol.
     b. Enter the community string and SNMP port number.
8. From the **Default Profile for** drop-down menu, to sync devices discovered in SCOM, select one of the following to make it as the default profile for the credential type you have selected.

   OMIMSSC uses the default profile to discover devices discovered in the native SCOM console.

   - iDRAC—Default profile for servers.
   - CMC—Default profile for Chassis Management Controller or OpenManage Enterprise Modular (CMC/ OME-M).
   - Network switch—Default profile for network switch.
   - None—To not set this profile as a default profile.

   The default iDRAC profile is used to access the device when you discover a device or perform synchronization.
9. Click **Finish**.

Results

The device credential profile is created and listed in the **Credential Profiles** list. To refresh the list, click **Refresh**.

Modify Device Credential Profile

Steps
1. On the SCOM console, in the left pane, click **Monitoring**.
2. In the **Monitoring** pane, click **Dell EMC OpenManage Integrations Views** > **Dell EMC OpenManage Integration Dashboard**.
3. Log in to the Dell EMC OpenManage Integration Dashboard.
4. Click **Profiles and Configuration** > **Credential Profile**.
5. Select the Device Credential Profile that you want to edit, and then click **Edit**.
6. Modify the settings and click **Save**.

Delete Device Credential Profile

Steps
1. On the SCOM console, in the left pane, click **Monitoring**.
2. In the **Monitoring** pane, click **Dell EMC OpenManage Integrations Views** > **Dell EMC OpenManage Integration Dashboard**.
3. Log in to the Dell EMC OpenManage Integration Dashboard.
4. In the left pane, click **Profiles and Configuration** > **Credential Profile**.
5. Select the Device Credential Profile that you want to delete, and then click **Delete**.

Prerequisites to discover and monitor Dell EMC devices using the SCOM console

Before you begin to discover and monitor Dell EMC devices on the SCOM console, ensure that you have:

- Selected the required monitoring scope—Servers, chassis, and/or network switches and monitoring mode—Scalable or Detailed during the enrollment of SCOM Management Servers with the OMIMSSC appliance. To change either the monitoring scope or mode, edit the enrollment settings on the OMIMSSC Admin portal.
- Based on the number of Dell EMC devices you want to discover and monitor using OMIMSSC on the SCOM console, configure and onboard one or more Dell EMC Alert Relay Servers. For more information about selecting the Windows system to be used as an Alert Relay Server and to install and configure Alert Relay Server, see Setting up Dell EMC Alert Relay Servers.

(i) **NOTE:** OMIMSSC configures the appliance as the trap destination on the PowerEdge servers during every discovery cycle. Therefore, the iDRAC Administrator user role is required to discover and monitor PowerEdge servers using the OMIMSSC for SCOM appliance.

Synchronize details of Management Servers and Dell EMC Alert Relay Servers with OMIMSSC

Steps

1. In the left pane of SCOM, click **Monitoring**.
2. Click **Dell EMC** > **Dell EMC OpenManage Integrations Views** > **Dell EMC OpenManage Integration Dashboard**. The OMIMSSC login page is displayed in the working pane.
3. Enter credentials to log in to OMIMSSC. Enter the username in the format: `domain\username`.
4. On the **Overview** page, scroll down to the **Synchronized SCOM Management Servers and Dell EMC Alert Relay Servers** section and click **Sync with SCOM MS**.
5. On the **Synchronize SCOM Management Servers and Dell EMC Alert Relay Servers** dialog box, Dell EMC Alert Relay Servers which are added or removed from the SCOM Management Group are listed. Click **Synchronize**.

Results

On the **Overview** page, the count of SCOM Management Servers and Dell EMC Alert Relay Servers is updated. Click **View Alert Relay Servers** to view all the configured Dell EMC Alert Relay Servers.

Discovery and monitoring of PowerEdge servers by using the licensed monitoring features of OMIMSSC

Topics:

Introduction to the licensed monitoring features of OMIMSSC for PowerEdge servers and rack workstations

Based on your method of discovery and monitoring of the following devices, the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature provides Detailed or Scalable inventory:

- 12th Generation, 13th Generation, and iDRAC9—based PowerEdge servers
- PowerVault servers
- Dell Precision Racks
- Dell branded OEM servers
- Dell OEM Ready servers
- Dell EMC Microsoft Storage Spaces Direct Ready nodes

This is a licensed feature. You can discover and monitor these devices through iDRAC or iDRAC Service Module (iSM) installed on the managed Dell EMC Server or Rack Workstation through one of the following methods that are based on your monitoring preference:

- iDRAC WS-Man
- iDRAC access using Host operating system
- iSM-WMI

Scalable and detailed editions of licensed monitoring feature in OMIMSSC

Scalable Edition

- Generate inventory up to an individual group level only for licensed monitoring feature using iSM-WMI.
- Inventory up to the instance level is available in the Scalable Edition.
- Health monitoring at server, Rack Workstation, and component-group level.

Detailed Edition

- Inventory and health monitoring of individual components.
- View metrics about power, temperature, NICs, processor, memory, Compute Usage per Second (CUPS), PCIe SSD wear percentage, and I/O performance metrics.

Discovery and classification of PowerEdge servers and workstations by using WS-Man or iDRAC access using Host operating system

The OMIMSSC appliance enables you to discover and classify PowerEdge servers and rack workstations. The following table lists information about the hardware discovery and grouping by the Dell EMC Server and Rack Monitoring (Licensed) feature by using iDRAC–WS-Man:

Table 7. PowerEdge servers discovery and grouping

Group	Diagram View	Hardware Type
Dell EMC PowerEdge Servers	- Dell EMC Monolithic Servers - Dell EMC Modular Servers - Dell EMC Sled Group	- Dell PowerEdge systems - Dell PowerVault systems
Dell EMC Rack Workstation	Dell EMC Rack Workstation Diagram	Dell Precision Racks

Prerequisites to discover PowerEdge Servers using Dell EMC Server and Rack Monitoring (Licensed)

- Common prerequisites:
  - Before discovering a Dell EMC PowerEdge Server using Dell EMC Server and Rack Monitoring (Licensed) feature, install Microsoft SMASH Library (MPB) file. For more information about installing the Microsoft SMASH Library (MPB) file, see Install Web Services Management (WS-Man) and SMASH device template.
- For iDRAC access using Host operating system:
  - Required iSM version is installed on the managed node.
  - iDRAC access using Host operating system is enabled.

  For more information about Discovering PowerEdge servers using iDRAC access using Host operating system, see the iDRAC access via Host operating system section in the iDRAC7 or iDRAC8 User's Guide at support/home/idracmanuals.

Discover PowerEdge servers by using iDRAC WS-Man through OMIMSSC

About this task

You can discover the Dell EMC PowerEdge servers using iDRAC WS-Man through **Dell EMC OpenManage Integration Dashboard** on the SCOM console by using an IP address or an IP range.

To discover PowerEdge servers by using iDRAC WS-Man though OMIMSSC:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC OpenManage Integration Views**, and then select **Dell EMC OpenManage Integration Dashboard**.
   The OMIMSSC login page is displayed in the working pane.
3. Enter credentials for viewing the OMIMSSC dashboard, and then log in to OMIMSSC. Enter the username in the format: `domain\username`.
4. Select **Monitoring** and click the **View Servers** link to discover PowerEdge servers.

5. On the **Server View** page, click **Discover**.
6. In the **Discover** dialog box, enter the iDRAC IP address and the device type credentials of a server to discover. When you are discovering servers by using an IP range, enter an IP (IPv4) range within a subnet by including the start and end range.
   a. On the **Discovery using an IP Range or IP Address Range**:
   - To discover a server by using its IP address:
     a. In the **iDRAC IP Address** box, enter an IP address of the server to discover.
   - To discover multiple servers by using a range of IP addresses:
     a. Enter the IP address range.
     b. To exclude IP addresses from getting discovered, select the **Enable Exclude Range** check box and enter the IP address range to exclude.

     You can discover a maximum of 250 servers at a time and successive discovery jobs can be triggered in an interval of one hour.

7. From the **Apply this Credential Profile** drop-down menu, select the device credential profile that must be used for discovering the device. To create a device credential profile, click **Create New**. See Create a device credential profile in OMIMSSC.
8. To view the status of this job, select the **Go to the Job list** check box.
9. Enter a job name for this discovery task.
10. Click **Finish**.
    A discovery job is created and started, and the discovered servers are listed on the **Server View** page.

Discover PowerEdge servers by using the SCOM console

Steps

1. In the left pane of the SCOM console, select **Authoring**.
2. In the left pane, click the **Add Monitoring Wizard** link and perform the following actions:
3. In the **Add Monitoring Wizard** dialog box, under **Monitoring Type**, select **WS-Management and SMASH Device Discovery**, and then click **Next**.
4. Under **General Properties**, enter a name and description for the template.
   a. Under **Management pack**, click **New**.
   b. Enter a name for the management pack in the **Name** field and click **Next**.

      For information about creating a management pack, see the Microsoft SCOM documentation.
   c. Click **Create**.
      The management pack that you created is selected in the Management pack drop-down menu.
5. Click **Next**.
6. Under **Select Target**, from the **Specify the target** drop-down menu, select a resource pool for monitoring these devices and click **Next**.
7. Under **Credentials**, click **New** and create a simple authentication run-as account.

   (i) **NOTE:** If you are using AD domain credentials for iDRAC, then enter the credentials in the following format:
   `username@domainname.com`.

   a. Select the Run As Account you created from the **Run As Account** drop-down menu and click **Next**.
8. Under **Devices**, click **Add**.
   a. On the **Add Devices** screen, specify the iDRAC IP (if your preferred discovery method is iDRAC WS-Man) or the Host IP (if your preferred discovery method is iDRAC access using Host operating system) address of the systems you want to discover, based on your monitoring preference. You can specify the preferred IP address of the systems by:
   - Scanning the **IP Subnet** that you provided.
   - Scanning a specified **IP Range**.
   - Importing a text file containing the list of iDRAC IP/ Host IP addresses.
     For more information, see the **Configuration by using iSM PowerShell script** section in the Integrated Dell Remote Access Controller7/9 with Lifecycle Controller User's Guide at dell.com/support/home/idracmanuals.
   b. Click **Advanced Options**, select the **Skip CA Check** and **Skip CN Check** options, and then click **OK**.

c. Click **Scan for Devices** to search for Dell EMC PowerEdge Servers on your network.
   The IP addresses are listed under **Available Devices**.
d. Click **Add** to add the list of IP addresses you want to monitor and click **OK**.

9. Under **Specify the devices you want to monitor**, click **Create**.

10. Click **Close**.
    The scanned PowerEdge servers are initially listed under **Monitoring** > **WS-Management and SMASH Monitoring** > **WS-Management Device State**. After the automatically triggered SMASH discovery is completed by the Operations Manager, the PowerEdge servers are listed under **Monitoring** > **WS-Management and SMASH Monitoring** > **SMASH Device State**.

11. Enable the Dell EMC Server and Rack Monitoring (Licensed) feature through the **Dell EMC Feature Management Dashboard**.

Object discoveries using WS-Man

- Discovery Object—Dell EMC PowerEdge Server Discovery
- Description—Classifies the Dell EMC PowerEdge Servers and populates the key attributes and components.
- Discovery Object—Dell Device Helper Discovery
- Description—Discovers the Dell Device Helper as an object.
- Discovery Object—Dell Host NIC Correlation Discovery
- Description—Correlates the Host NIC interfaces with Physical interfaces.

ⓘ **NOTE:** Teamed network interfaces display only one of the NICs in the team.

Configuration of alert settings on iDRAC and SCOM console

After discovering the PowerEdge Servers, the OMIMSSC appliance automatically performs the following actions on the target iDRAC to receive alerts on the SCOM console:

- The option to send alert notifications from iDRAC is enabled under **System Settings** > **Alert Configuration** > **Alerts** or under **Alert Settings** depending on the PowerEdge Server.
- Under **SNMP Traps Configuration**, the **Destination Address** is set to the IP address of the Alert Relay Server associated with the device in an available Destination Number field.

On the SCOM console, a **DellEMC_OMIMSSC_SNMP_RunAsAccount** account of the Community String type is created on the SCOM console. A corresponding Run As Configuration profile—**SNMP Monitoring Account** is created with the SNMP v1 or v2 Community String. By default, the DellEMC_OMIMSSC_SNMP_RunAsAccount is associated with the Dell EMC Hardware class. With the SNMP Monitoring account configured in SCOM, the Dell EMC Servers and Rack Workstation (licensed) alert view displays the SNMP alerts from iDRAC. To update the SNMP v1 or v2 Community String or change the associated class, see Create Run-As-Account for SNMP monitoring and Associate multiple Run-As accounts.

Monitoring PowerEdge servers and rack workstations on the SCOM console

The OMIMSSC appliance provides the following types of views for the monitored servers and rack workstations under the **Dell EMC** folder on the SCOM console:

- Alerts view for the monitored servers and rack workstations
- Diagram views for the monitored servers and rack workstations
- View performance and power monitoring of PowerEdge servers
- View the State Views of PowerEdge servers and rack workstations

Alerts view for the monitored servers and rack workstations

The Alerts Views option is available for managing hardware and storage alerts from Dell EMC Servers and Rack Workstations. The Link-up and Link-down alerts for events received from Broadcom and Intel network interface cards for PowerEdge servers, PowerVault servers and supported Dell Precision Racks are displayed by the **Dell EMC Server and Rack Workstation Monitoring (Licensed)** feature.

View alerts of the monitored servers and rack workstations

About this task

To view the Dell EMC Server and Rack Monitoring (Licensed) feature alerts on the SCOM console:

Steps

1. In the left pane, click **Monitoring**, and then expand **Dell EMC** > **Dell EMC Alert Views**.

   The following Dell EMC Alerts Views are displayed:
   - Dell EMC Network Interface Alerts View—Link-up and Link-down alerts from the discovered NICs are displayed.
   - Dell EMC Server and Rack Workstation (Licensed) Alerts View and Dell EMC Server and Rack Workstation Alerts View—SNMP traps for 12th, 13th generation, and iDRAC9-based PowerEdge servers, PowerVault servers, and Dell Precision Racks with iDRAC7, iDRAC8, or iDRAC9 are displayed.
   - Dell EMC Rack Workstation Alert Views
     - Dell EMC Network Interface Alerts
     - Dell EMC Rack Workstation Alerts

2. Select **Dell EMC Server and Rack Workstation (Licensed) Alerts View**.
   In the working pane, alerts that meet the criteria you specify, such as alert severity, resolution state, or alerts that are assigned to you, are displayed.

3. Select the alert to view information about that alert in the **Alerts Details** section.

Diagram views for the monitored servers and rack workstations

The **Dell EMC Diagram Views** provide a hierarchical and graphical representation of PowerEdge servers and supported Precision Rack Workstations on the network.

View the Diagram Views of servers and rack workstations

Steps

1. On the SCOM console, in the left pane, click **Monitoring**, and then expand **Dell EMC** > **Dell EMC Diagram Views**.
   For more information about the available diagram views, see Diagram views displayed by different monitoring features of OMIMSSC.

2. Based on the servers or rack workstations whose status you want to view, select the respective Diagram view.

   In the right pane, the hierarchical and graphical representation of the selected Dell EMC Server or Rack Workstation is displayed.

3. To view more information about a device, select a component in the diagram.
   The component details are displayed in the **Detail View** section.

View performance and power monitoring of PowerEdge servers

Steps

1. In the left pane of SCOM, click **Monitoring**.

2. Select **Dell EMC** > **Dell EMC Performance and Power Monitoring Views**.
   (i) **NOTE:** All performance metric rules are disabled by default for Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.

For more information about the available performance and power monitoring views, see Performance and power monitoring views displayed by different monitoring features.

3. To view the **System Board Usage** metrics, select **Dell EMC Performance and Power Monitoring** > **Dell EMC System Board Usage**. See Performance and power monitoring views displayed by different monitoring features.

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

Results

A unit monitor monitors the performance counter over two successive cycles to check if it exceeds the configured critical threshold value. When the critical threshold value is exceeded, the server changes state and a critical alert is generated. This unit monitor is disabled by default. You can override (enable) the threshold values from the **Authoring** pane of the SCOM console. Unit monitors are available under the **Dell Server** objects for the Licensed monitoring feature. To enable the unit monitors and set threshold values of unit monitors, see Enable performance and power monitoring unit monitors.

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

ⓘ **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.

Enable performance and power monitoring unit monitors

Steps

1. In the left pane of the SCOM console, click **Authoring**.
2. Expand **Management Pack Objects**, and then select **Monitors**.
3. In the working pane, in the **Look for** field, search for `Performance`.
   A list of devices whose performance is monitored is listed.
4. Scroll down until you find Dell Server and expand **Performance**.
   The performance unit monitors associated with the Dell Servers are listed.
5. Right-click the unit monitor that you want to enable, and then click **Overrides** > **Override the Monitor** > **For all objects of class: Dell Server**.
6. 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.
      To create a management pack for OMIMSSC, click **New**.
7. Click **Apply**.

View the State Views of PowerEdge servers and rack workstations

Steps

1. In the left pane of SCOM, select **Monitoring**, and then expand **Dell EMC** > **Dell EMC State Views**.
   The status of Dell EMC servers and rack workstations that are managed by SCOM on the network is displayed. See State views displayed by different monitoring features of OMIMSSC.
2. To view data about a component, select a component.
   Details are displayed in the **Detail View** section.
   ⓘ **NOTE:** The group health is a rollup status of subcomponent health.

Discover and manage PowerEdge servers by using iSM-WMI

Topics:

About this task

Dell EMC Server and Rack Workstation Monitoring feature using iSM-WMI provides Detailed or Scalable inventory, based on your method of discovery and monitoring of the following devices:

* YX2X, YX3X, and iDRAC 9-based PowerEdge servers
* PowerVault servers
* Dell Precision Racks
* Dell-branded OEM servers
* Dell OEM Ready servers
* PowerEdge Storage Spaces Direct Ready nodes

Inventory and monitoring of these devices could be done through iDRAC Service Module (iSM) installed on the managed Dell EMC Server or Rack Workstation through iSM–WMI. For the list of Supported Platforms for iSM, see the *iDRAC Service Module Installation Guide* on the Dell Technologies support site.

Scalable and Detailed editions for PowerEdge servers and rack workstations using iSM-WMI

About this task

Servers and rack workstations discovered using the iSM-WMI monitoring feature are classified as Servers (iSM-WMI) in the SCOM console.

* Scalable Edition
  * Generate inventory up to an individual component level.
  * Health monitoring at server, Rack Workstation, and component-group level.
* Detailed Edition
  * Inventory and health monitoring of individual components.
  * View metrics about power, temperature, NICs, processor, memory, Compute Usage per Second (CUPS), PCIe SSD wear percentage, and IO performance metrics.

Discovery and classification of PowerEdge servers and rack workstations using iSM-WMI

About this task

The following table lists information about the hardware discovery and grouping by the Dell EMC Server and Rack Monitoring feature by using iSM-WMI:

Table 8. PowerEdge servers discovery and grouping by using iSM-WMI

Group	Diagram View	Hardware Type
Dell EMC PowerEdge Servers	● Dell EMC Monolithic Servers ● Dell EMC Modular Servers ● Dell EMC Sled Group	● Dell PowerEdge systems ● Dell PowerVault systems
Dell EMC Rack Workstation	Dell EMC Rack Workstation Diagram	Dell Precision Racks

Prerequisites for discovering PowerEdge servers by using iSM-WMI

● Required version of iSM is installed on the managed node. See Support Matrix.

> (i) **NOTE:** If you are monitoring devices by using the iSM−WMI feature on systems running Microsoft Nano server, see the I**nstalling iDRAC Service Module on Nano operating system** section in the iDRAC Service Module Installation Guide on the Dell Technologies support site.

● Windows Management Instrumentation (WMI) feature is enabled on the host. For more information, see the **Windows Management Instrumentation providers** section in the Integrated Dell Remote Access Controller7/8/9 with Lifecycle Controller User's Guide on the Dell Technologies support site.

● In **Dell EMC Feature Management Dashboard**, the **Enable Agent Proxying** task is run for the Dell EMC Server and Rack Workstation monitoring feature using iSM-WMI.

Discover PowerEdge servers by using iSM-WMI

Steps

1. In the left pane of the SCOM console, select **Administration**.
2. In the left pane, select **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.

> (i) **NOTE:** The installer automatically imports the Dell EMC Server and Rack Workstation Monitoring (Licensed) 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 **Dell EMC Feature Management Dashboard** on the SCOM console.

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

The discovered servers are displayed under **Dell EMC Servers (iSM) State View** under **Dell EMC State Views**.
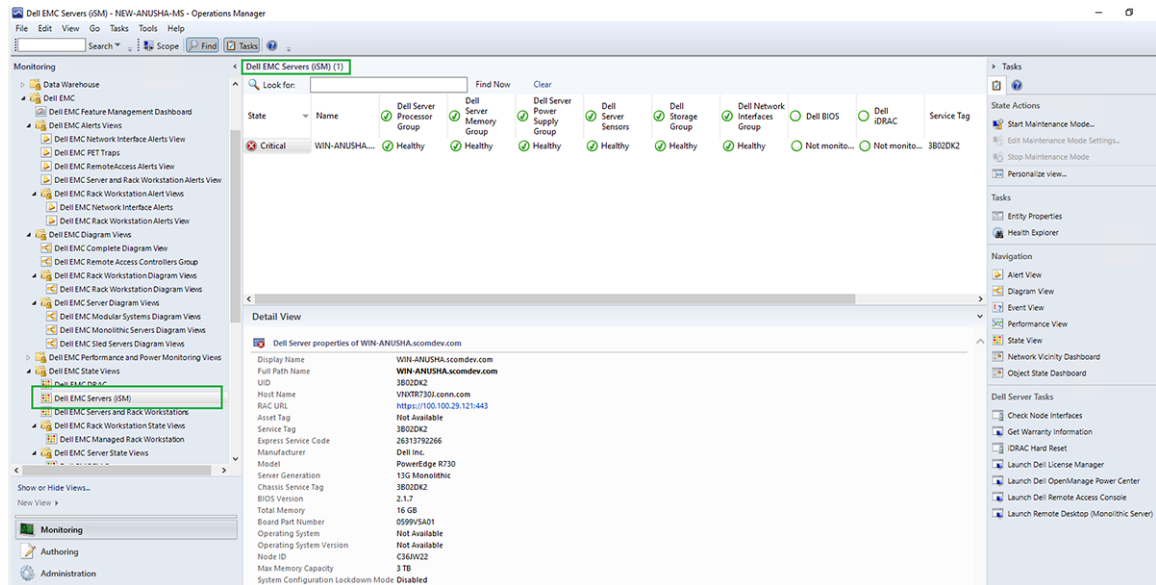
Figure 6. Discovered PowerEdge servers by using iSM-WMI

A `Dell Server (iSM) informational alert` is generated when a Dell EMC PowerEdge Server is discovered through iDRAC Service Module (iSM) for the first time. This informational alert is a one-time alert.

Object discoveries using iSM-WMI

About this task

Dell EMC PowerEdge Server Discovery—Classifies the Dell EMC PowerEdge Servers and populates the key attributes and components.

Monitoring features for PowerEdge servers and rack workstations using iSM-WMI

The **Monitoring** pane of the SCOM console is used to select views that provide health information of the discovered Dell EMC PowerEdge Servers. The Severity levels of devices that are discovered by the SCOM console enables you to indicate the health of the Dell EMC PowerEdge servers on the network.

It includes monitoring the health of Dell EMC Modular and Dell EMC Monolithic servers and Dell Precision Rack Workstations at their group level—both at regular intervals and at the occurrence of events.

View options for Dell EMC Server and Rack Workstation Monitoring feature by using iSM-WMI

The following types of views are provided for monitoring servers and rack workstations by selecting **Monitoring** > **Dell EMC** on the SCOM console:

● Alert view in the monitoring feature by using iSM-WMI
● Diagram views in the monitoring feature by using iSM-WMI
● Performance and power monitoring views in the monitoring feature by
● State views in the monitoring feature by using iSM-WMI

Alert view in the monitoring feature by using iSM-WMI

This view is available for managing hardware and storage events from the Dell EMC Server and Rack Workstation Monitoring feature using iSM-WMI. 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 DSMPS for PowerEdge servers and workstations using iSM-WMI:

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC Alerts Views**. The following alerts are displayed:
   - **Dell EMC Network Interface Alerts Views**—Link-up and Link-down alerts from the discovered NICs.
   - **Dell EMC Server and Rack Workstation Alerts Views**—SNMP traps for 12th, 13th, generation, and iDRAC9-based PowerEdge servers, PowerVault servers, and Dell Precision Racks with iDRAC7, iDRAC8, or iDRAC9 are displayed.
   - 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**
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 monitoring feature by using iSM-WMI

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 of OMIMSSC.
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 by using iSM-WMI

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:
   - **Dell Performance View (iSM)**
   - **Disk Performance - iSM (%)**

   (i) **NOTE:** All performance metric rules are disabled by default for Dell EMC Server and Rack Workstation Monitoring feature.

3. To view the System Board Usage metrics, click **Dell EMC Performance and Power Monitoring** > **Dell EMC System Board Usage** for the following views:
   - **CPU Usage - iSM (%)**
   - **IO Usage - iSM (%)**

- **Memory Usage - iSM (%)**
- **Overall System Usage - iSM (%)**

4. 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.

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.

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 by using iSM-WMI

About this task

The State View is available for viewing the health of Dell EMC devices that are monitored by different monitoring features. 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 of OMIMSSC.
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 explain the various state components with their corresponding severity levels.

Discovery and monitoring of Dell EMC chassis using OMIMSSC

The Dell EMC chassis monitoring feature supports discovery and monitoring of Dell EMC Chassis Management Controller/ OpenManage Enterprise—Modular (CMC/OME-M) on PowerEdge MX7000, PowerEdge FX2 or FX2s chassis, PowerEdge VRTX chassis, PowerEdge M1000E chassis, and Dell OEM Ready chassis using:

- SNMP and/or WS-Man protocol
- Redfish

Dell EMC Chassis monitoring feature also supports Detailed Edition monitoring of individual chassis components in the supported SCOM version.

ⓘ **NOTE:** The RACADM utility must be installed on all Dell EMC Alert Relay Servers because the health monitoring of Dell EMC chassis requires RACADM.

Topics:

Discovery and classification of chassis

The OMIMSSC appliance enables you to discover and classify Dell EMC Chassis Management Controller/ OpenManage Enterprise—Modular (CMC/OME-M) on PowerEdge MX7000, PowerEdge FX2/ FX2s, PowerEdge M1000e, and PowerEdge VRTX.

The following table lists the details of the hardware discovery and grouping by the Dell EMC Chassis monitoring feature:

Table 9. Dell EMC Chassis discovery and grouping

Group	Diagram View	Hardware type
Dell EMC CMC/ OME-M	Dell Chassis Diagram Views	CMC/OME-M instances on the network, chassis and its components, and server module slots occupied in the chassis.
Dell EMC PowerEdge M1000e	Dell EMC M1000e Chassis Diagram View	PowerEdge M1000e
Dell EMC PowerEdge VRTX	Dell EMC VRTX Chassis Diagram View	PowerEdge VRTX
Dell EMC FX2	Dell EMC FX2 Chassis Diagram View	PowerEdge FX2
Dell EMC PowerEdge MX7000	Dell EMC MX7000 Chassis Diagram View	PowerEdge MX7000

Discover Dell EMC PowerEdge Chassis by using OMIMSSC

About this task

You can discover the Dell EMC PowerEdge chassis using the **Dell EMC OpenManage Integration Dashboard** by using an IP address or an IP range. To discover a chassis, enter the chassis IP address and the device type credentials of the chassis. When you are discovering chassis by using an IP range, enter an IP (IPv4) range within a subnet by including the start and end range.

To discover Dell EMC PowerEdge chassis by using OMIMSSC:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC OpenManage Integration Views**, and then select **Dell EMC OpenManage Integration Dashboard**.
   The OMIMSSC login page is displayed in the working pane.
3. Enter credentials for viewing the OMIMSSC dashboard, and then log in to OMIMSSC. Enter the username in the format: **domain\username**.
4. Select **Monitoring** and click the **View Modular Servers** link to discover chassis.
5. On the **Modular Systems View** page, click **Discover**.
6. In the **Discover** dialog box, do the following:
   a. On the **Discovery using an IP Range or IP Address Range**:
   - To discover a chassis by using its IP address:
     a. In the **IP Address** box, enter an IP address of the chassis to discover.
   - To discover multiple chassis by using a range of IP addresses:
     a. Enter the IP address range.
     b. To exclude IP addresses from getting discovered, select the **Enable Exclude Range** check box and enter the IP address range to exclude.
7. From the **Apply this Credential Profile** drop-down menu, select the device credential profile that must be used for discovering the device. To create a device credential profile, click **Create New**. See Create a device credential profile in OMIMSSC.
8. To view the status of this job, select the **Go to the Job list** check box.
9. Enter a job name for this discovery task.
10. Click **Finish**.
    A discovery job is created and started, and the discovered chassis are listed on the **Modular Systems View** page.

Discover Dell EMC PowerEdge Chassis by using SCOM

About this task

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

Steps

1. In the left pane of the SCOM console, click **Administration**.
2. In the left pane, click **Discovery Wizard**.
3. 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.

   (i) **NOTE:** Select the Run As Account that is created for discovering the chassis devices.

4. On the **Add a Device Console** screen, enter the IP address of the chassis that you want to discover.
5. Select the necessary Run As Account from the SNMP V1 or SNMP V2 **Run As Account** drop-down menu.

6. Enable the Chassis monitoring feature by using the **Dell EMC Feature Management Dashboard**.

    Perform the Sync with Microsoft System Center from OMIMSSC console operation to complete the discovery of the chassis devices that are discovered in the SCOM console.

Configuration of SNMP RunAsAccount on the SCOM console for chassis

After discovering Dell EMC PowerEdge Chassis, to receive alerts, you must manually enable the option to send alert notifications from the Dell EMC Chassis Management Controller or OpenManage Enterprise—Modular (CMC/OME-M) to the SCOM console.

On the SCOM console, a **DellEMC_OMIMSSC_SNMP_RunAsAccount** account of the Community String type is created on the SCOM console. A corresponding Run As Configuration profile—**SNMP Monitoring Account** is created with the SNMP v1 or v2 Community String. By default, the DellEMC_OMIMSSC_SNMP_RunAsAccount is associated with the Dell EMC Hardware class. To update the SNMP v1 or v2 Community String or change the associated class, see Create Run-As-Account for SNMP monitoring and Associate multiple Run-As accounts.

Chassis monitoring feature in OMIMSSC

You can use the **Monitoring** pane of the Operations Manager to select views that provide complete health information of the discovered Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M) devices. The Dell EMC Chassis monitoring feature discovers and monitors the health of the Dell CMC/OME-M devices. The Severity levels of discovered devices indicates the health of the Dell CMC/OME-M devices on the network.

Chassis Monitoring includes monitoring the health of the Dell chassis devices, both at regular intervals and on occurrence of events.

ⓘ **NOTE:** The RACADM utility must be installed on all Dell EMC Alert Relay Servers because the health monitoring of Dell EMC chassis requires RACADM.

ⓘ **NOTE:** To perform the Dell EMC Chassis Detailed monitoring, associate the WS-Man credentials Run As account that is required for accessing the Dell CMCs with the target as Dell Modular Chassis class or respective CMC object (if you have different Run As accounts for different CMC/OME-M devices) to the profile—Dell CMC Login Account Run As Profile.

Monitored chassis views on the SCOM console

The OMIMSSC appliance provides the following types of views for monitoring Dell EMC chassis under **Monitoring** > **Dell EMC** on the SCOM console:

● View alerts of the monitored Dell EMC Chassis
● View the Diagram Views of chassis
● View performance and power monitoring of PowerEdge chassis on the.
● View the State Views of chassis

View alerts of the monitored Dell EMC Chassis

About this task

The alerts view for the monitored chassis is available for managing hardware and storage events from Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M) devices. The SNMP traps that are sent by Chassis devices are displayed by the Dell EMC Chassis monitoring feature.

To view the Chassis monitoring alerts:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC Alerts Views**.
    The following alert views are displayed:

- **Dell EMC Chassis Alerts**—SNMP traps from the discovered Chassis devices are displayed.
- **Dell EMC Chassis Alert Views**
  - **Dell EMC FX2 Chassis Alert View** —SNMP traps from the discovered PowerEdge FX2 chassis devices are displayed.
  - **Dell EMC M1000E Chassis Alert View** —SNMP traps from the discovered PowerEdge M1000E chassis devices are displayed.
  - **Dell EMC MX7000 Chassis Alert View** —SNMP traps from the discovered PowerEdge MX7000 chassis devices are displayed.
  - **Dell EMC VRTX Chassis Alert View** —SNMP traps from the discovered PowerEdge VRTX chassis devices are displayed.

3. Select the required alerts view.
   The alerts that meet the criteria you specify, such as alert severity, resolution state, or alerts that are assigned to you are displayed in the working pane.
4. Select an alert to view information about that alert in the **Alert Details** section.

View the Diagram Views of chassis

About this task

For the diagram view of the monitored chassis on the SCOM console:

Steps

1. In the left pane of the SCOM console, select **Monitoring**, and then expand **Dell EMC** > **Dell EMC Diagram Views**.
2. Select the **Dell EMC Diagram Views** folder for the following views:
   - View the Dell EMC Chassis Management Controllers Group diagram view..
   -   - Dell EMC FX2 Chassis Diagram View
       - Dell EMC M1000E Chassis Diagram View
       - Dell EMC MX7000 Chassis Diagram View
       - Dell EMC VRTX Chassis Diagram View
   See Diagram views displayed by different monitoring features of OMIMSSC.
3. Select the required diagram view.
   On the working pane, the hierarchical and graphical representations of the selected Dell EMC chassis are displayed.
4. Select a component in the diagram to view its details in the **Detail View** section.

View the Dell EMC Chassis Management Controllers Group diagram view

The **Dell EMC Chassis Management Controllers Group** diagram view offers a graphical representation of all Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M); PowerEdge MX7000, PowerEdge FX2, PowerEdge M1000E, and PowerEdge VRTX, and their inventory.
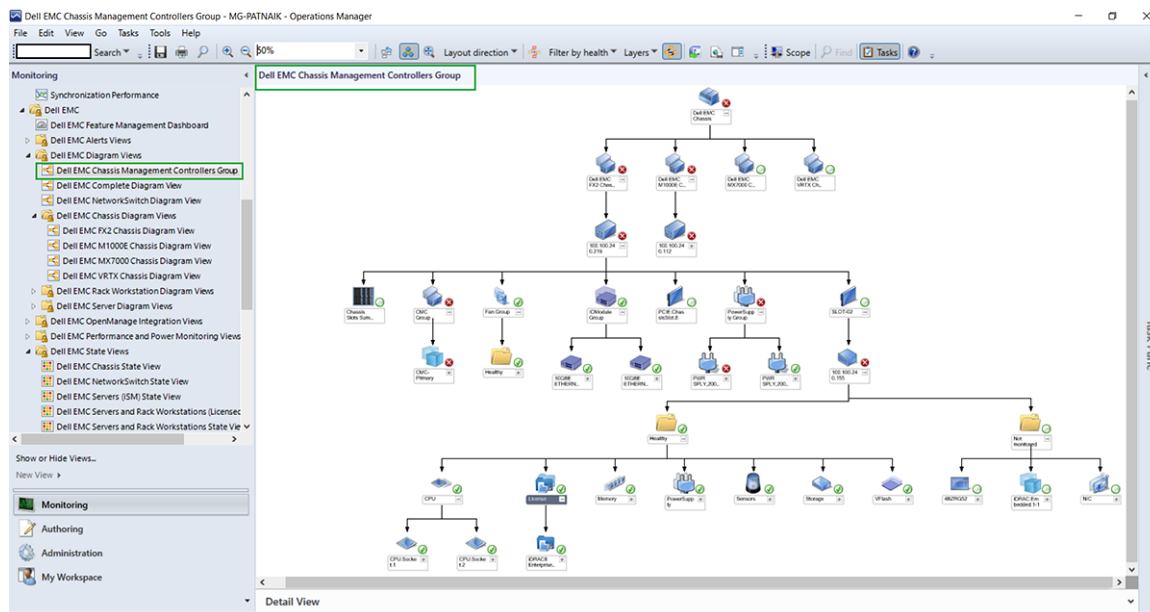
Figure 7. Dell EMC Chassis Management Controllers Group diagram view

For discovered Dell EMC CMC chassis, enable slot discovery which is disabled by default to view:

- The occupied and free slot summary in the **Chassis Slots Summary**.
- The slot-inventory details modified on CMC chassis that are reflected in the **Diagram View.**
- The correlation of discovered Dell EMC PowerEdge Servers using licensed or license-free monitoring feature with the slots of CMC chassis that are displayed in the **Dell EMC Chassis Management Controllers Group** diagram. The Dell EMC PowerEdge server is visible under the slot in the diagram.

(i) **NOTE:** Create **Run As Account** for CMC/OME-M slot discovery with simple, basic, or digest authentication only.

(i) **NOTE:** The iDRAC firmware of the modular systems should be compatible with the CMC firmware. Else, the Service Tag is displayed as **Not Available** and the Chassis Blade correlation may not be possible.

View performance and power monitoring of PowerEdge chassis on the SCOM console

About this task

The **Dell EMC Chassis Performance View** is available only when the detailed feature of the Dell EMC Chassis Monitoring feature is installed, and when you have selected Metrics Monitoring while overriding the metrics parameters. For more information about overriding the metrics parameters, see Override properties to customize the device discovery process.

To view the performance and power monitoring of the Dell EMC chassis:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC Performance and Power Monitoring Views** > **Dell EMC Chassis Performance View**.
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 graphically for each system.

View the State Views of chassis

The state views for the Dell EMC chassis are available for viewing the health of the Dell EMC Chassis Management Controller/ OpenManage Enterprise Modular (CMC/OME-M) devices.

1. In the left pane of the SCOM console, select **Monitoring**, and then expand **Dell EMC** > **Dell EMC State Views**.
2. Select the required chassis group to view the health state. You can view the status for the following:

- Dell EMC State Views
- Dell EMC Chassis State Views
- Dell EMC FX2 Chassis State View
- Dell EMC M1000E Chassis State View
- Dell EMC MX7000 Chassis State View
- Dell EMC VRTX Chassis State View

See State views displayed by different monitoring features of OMIMSSC.

The health of a component is derived by reviewing the unresolved alerts that are associated with the component. The Severity levels of discovered devices indicates the various state components that OMIMSSC uses with their corresponding severity levels.

Chassis modular server correlation feature

Chassis Modular Server Correlation feature supports:

- Correlation of discovered Modular Servers using the licensed or license-free monitoring feature with Chassis slots.
  - (i) **NOTE:** Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M) slot discovery is disabled by default. Hence, enable CMC/OME-M slot discovery for the correlation feature to work.
- Correlation of Chassis Shared Storage components with Dell EMC PowerEdge Servers.
  - (i) **NOTE:** Imports the Dell EMC Chassis Detailed monitoring edition for the correlation of chassis-shared components with Dell EMC PowerEdge Servers.

Objects discovered by using the chassis modular server correlation feature

- **Discovery Object**—Dell EMC chassis to modular server correlation discovery.
- **Description**—Discovers the correlation between the Dell EMC chassis and the Dell modular systems.
- **Discovery Object**—Dell EMC chassis storage to blade server correlation.
- **Description**—Discovers the correlation between chassis shared components with Dell EMC PowerEdge Servers that are discovered through the Dell EMC Server and Rack Workstation Monitoring.
- (i) **NOTE:** The performance graphs for the discovered correlated modular servers are displayed in both Dell EMC Server Performance View and Dell EMC Chassis Performance View.

Discovery and monitoring of Dell EMC Network Switches using OMIMSSC

The Dell EMC Network Switch Monitoring feature supports discovery and monitoring of the network switches such as M-Series, Z-Series, N-Series, and S-Series switches. In the Dell EMC Network Switch monitoring feature, the SNMP-based communication is performed.

The Dell EMC Network Switch Monitoring feature also supports detailed level of monitoring of individual switch components in the supported version of SCOM.

Topics:

- Discovery and classification of network switches
- Override properties to customize the network switch discovery process
- Discover Dell EMC Network Switches by using OMIMSSC
- Discover Dell EMC Network Switches by using SCOM
- Configuration of SNMP RunAsAccount on the SCOM console for network switches
- Network Switches monitoring feature in OMIMSSC

Discovery and classification of network switches

The details of the hardware discovery and grouping by the Network Switch Monitoring feature are as follows:

- Group—Dell EMC Network Switch
- Diagram View—Dell EMC Network Switch Diagram Views
- Hardware type—Switch instances on the network, switch, and its components.

Override properties to customize the network switch discovery process

You can customize the discovery of network switch by overriding the discovery parameters, performance, and health metrics. To override discovery parameters and health metrics of network switches, see Override properties to customize the device discovery process. On the **Override discovery, monitoring and performance intervals** page, to edit the switch parameters, select the **Network Switches** check box.

Discover Dell EMC Network Switches by using OMIMSSC

About this task

You can discover the switches by using an IP address or an IP range. To discover switches, provide the switch IP address and the device credential profile of the switch. When you are discovering switches by using an IP range, specify an IP (IPv4) range (within a subnet) by including the start and end IP address in the range.

To discover a network switch by using OMIMSSC:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.

2. Expand **Dell EMC** > **Dell EMC OpenManage Integration Views**, and then select **Dell EMC OpenManage Integration Dashboard**.
   The OMIMSSC login page is displayed in the working pane.
3. Enter credentials to log in to OMIMSSC. Enter the username in the format: `domain\username`.
4. In the left pane, select **Monitoring** > **Network Switch View**, and then click **Discover**.
5. In the **Discover** dialog box:
   - To discover multiple network switches by using a range of IP addresses, on the **Discovery using an IP Range or IP Address Range**:
     a. Enter the IP address range.
     b. To exclude IP addresses from getting discovered, select the **Enable Exclude Range** check box and enter the IP address range to exclude.
   - To discover a network switch by using its IP address:
     a. In the **Network Switch IP Address** box, enter an IP address of the network switch to discover.
6. From the **Apply this Credential Profile** drop-down menu, select the device credential profile that must be used for discovering the device. To create a device credential profile, click **Create New**. See Create a device credential profile in OMIMSSC.
7. To view the status of this job, select the **Go to the Job list** check box.
8. Enter a job name for this discovery task.
9. Click **Finish**.
   A discovery job is created and started, and the discovered network switches are listed on the **Network Switch View** page.

Discover Dell EMC Network Switches by using SCOM

Prerequisites

Prerequisites: Import the Dell EMC Network Switch Management Pack into the SCOM console from the OMIMSSC Admin Portal.

About this task

The Dell EMC Network Switches can be discovered as network devices in the SCOM console.

To discover network switches by using SCOM:

Steps

1. In the left pane of the SCOM console, click **Administration**.
2. In the left pane, click **Discovery Wizard**.
3. Select **Network devices**, and then complete the tasks that are prompted by the **Computer and Device Management Wizard**. For more information, see the Microsoft Operations Manager documentation.
4. Select the necessary Run As Account from the SNMP V1 or V2 **Run As Account** drop-down menu.
5. The Network Switch Monitoring feature is enabled when the network switch management pack is imported from the OMIMSSC Admin portal.

   (i) **NOTE:** Perform the Sync with Microsoft System Center from OMIMSSC console to complete the discovery of the network switches that are discovered in the SCOM console.

Configuration of SNMP RunAsAccount on the SCOM console for network switches

After discovering Dell EMC Network Switches, to receive alerts, you must manually enable the option to send alert notifications from the network switches to the SCOM console.

On the SCOM console, a **DellEMC_OMIMSSC_SNMP_RunAsAccount** account of the Community String type is created on the SCOM console. A corresponding Run As Configuration profile—**SNMP Monitoring Account** is created with the SNMP v1 or v2 Community String. By default, the DellEMC_OMIMSSC_SNMP_RunAsAccount is associated with the Dell EMC Hardware

class. To update the SNMP v1 or v2 Community String or change the associated class, see Create Run-As-Account for SNMP monitoring and Associate multiple Run-As accounts.

Network Switches monitoring feature in OMIMSSC

The Dell EMC Network Switch monitoring feature discovers and monitors the health of Dell EMC Network Switches. You can use the **Monitoring** pane of the SCOM console to select views that provide complete health information of the discovered Dell EMC Network switches. The Severity levels of discovered devices indicates the health of the Dell EMC Network Switches on the network.

The Dell EMC Network Switch monitoring feature includes monitoring the health of the Dell EMC Network Switches—both at regular intervals and on occurrence of health state changes.

ⓘ **NOTE:** When you are monitoring the health of network switches, associate the community string Run As Account with the SNMP Monitoring Account that is targeted at the Dell EMC Network switch class or respective switch object (if you have different Run As Accounts for different Network switch devices).

Monitored network switch views on the SCOM console

The OMIMSSC appliance provides the following types of views for monitoring Dell EMC Network Switches under **Monitoring** > **Dell EMC** on the SCOM console:
- View alerts of the monitored Dell EMC Network Switches
- View the Diagram View of network switches
- View the State view of network switches

View alerts of the monitored Dell EMC Network Switches

About this task

The alerts view is available for managing hardware from the Dell EMC Network switches. The SNMP traps that are sent through the discovered network device or switch are displayed in the Dell EMC Network Switch Alerts view.

To view the network switch monitoring alerts:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC Alerts Views**.
   Alerts that meet the predefined criteria and alerts which are assigned to the network switches are displayed.
3. Select an alert to view information about that alert in the **Alert Details** section.

View the Diagram View of network switches

About this task

The Dell EMC Diagram view provides a hierarchical and graphical representation of all discovered Dell EMC Network switches. To view the diagrams for network switch monitoring feature on the SCOM console:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Expand **Dell EMC** > **Dell EMC Diagram Views**.
3. Select the **Diagram Views** folder to view:
   - Complete Diagram View
   - Dell EMC Network Switch Diagram View
   See Diagram views displayed by different monitoring features of OMIMSSC.
4. Select the required diagram view.
5. Expand the network switches group to view the discovered supported and unsupported switches.

6. The switch component in the Diagram view can be further expanded to view the underlying components.
   Select any component to view the details in the **Detail View** section.
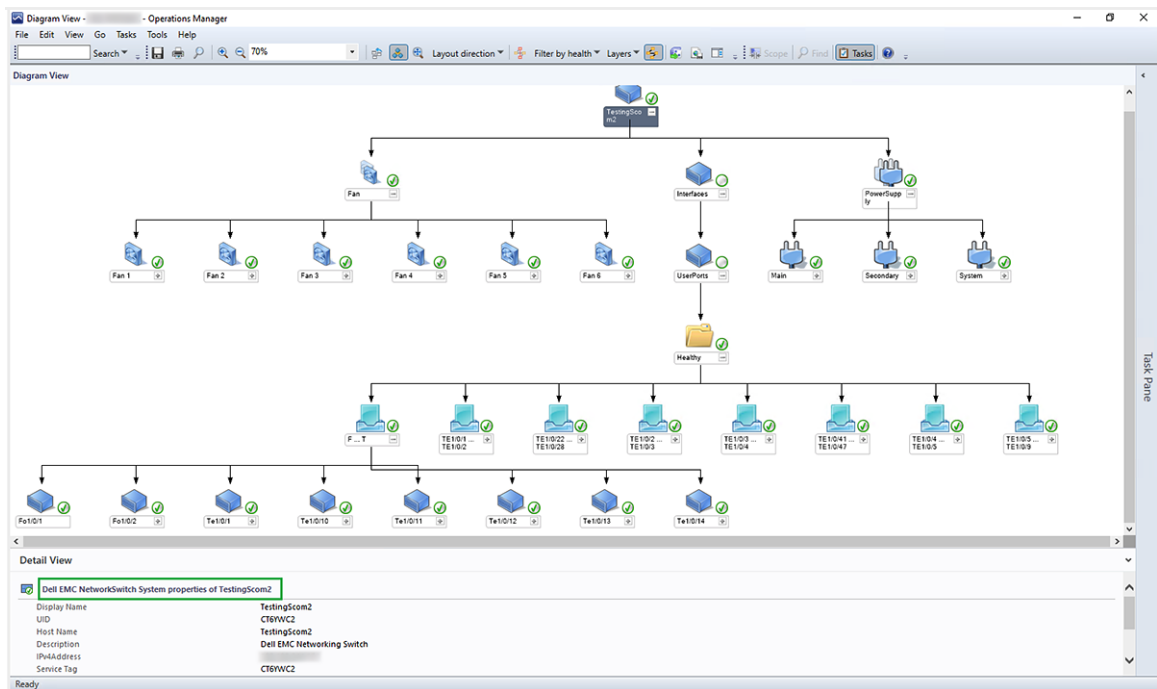
Figure 8. Dell EMC Network Switch Diagram View

View the State view of network switches

About this task

To view health states of the discovered Dell EMC network switches in the SCOM console:

Steps

1. In the left pane of the SCOM console, select **Monitoring**, and then expand **Dell EMC** > **Dell EMC State Views**.
2. Select **Dell EMC Network Switch State View**.
   The health states of all the discovered network switches are displayed. See State views displayed by different monitoring features of OMIMSSC.

   (i) **NOTE:** The group health is a rollup status health of all the subcomponents.

3. Select a component in the Dell EMC Network Switch State View to view the details in the **Detail View** section.

Manage Dell EMC devices using the OMIMSSC appliance

Topics:

- Synchronize data of the devices discovered in the enrolled SCOM with OMIMSSC
- Delete Dell EMC devices from OMIMSSC

Synchronize data of the devices discovered in the enrolled SCOM with OMIMSSC

Prerequisites

Prerequisites:

Create a credential profile before performing synchronization with the OMIMSSC.

About this task

Based on the type of device you plan to synchronize with OMIMSSC, set the default profile to iDRAC, CMC, or Network Switch from the drop-down menu. By default, the devices are synchronized after every six hours. To synchronize a device by using the OMIMSSC appliance, do the following:

Steps

1. In the left pane of SCOM, click **Monitoring**.
2. Click **Dell EMC** > **Dell EMC OpenManage Integrations Views** > **Dell EMC OpenManage Integration Dashboard**.
   The OMIMSSC login page is displayed in the working pane.
3. Enter credentials to log in to OMIMSSC. Enter the username in the format: `domain\username`.
4. Select **Monitoring** and click the link corresponding to the device type you want to synchronize:
   - To synchronize a PowerEdge server, click **View Servers**.
   - To synchronize CMC or chassis, click **View Modular Systems**.
   - To synchronize network switches, click **View Network Switches**.
5. On the **<Device type> View** page, select the device, and then click **Synchronize with MSSC**.
6. When prompted, click **Yes**.

Results

A job is created, and the data of the selected devices in the enrolled SCOM are synchronized with OMIMSSC.

Delete Dell EMC devices from OMIMSSC

Steps

1. On the SCOM console, in the left pane, click **Monitoring**.
2. Click **Dell EMC OpenManage Integration Views** > **OpenManage Integration Dashboard**.
3. Log in to OMIMSSC as an administrator.
4. Select **Monitoring** and select the device type that you want to delete. For example, to delete a server, click **View Servers**.
   A list of devices that are monitored by OMIMSSC is displayed.
5. In the **<Device type> View** page, select the device.

6. Click **Delete**.

7. When prompted, click **Yes**.

Results

A job is started to delete the device from OMIMSSC. To view the status of the job, see the **Jobs and Logs** page. The deletion process takes a few minutes.

(i) **NOTE:** If the delete operation is triggered from the SCOM console, then it takes one discovery cycle to delete the object.

Run tasks on the SCOM console for OMIMSSC monitoring features

Topics:

- Run OMIMSSC monitoring feature-based tasks on SCOM
- Tasks run on Dell EMC devices by using the OMIMSSC monitoring features

Run OMIMSSC 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 used by the device is displayed in the **Tasks** pane of the SCOM console.
5. In the **Tasks** pane, click the task 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 OMIMSSC monitoring features

When you select a device or a component, the relevant tasks are displayed in the **Tasks** pane of the SCOM console. This is a list of the tasks that you can run on Dell EMC devices by using different monitoring features of OMIMSSC.

For more information about the tasks supported by Server and Rack Workstation monitoring feature using OMSA, see the *Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for Microsoft System Center Operations Manager User's Guide* on the support site.

Table 10. Tasks run on Dell EMC devices by using the OMIMSSC Monitoring Feature

OMIMSSC tasks run on the SCOM console	OMIMSSC Monitoring Feature			
	Server and Rack Workstation (iDRAC WS-Man)	Server and Rack Workstation (iSM-WMI)	Chassis	Network Switches
Check Node Interface	Yes	Yes	Yes	No
Get Warranty Information	Yes	Yes	No	No

OMIMSSC tasks run on the SCOM console	OMIMSSC Monitoring Feature			
	Server and Rack Workstation (iDRAC WS-Man)	**Server and Rack Workstation (iSM-WMI)**	**Chassis**	**Network Switches**
Launch Dell OpenManage Server Administrator (Monolithic Server)	Yes	No	No	No
Launch Dell EMC Remote Access Console	Yes	Yes	No	No
Launch Remote Desktop (Monolithic Server)	Yes	Yes	No	No
iDRAC Hard Reset	No	Yes	No	No
Clear ESM Logs	No	No	No	No
Launch Dell EMC CMC Console	No	No	Yes	No
Power management-related tasks				
Check Power Status	No	No	No	No
Force Power Off	No	No	No	No
Power Cycle	No	No	No	No
Power off Gracefully	No	No	No	No
Power On	No	No	No	No
Power Reset	No	No	No	No
Turn LED Identification On	No	No	No	No
Turn LED Identification Off	No	No	No	No

To run the monitoring feature-based tasks on a SCOM console, see Run OMIMSSC monitoring feature-based tasks on SCOM.

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 launch the Dell OMSA application.

ⓘ **NOTE:** The Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager 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 launch 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 start Dell EMC Remote Desktop only if Windows operating system is installed, and Remote Desktop is manually enabled on the managed node.

Perform a remote iDRAC hard reset operation

You can remotely reset an iDRAC without shutting down the operating system of a server. This task is available only on PowerEdge servers that are discovered through iDRAC Service Manager (iSM) by using WMI. To reset the iDRAC remotely, you must first ensure that you have administrative privileges on the host operating system.

To remotely reset iDRAC, do the following on the SCOM console:
1. In the left pane, click **Monitoring**.
2. Click **Dell EMC** > **Dell EMC State Views** > **Dell EMC Servers (iSM) State View**.

   The state information is displayed, and the servers that are discovered though iSM by using WMI are listed in the working pane.

3. Select the server on which you want to remotely reset iDRAC.

   In the
   Tasks section of the right pane, the tasks that you can perform on the selected server are displayed.

4. Click **iDRAC Hard Reset**.

   The
   Run Task - iDRAC Hard Reset window is displayed.

5. Click **Run**.

   The
   Task Status - iDRAC Hard Reset window is displayed with the status of the reset.

6. Click **Close**. The iDRAC is successfully reset without shutting down the server operating system.

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

Supported by Server and Rack Workstation monitoring feature using OMSA.
- Check power status of Dell EMC PowerEdge servers and Rack Workstations—You can run this task only on servers that are monitored by the license-free version of Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager. 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**.

Launch the Dell CMC console

By running the Launch Dell EMC CMC Console task, you can launch the Chassis Management Controller (CMC) application that is installed on a Dell EMC chassis.

Backup and restore OMIMSSC appliance settings and data

The backup feature of OMIMSSC saves information about all the enrolled SCOM consoles, discovered devices along with license information, jobs running in OMIMSSC dashboard, credential profiles, and the configuration settings. To restore the OMIMMSC appliance data in a new VM, deploy the OMIMSSC appliance on the new VM and restore the backed-up file.

ⓘ **NOTE:** You can backup existing OMIMSSC appliance data and restore in a new OMIMSSC appliance VM of the same appliance version only. For example, you can backup OMIMSSC version 7.3 appliance data and restore in a new OMIMSSC version 7.3 appliance VM only.

Topics:

* Back up settings and data of OMIMSSC by using the OMIMSSC Admin portal
* Restore settings and data of OMIMSSC appliance

Back up settings and data of OMIMSSC by using the OMIMSSC Admin portal

Prerequisites

Ensure that you have created a Windows Network Share in the same domain as SCOM Management Server.

About this task

The backup function backs up the OMIMSSC appliance data and creates a backup file in the custom Windows Network Share.

To back up the OMIMSSC appliance data, do the following:

Steps

1. Log in to the OMIMSSC Admin portal as the default admin by entering password.
   The Admin Portal login page is displayed.
2. In the left pane, select **Settings** > **Backup Appliance**.
   The **Backup OMIMSSC Appliance Settings and Data** wizard is displayed.

Figure 9. Backup OMIMSSC Appliance Settings and Data wizard

3. In the **Windows Network Share Path for backup** box, enter the Windows Network Share path to save the backup file.

   (i) **NOTE:** Ensure that the Windows Network Share is in the same domain as the SCOM Management Server.

4. From the **Credential Profile for Windows Network Share** drop-down menu, select the Credential Profile to access the Windows Network Share.

   To create a Windows Credential profile, click **Create New**.

5. To encrypt the backup file, enter a strong password, and then reconfirm it.

6. Click **Test Connection**.

   If the connection to the Windows Network Share is successful, a message is displayed.

7. Click **Backup**.

   A message is displayed to indicate that the backup operation is completed.

   (i) **NOTE:** The Backup file is saved on the specified Windows Network Share as a ZIP file.

8. Click **Close**.

Restore settings and data of OMIMSSC appliance

About this task

Restores all the enrolled SCOM consoles, discovered devices along with license information, jobs running in OMIMSSC dashboard, credential profiles, device discovery configuration settings, and information about Dell EMC Alert Relay Servers. To restore the OMIMSSC appliance settings and data, do the following:

Steps

1. Log in to OMIMSSC Admin portal as the default admin.

2. In the left pane, select **Settings** > **Restore Appliance**.
   The **Restore OMIMSSC Appliance Settings and Data** wizard is displayed. Read through the information and alert message.

3. In the **Windows Network Share path of backup file** box, enter the Windows Network Share file location (where you have saved backup) in the following format: `\\<share name>\<folder name>\<filename>.tar.gz`

    ⓘ **NOTE:** Ensure that the Windows Network Share of the backup file is in the same domain as the SCOM Management Server.

4. From the **Credential Profile for Windows Network Share** drop-down menu, select the credential profile that OMIMSSC must use to access the Windows Network Share. To create a Windows Credential profile, click **Create New**.

Figure 10. Restore OMIMSSC Appliance Settings and Data wizard

5. In the **Password** box, enter the password of the encrypted backup file.

    ⓘ **NOTE:** The password encrypts the backed-up files. Therefore, the restoration process fails when a password is incorrect.

6. Click **Test Connection**.
    If the connection is successfully started, then a message is displayed.

7. Click **Restore**.

    A message is displayed to indicate that the restoration operation is completed:

    ```
    When you restore an OMIMSSC appliance, the current OMIMSSC admin portal session is
    closed, and the OMIMSSC appliance restarts. To view the status, log in to the OMIMSSC
    admin portal after approximately 30 minutes, and view the log files
    ```

8. To continue, click **Yes**.

The OMIMSSC appliance settings and data are restored, and the appliance is automatically restarted. To view the status of a Restore operation, see View status of restoring the OMIMSSC appliance data.

(i) **NOTE:** The previously set **Repository URL** in the Service Pack Updates section is not retained after restoring the appliance settings and data, and is restored to the default path. You must re-enter the **Repository URL** in the Service Pack Updates section for upgrading the appliance using service packs from a custom repository.

Upgrading the OMIMSSC appliance for SCOM

You can upgrade to the latest version of the OMIMSSC appliance for SCOM by using:

● The service packs available on linux.dell.com/repo/omimssc-scom—To be used when you upgrade OMIMSSC version 7.2 to version 7.3.
● The Backup and Restore feature of OMIMSSC—To be used when you upgrade OMIMSSC version 7.1 and 7.1.1 to version 7.2. You can then use the service packs to upgrade from OMIMSSC version 7.2 to version 7.3.

Additionally, you can access the **Updates and Recommendations** page on the SCOM console to check if any updates are available to the Dell EMC OpenManage Integration for Microsoft SCOM.

ⓘ **NOTE:** If a custom resource pool is created, the SCOM Management Servers present in the custom resource pool would be enrolled with OMIMSSC appliance version 7.2. Perform the following steps to de-enroll the SCOM Management Servers in the custom resource pool and to enroll the All Management Server Resource Pool (AMSRP) SCOM Management Servers with the OMIMSSC appliance:

  ● De-enroll the SCOM Management Group with OMIMSSC appliance version 7.2. See **Dell EMC OpenManage Integration Version 7.2 with Microsoft System Center for System Center Operations Manager User's Guide** on the support site.
  ● Upgrade the OMIMSSC appliance from version 7.2 to 7.3 using the service packs.
  ● After the upgrade, enroll the SCOM Management Servers with OMIMSSC appliance version 7.3 for SCOM. See Enrolling (registering) SCOM Management Group with OMIMSSC appliance for SCOM.

Topics:

Upgrade the OMIMSSC appliance version by using service packs

Prerequisites

● Ensure that no jobs are running. If running, wait until the jobs are completed.
● As per the scalability guidelines provided in the **Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) Technical White Paper (Initial release A00)**, configure Dell EMC Alert Relay Servers—previously known as Proxy Management Servers—using the OMIMSSC appliance version 7.2 and synchronize with the OMIMSSC appliance.

About this task

After deploying and setting up the OMIMSSC appliance for SCOM, if a service pack update is available with any necessary critical defect fixes or feature additions made available then you can upgrade by using the Service Pack Update feature in OMIMSSC. A few key benefits of service packs are:

● You can save the service pack files directly in any HTTP server and use the service pack files for updates.
● You can incrementally apply these service packs. However, you cannot roll back, if once updated.
● A service pack is cumulative-The latest service pack has fixes from all the previous releases.

ⓘ **NOTE:** Upgrading the OMIMSSC appliance from OMIMSSC versions 7.1 and 7.1.1 to OMIMSSC version 7.3 by using the Service Pack Update feature is not supported. To upgrade, back up the data of your OMIMSSC appliance and restore it

in the OMIMSSC version 7.2 appliance. Use the service packs to upgrade OMIMSSC version 7.2 to version 7.3. For more information about creating a backup file and restoring OMIMSSC appliance data, see the **Backup and restore OMIMSSC appliance for SCOM data** section.

Upgrade OMIMSSC by using service packs stored offline or online:

Steps

1. Log in to the OMIMSSC Admin portal, select **Settings** > **Service Pack Updates**.
2. Select either the online or offline method of service pack upgrade:
   - **Online method**
     a. Click **Reset to Default Repository** to reset the default repository path to **https://linux.dell.com/repo/ omimssc-scom/latest/**.
   - **Offline method**
     a. Download the **OMIMSSC_v7.3.0_<build>_SCOM-yumRepo_<revision>.zip** file from [linux.dell.com/repo/ omimssc-scom](linux.dell.com/repo/omimssc-scom) and save it in a repository.
     b. Extract the service pack update files from the ZIP file and host the repository over HTTP.
     c. In the **Repository URL** box, enter the URL information in the following format: **https:// <servername>:<portname>/<repository path>**. Do not enter an underscore (_) in the repository URL.

   Ensure that the files' formats in the service pack are supported by the HTTP server. If not, check with the HTTP administrator to add the support. The following file formats are supported:
   - RPM
   - XML
   - TXT
   - BZ2. To enable the BZ2 file format:
     a. Start the IIS Manager on the server where the repository files are saved.
     b. Expand the hostname. Click **Sites** > **Default Web Site**.
     c. In the **Action** pane, click **Add**.
     d. Enter the file name extension as BZ2 and MIME type as APP or BZ2.
     e. Click **Ok**.

Figure 11. Service Pack Updates wizard

3. If required, select the **Proxy Server Settings** check box, and then enter proxy server information and credentials to access the server.
4. Click **Check for Updates**.
   The current version of the OMIMSSC appliance and service pack update available in the repository is displayed.
5. Click **Apply**, and then click **OK**.

6. To view the logs, in the left pane, click **Settings** > **Logs**.

7. In the upgrade logs directory to view or download the log files for the service pack upgrade:

   a. Select the `<service pack version number>` directory.

      For example, the **7.1.1.2035 directory** to view or download the log files for the service pack upgrade.

8. The OMIMSSC appliance VM restarts to apply the service pack updates. Wait for 15 to 20 minutes and log in to the OMIMSSC Admin Portal, and then delete the browser cache history.

Next steps

After upgrading to the OMIMSSC appliance version 7.3, perform the following actions:

1. On the SCOM console, identify the Dell EMC Alert Relay Servers—previously known as Proxy Management Servers, from the DellProxyMSgroup by navigating to **Authoring** > **Groups**. Right-click **DellProxyMSgroup** and select **View group members**.

2. From the OMIMSSC Admin Portal, download **Dell EMC Alert Relay Server Installer**.

3. On the identified Dell EMC Alert Relay Servers (or Proxy Management Servers) previously configured using OMIMSSC version 7.2, install the **Dell EMC Alert Relay Server Installer** and configure as the guidelines provided in the **Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) Technical White Paper (A01 version)**.

4. Discover Alert Relay Servers as agent-managed systems.

   (i) **NOTE:** The Alert Relay Servers are listed under **Dell EMC Alert Relay Server State View**

   .

5. Clear the cache of the default web browser and log in to the Dell EMC OpenManage Integration Dashboard. Select **Sync with SCOM MS** to synchronize details related to Alert Relay Servers and Management Servers with the OMIMSSC appliance.

6. To delete the Proxy Management Server related details which are not required:

   a. Identify the Proxy Management Server overrides—Dell EMC Agent Resource <X> Override, where X is a value between 0 and 19 in a Scalable mode setup with 20 Proxy Management Servers, and then delete from the SCOM console.

   b. Remove the members from the DellProxyMSgroup, except the agents.

   c. Remove **DellProxyMSGroup**.

   d. Navigate to **Administration** > **Installed Management Packs** and then delete the Dell EMC management packs in the sequence in which they are listed. Finally, delete the Dell EMC Group Creation Library version 7.2.0.0 management pack from the SCOM console.

Upgrade the appliance by backing up and restoring OMIMSSC appliance data

The backup feature of OMIMSSC saves information about all the enrolled SCOM consoles, discovered devices along with license information, jobs running in OMIMSSC dashboard, credential profiles, and the configuration settings. To upgrade the OMIMSSC appliance from versions 7.1 and 7.1.1 to the latest version 7.3, you must:

● Restore the backed-up file in the OMIMSSC appliance for SCOM version 7.2.

● Upgrade OMIMSSC version 7.2 to 7.3 using the service packs available on the support site.

(i) **NOTE:** Upgrading the OMIMSSC appliance from versions 7.1 and 7.1.1 to the latest version 7.3 using the service packs is not supported.

Back up data of OMIMSSC 7.1 and OMIMSSC 7.1.1

About this task

If there are any jobs running on the OMIMSSC dashboard, wait until the jobs are completed, and then back up the appliance data.

To back up the OMIMSSC appliance data:

Steps

1. Start the OMIMSSC appliance VM.

The Text-based User Interface (TUI) is displayed.

2. Enter the admin password, and then press Enter.
   The appliance configuration options are displayed.

3. By using the arrow keys, go to **Backup Appliance Data**, and then press Enter.

Restore data of OMIMSSC 7.1 and 7.1.1 versions by using an IP address

Steps

1. Deploy OMIMSSC appliance version 7.2 on Hyper-V or ESXi. For more information about downloading and deploying OMIMSSC, see Deploy and configure the OMIMSSC appliance for SCOM.

2. Log in to the OMIMSSC Admin portal as the default admin by entering password.

3. In the left pane, select **Settings** > **Backup Appliance**.
   The Restore Appliance wizard is displayed. Read through the information and alert message.

4. Select the **Restore Appliance using an IP Address** option.

5. In the **Appliance Address** box, enter the IP address of the OMIMSSC 7.1 or 7.1.1 appliance where the backup data is saved.

6. In the **Enrolled SCOM MS FQDN** box, enter the FQDN of the SCOM-managed server that is enrolled to OMIMSSC. See Retrieve FQDN of the enrolled SCOM management server.

Figure 12. Restore appliance by using an IP address

(i) **NOTE:** When the Enrolled SCOM management server's FQDN parameter is not entered or incorrectly entered, there may be some discrepancies on the Dell EMC Feature Management Dashboard. After the restore operation is completed, update the available version for all the installed features on the Dell EMC Feature Management Dashboard.

7. Select **Restore**.
   The OMIMSSC 7.1 or OMIMSSC 7.1.1 data is restored and the appliance is automatically restarted. To view the status of the Restore operation, see View status of restoring the OMIMSSC appliance data.

Retrieve FQDN of the enrolled SCOM management server

Steps

1. Start the SCOM console.
2. In the left pane, select **Authoring**.
3. Click **Management Pack Objects**, and then double-click **Object discoveries**.
4. In the **Look for** box, search for `Dell EMC Feature Management Host Discovery`.
5. Right-click, and then select **Override** > **Summary** > **For all objects of class: Management Server**
   The **Overrides Summary** wizard dialog box is displayed.
6. Search for Class=`Object Discovery`, Parameter=`FMP Host FQDN`, and then corresponding Effective value for the MS FQDN name.

View status of restoring the OMIMSSC appliance data

About this task

After restoring the OMIMSSC appliance data, it is recommended that you wait for 15 minutes before you log in so that all services are initiated. To view the status of a job run on OMIMSSC to restore the appliance data, do the following:

Steps

1. Log in to the OMIMSSC Admin portal as a default administrator.
2. To view the restore logs, **Select Settings** > **Jobs and Logs Center**.
3. Click **Generic Logs** > **Appliance Logs**.

   (i) **NOTE:** When you restore from OMIMSSC appliance version 7.1 and 7.1.1, wait until all the management packs are updated to the OMIMMSC 7.2 version. Also, ensure that the Feature Management Dashboard gets updated and the appliance is automatically restarted. Wait for an hour to view the updated dashboard.

   (i) **NOTE:** After the OMIMSSC data is restored, power off the VM with the earlier version of the OMIMSSC appliance where data was backed up.

Upgrade OMIMSSC version 7.2 to 7.3

About this task

After restoring the OMIMSSC appliance version 7.1 or 7.1.1 data to OMIMSSC appliance version 7.2, you can use the service packs available on Dell Technologies support site to upgrade OMIMSSC version 7.2 to the latest version 7.3. For more information about downloading and using the service packs to upgrade, see Upgrade the OMIMSSC appliance version by using service packs.

Update OMIMSSC appliance using Updates and Recommendations page on the SCOM console

Prerequisites

Ensure that either of the prerequisites are met:

A Dell EMC PowerEdge Server is discovered and monitored on the SCOM console.

Dell EMC OpenManage Integration Dashboard View management pack is installed as part of the previous deployment of the OMIMSSC appliance.

About this task

The Updates and Recommendations page on the SCOM console lists any available updates to the OMIMSSC appliance. You can get information about the installed version, the latest version, and the release date of the latest version of the OMIMSSC appliance.

To update to the latest version of the OMIMSSC appliance for SCOM:

Steps

1. In the left pane of the SCOM console, select **Administration** > **Management Packs** > **Updates and Recommendations**.
2. In the working pane, right-click **Dell EMC OpenManage Integration for Microsoft SCOM** and select **Get MP**.
   If the OMIMSSC appliance is already installed then the status column displays **Update available**, else the status will be **Not installed**.
3. Click **Install**.
   The Dell Technologies downloads page for the latest version of the OMIMSSC appliance is displayed. To deploy the OMIMSSC appliance for SCOM, download the OVA or VHD file and following the instructions provided in the **Deploy and configure the OMIMSSC appliance for SCOM** section.

De-enroll (Deregister) SCOM Management Group enrolled with OMIMSSC

About this task

(i) **NOTE:** Before de-enrolling SCOM Management Servers in a SCOM Management Group, if opened in any of the Management Servers, close the OMIMSSC appliance share location.

Steps

1. Log in to the OMIMSSC Admin portal as an OMIMSSC ADMIN.
2. To expand the left pane, click the **>** icon, and then select **Settings** > **Console Enrollment**.
   All the enrolled SCOM Management Servers are displayed.
3. To de-enroll the SCOM Management Server, select the enrollment name and click **De-enroll**.
   If there are multiple SCOM Management Servers within the SCOM Management Group, then this operation de-enrolls all the SCOM Management Servers from the OMIMSSC appliance for SCOM. All the Dell EMC management packs and Dell EMC devices that are monitored using the appliance are removed from the SCOM console after the de-enrollment is completed.
4. To confirm, click **Yes**.
   The **Jobs and Logs** page is displayed. The de-enrollment job is listed under the **Running** tab, and the progress of the job is displayed under **Progress Status**.

   Expand the de-enrollment job to view the status of the sub tasks. During the de-enrollment, the OMIMSSC appliance performs the following activities on the SCOM console:

   ● The discovered devices and its associated jobs are deleted from the SCOM console and the OMIMSSC appliance.
   ● All the imported Dell EMC management packs are deleted.
   ● Registry entries of the OMIMSSC appliance are deleted.
   ● Prerequisites such as enabling the client for NFS and Remote PowerShell are reverted to the previous settings.

Results

The de-enrollment job takes 15 minutes to an hour or more to complete successfully depending on the selected monitoring scope, monitoring mode, and the number of devices discovered in the SCOM environment. If the de-enrollment job takes more time to complete and is unable to complete successfully, or if the SCOM Management Server is not reachable when the de-enrollment is initiated, you can use the **Force De-enroll** option under **Console Enrollment** > **More** > **Force De-enroll**. The enrolled SCOM Management Server entries are forcefully deleted from the OMIMSSC for SCOM appliance. The previous configurations on the SCOM console, before enrolling with OMIMSSC appliance, are not reverted and you must manually delete all the imported Dell EMC management packs, registry entries of OMIMSSC appliance, and Dell EMC device details. For more information, see Manually clean the SCOM console that is unreachable during the...

⚠ **CAUTION: Dell Technologies recommends that you choose the "De-enroll" option to de-enroll the SCOM Management Servers with the OMIMSSC for SCOM appliance. The Force De-enroll option is not recommended at all scenarios to avoid any loss of data. It must be used only when the SCOM console is not reachable and or when the de-enroll operation is unable to complete.**

Remove an OMIMSSC VM

About this task

Before removing the OMIMSSC appliance VM, ensure that you have performed de-enrollment of one or more enrolled management servers. To remove an OMIMSSC appliance VM:

Steps

1. In a Windows Server, in Hyper-V Manager, on a VM with OMIMSSC, right-click **Appliance VM** and click **Turn Off**.
2. Right-click **Appliance VM**, and then click **Delete**.

Troubleshooting

Topics:

- Deployment of OMIMSSC appliance and OMIMSSC Admin Portal-related issues
- Enrollment of SCOM Management Group with OMIMSSC appliance-related issues
- De-enrollment of SCOM Management Group with OMIMSSC appliance-related issues
- Discovery and monitoring Dell EMC devices-related issues
- Other issues

Deployment of OMIMSSC appliance and OMIMSSC Admin Portal-related issues

After deploying the OMIMSSC appliance, an IP address is not assigned to the OMIMSSC appliance

After creating and starting the appliance, the IP address is not assigned or displayed on the Command Line Interface (CLI).

Workaround—Check if the virtual switch, which is mapped to a physical switch, is configured correctly, and then connect to the OMIMSSC appliance.

Unable to start the OpenManage Integration Dashboard in the SCOM console

About this task

After enrollment, the OpenManage Integration Dashboard is not loading in the SCOM console, or if there is any change in the OMIMSSC Appliance IP.

Workaround—Update the OMIMSSC appliance IP under Unit Monitors:

Steps

1. In the left pane of the SCOM console, select **Authoring**.
2. Select **Authoring** > **Management Pack Objects** > **Monitors**.
3. In the **Look for** field, under Management Server, search for `Dell EMC SDK Override Appliance IP`.
4. Right-click **Dell EMC SDK Override Appliance IP**, and then click **Override** > **Override the Monitor** > **For all objects of class**.
   The **Override properties** wizard is displayed.
5. Select **Dell EMC Appliance IP** under parameter name.
6. Update the Override value and click **OK**.
   (i) **NOTE:** Ensure that you do not select any other override parameters.

Unable to log in to the OMIMSSC Admin portal by using the Mozilla Firefox browser

When accessing the OMIMSSC admin portal by using the Mozilla Firefox browser, the following warning message is displayed:

```
Secure Connection Failed
```

Workaround——Delete the certificate created from a previous entry of the Admin portal in the browser.

Unable to connect to the OMIMSSC appliance

After deploying the OMIMSSC appliance, and double-clicking the OMIMSSC appliance icon, the following message is displayed:

```
Connection to server failed.
```

Workaround:

● Add the OMIMSSC appliance IP and FQDN as a trusted site.
● In the DNS, add the Appliance IP and FQDN in the forward and reverse lookup zones.
● Check if there are any error messages in the `C:\ProgramData\VMMLogs\AdminConsole` file.

Connection is unavailable between OMIMSSC and the SCOM console

About this task

When you restart the server in which OMIMSSC is deployed, connectivity is lost between the OMIMSSC appliance and SCOM console. This is because the execution policy of the SCOM console for the user is not active. Log in to the SCOM console server using the SCOM console user account to make the execution policy active. However, after logging in, the connection is not restored until the following tasks are completed.

Steps

1. Set PowerShell execution policy for:
   ● Local system=RemoteSigned
   ● The SCOM console Account=Unrestricted.

   For information about policy settings, see the following Microsoft documents:
   ● PowerShell Execution policy— microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_execution_policies?view=powershell-7.4&viewFallbackFrom=powershell-7.
   ● PowerShell Group Policy— microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_group_policy_settings?view=powershell-7.4&viewFallbackFrom=powershell-7.

2. After the execution policy is set, restart the SCOM console server.

Enrollment of SCOM Management Group with OMIMSSC appliance-related issues

After deploying the OMIMSSC appliance, enrollment of Management Servers with OMIMSSC is unsuccessful or Dell EMC management packs are not successfully installed.

Workaround:

● While deploying the OMIMSSC appliance, ensure that Synchronize guest time with host option on the VM is enabled.
● While configuring OMIMSSC VM network settings, under IPv4 CONFIGURATION, if you are assigning a Static IP address, enter the IP address and save the changes. Re-open the **Configure Network** option on the CLI and change the hostname. See Configure OMIMSSC VM network settings.

Issues observed when usernames of local account and domain account match but the passwords differ

The following issues are observed if the usernames are same and passwords are different for the domain user account and the local user on the Management Server and/or on the Alert Relay Server:

- Unable to successfully test connection between the OMIMSSC appliance and the SCOM console.
- After a discovery job is completed successfully in the Dell EMC OpenManage Integration Dashboard, SCOM objects are not discovered in the respective Dell EMC device state views and diagram views.
- Devices discovered in the SCOM console remain in the unmonitored state in the Dell EMC device state views and diagram views.

For example,

- Domain user account: domain\user1, pwd1
- Local user account: user1, Pwd2

When the user tries to enroll with the above domain user account, the test-connection operation will not be successful.

Workaround—Use different usernames for the domain user and local user accounts or use a single user account as local user when enrolling a SCOM console to the OMIMSSC appliance.

Ensure to configure the modified domain user account on the Management Server and/or on the Alert Relay Server before discovering Dell EMC devices.

Importing of Dell EMC OpenManage Integration Dashboard View Management pack fails in Microsoft System Center-Operations Manager 2012 R2

About this task

To import the Dell EMC OpenManage Integration Dashboard View Management pack:

Steps

1. Install Update Rollup 14 for Microsoft System Center-Operations Manager 2012 R2. For more information about the latest Update Rollup information and installation procedure, see the respective Microsoft documentation.
2. After the latest Update Rollup is installed, the following management packs will be available on the Management Server under: `C:\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server\Management Packs for Update Rollups`. Import these management packs into the SCOM console.
   - Microsoft.SystemCenter.Visualization.ServiceLevelComponents
   - Microsoft.SystemCenter.Visualization.Library
   - Microsoft.SystemCenter.Visualization.Component.Library
3. Import the Dell EMC OMIMSSC Configuration Management Pack and enroll the SCOM Management Server from the OMIMSSC Admin portal. For more information about enrollment, see the *Dell EMC OpenManage Integration with Microsoft System Center for System Center Operations Manager User's Guide* on the support site.

De-enrollment of SCOM Management Group with OMIMSSC appliance-related issues

Manually clean the SCOM console that is unreachable during the de-enrollment

About this task

During de-enrollment, if the SCOM console is unreachable, and you forcefully de-enroll then the installed management packs are not cleaned up from the unreachable console. To delete the installed management packs on the SCOM console, do the following:

Steps

1. In the left pane of the SCOM console, select **Authoring**.
2. To view a list of groups, select **Groups**.
3. From the list of groups, select **DellProxyMSGroup**.
4. Check for any explicit members added in the group and delete.
5. Right click on the group and click **Delete**.
   The DellProxyMSGroup is deleted.
6. In the left pane, select **Administration**.
7. To view the list of the installed management packs, in SCOM 2016 and later, select **Administration** > **Management Packs** > **Installed Management Packs**.
8. To delete the management pack from the console, right-click the management packs in the following order, and then click **Delete**:
   - Dell EMC Chassis Modular Server Correlation Utility
   - Dell EMC Managed Server iSM Management Pack
   - Dell EMC Server OpenManage Integration Dashboard View
   - Dell EMC Windows Server (Scalable Edition)
   - Dell EMC Feature Management Task Refresher
   - Dell EMC Feature Management Override
   - Dell EMC Managed Server Model Library
   - Dell EMC Group Creation
   - Dell EMC Server Operations Library
   - Dell EMC Feature Management
   - Dell EMC Chassis CMC View
   - Dell EMC Chassis CMC Model
   - Dell EMC CMC Operations Library
   - Dell EMC Server View
   - Dell EMC SDK ApplianceIP Override
   - Dell EMC Server Model
   - Dell EMC Server View Library
   - Dell EMC Server Model Library
   - Dell EMC CMC Model
   - Dell EMC AgentResource 0 Override
   - Dell EMC NetworkSwitch View
   - Dell EMC NetworkSwitch
   - Dell EMC PerformanceThreshold Monitor Override
   - Dell EMC Base Hardware Library
   - Dell EMC Operations Library Common
   - Dell EMC Appliance Information Management Pack
   - Dell EMC Configuration Management Pack

   All the Management packs and overrides are deleted.

9. Delete the Dell Management pack folder that is present in local drive by following the path: `%PROGRAMFILES%\Dell Management Packs\Server Mgmt Suite\<version>\`

10. Delete the Dell Server Management Pack Suites Registry entry from the Registry Editor by doing the following:

   a. Select **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Dell**.
   b. Right-click **Dell Server Management Pack Suites** and delete the registry entry.

After the de-enrollment job completes, manually revert the prerequisites configured by the OMIMSSC appliance version 7.2

After the de-enrollment job completes in the OMIMSSC appliance version 7.3, prerequisites that are configured on the SCOM Management Servers by the OMIMSSC appliance version 7.2 are not reverted.

Workaround: Manually revert the following configurations on the SCOM Management Servers:

- SSL listener
- Basic Auth Support
- Firewall rule to allow WinRM HTTPS
- PS Remoting
- WinRM Client Authentication
- WinRM Service Authentication
- WinRM AllowUnencrypted service

Discovery and monitoring Dell EMC devices-related issues

Unable to discover and monitor devices after restarting OMIMSSC

About this task

When OMIMSSC restarts, the connectivity between the SCOM console and the OMIMSSC appliance is lost. After the appliance is started, all the discovery and monitoring features of the Dell EMC devices is restored during the next discovery and monitoring cycle respectively.

(i) **NOTE:** The default discovery and the monitoring cycle is 24 hours.

If you want to start the discovery and monitoring of the Dell EMC device before the 24 hours cycle, you can change the override values.

To change the override values, do the following:

Steps

1. Log in to OMIMSSC.
2. Select **Profiles and Configuration** > **Configuration**.
3. Click the **Edit** tab, and then select the device to edit the override value.
4. In the discovery interval column, edit the override value, and then click **Apply**.
   The discovery is triggered again immediately after changing the override values.

   (Optional) You can view the applied changes by selecting **Jobs and Logs Center** > **Scheduled** jobs.

A job run on OMIMSSC to discover a device stays in the Progress state for more than five hours

The device discovery job that is run from OMIMSSC gets stuck in the running task list for more than five hours.

Workaround—Create and run a new job for the device discovery with same set of IP addresses.

Unable to set the SNMP trap destination on the target device(s)

About this task

Causes:

- The user does not have administrative privileges.
- Slots are not available on the target device(s) to configure trap destination IP address.
- The System Lockdown Mode is enabled on the target iDRAC.

Workaround

- Ensure that the user has administrative privileges on the target device(s).
- Ensure slots are available on the target iDRAC to configure trap destination IP address.
- Disable System Lockdown Mode on target iDRAC.

Unable to receive alerts from the discovered chassis or network switches

About this task

After you discover chassis or network switches, manually configure the following to receive alerts on the SCOM console.

- A valid SNMP community string account is configured for chassis or network switch objects on the SCOM console under **Administration** > **Run As Configuration** > **Profiles** > **SNMP Monitoring Account**.
- Enable the event alerts option on the chassis or network switches.
- In the alert destination field on the chassis or network switches, enter the IP address of the associated Dell EMC Alert Relay Server.
  > (i) **NOTE:** After the discovery of the chassis or network switch, the **Alert Relay Server** column on the **Modular Systems View** or **Network Switch View** page lists the associated Dell EMC Alert Relay Server.

Resolve issues in synchronizing data of Dell EMC devices with OMIMSSC

About this task

Sometimes, devices that are discovered in SCOM may not be synchronized with OMIMSSC because of invalid credentials, HTTPS port number, SNMP port number, or community string. Because of such errors, OMIMSSC cannot discover devices and these devices are listed with their IP addresses. To resolve the synchronization errors, ensure that you provide relevant credentials.

To resolve synchronization errors, do the following:

Steps

1. In the left pane of the SCOM console, select **Monitoring**.
2. Select **Dell EMC OpenManage Integrations Views** > **OpenManage Integration Dashboard**.
3. Log in to the OMIMSSC as an administrator.
4. Select **Monitoring** > **Resolve Sync Errors**.
   A list of IP addresses of the devices for which synchronization has failed is displayed.
5. Select the device, and then select the device credential profile.

   To create a device credential profile, click **Create New**. See Create a device credential profile in OMIMSSC.
6. Enter a job name, and if necessary, select the **Go to the Job List** check box to view the job status automatically after the job is submitted.
7. Click **Finish**.

Other issues

Resolve issues in the Dell EMC Feature Management Dashboard

When using the Restore feature in OMIMSSC, some of the following issues are observed on the Dell EMC Feature Management Dashboard:

The OMIMSSC version is indicated as 7.1 because of an invalid FQDN or when FQDN information is not provided

When you provide wrong management server FQDN or do not provide the management server FQDN during restore operation in the OMIMSSC Admin portal, the available version of appliance for the monitoring features is indicated as 7.1 on Dell EMC Feature Management Dashboard.

1. After the Restore operation is complete, in the SCOM console, select **Authoring**.
2. Expand **Management Pack Objects**.
3. Double-click **Object Discoveries**.
4. In the **Look for** field, search for `Dell Feature Management Host Discovery`.
5. Right-click **Dell Feature Management Host Discovery**, and then click **Overrides** > **Override the Object Discovery** > **For all objects of class: Management Server**.
6. Select **FMP host FQDN**, and then set the override value to FQDN of the management server used during the restore operation. To retrieve FQDN name of the FMP host:
   a. Log in to OMIMSSC Admin portal.
   b. Select **Jobs and Logs Center** > **Generic Logs** > **Appliance logs**.
   c. In Activity Logs, view the following message:

   ```
   Information: The Dell registry entry on the MS with FQDN <name> has been updated.
   ```
7. Click **OK**.

The Feature Management Dashboard shows blank about the remaining management servers

When the management server used for enrollment in the OMIMSSC Admin Portal is removed from the SCOM management group, the Dell EMC Feature Management Dashboard displays blank about the remaining management servers. To recover the Feature Management dashboard feature:

1. Update the service pack.
2. Start the management server that had been removed from the management group.
3. At the **Command Prompt** window, run the following command:**Run reg export HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Server Management Pack Suites c:\Export.txt**
4. Start any of the management servers in the management group.
5. Copy the exported `C:\Export.txt` file to the management server.
6. At the **Common Prompt** window, run `reg import c:\Export.txt`.
7. Complete steps 1–6 in the **The OMIMSSC version is indicated as 7.1 because of an invalid FQDN or when FQDN information is not provided** section.
8. Click **OK**.

The Feature Management Dashboard indicates different OMIMSSC versions for Server and Rack Workstation and Chassis monitoring features

The Feature Management Dashboard displays two entries of OMIMSSC versions as available—One each for Dell EMC Server and Rack workstation Monitoring Feature and Dell EMC Chassis Monitoring Feature. For example, server monitoring indicates version 7.1, but chassis indicates version 7.2. To remove the monitoring features which have the available version as 7.1 from Feature Management Dashboard, do the following:

1. At the **Command Prompt** window, run the following command:

```
Run reg export HKEY_LOCAL_MACHINE\SOFTWARE\Dell\Dell Server Management Pack Suites C:
\Export.txt
```

2. After exporting, run the following commands:
   - **reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Dell**

     (i) **NOTE:** Prompts if you want to permanently delete the registry entries.
   - **reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Dell (Yes/No)?**

     (i) **NOTE:** Type **Y** to confirm, else type **N**

     .

     (i) **NOTE:** To get the enrolled management server FQDN, see the **Restore OMIMSSC appliance** section in this guide.

After deleting the registry entry, it takes 10–15 minutes to reflect the Feature Management Dashboard with updated available version of the OMIMSC.

(i) **NOTE:** To view the registry entry for the 7.1 version, ensure that you start the Registry Editor on the management server that had been enrolled previously.

(i) **NOTE:** Two different version numbers of OMIMSSC are displayed even when:
- You have not imported the Dell EMC Network Switch Monitoring Feature and DRAC Monitoring Feature during version upgrade.
- You have imported after performing restore.

Event ID 33333: Data Access Layer rejected retry on SqlError

About this task

Warning event with the event id 33333 is generated on management server when iSM management pack tries to discover Proxy Agents. To suppress this event, you must disable the iSM discovery that is targeted on proxy agents.

To disable the iSM discovery that is run on proxy agent and to suppress the event ID 33333 from getting regenerated, do the following:

Steps

1. Log in to the SCOM console.
2. In the left pane, select **Authoring** > **Management Pack Objects**, and then double-click **Object Discoveries**.
3. In the **Look for** field, search for **iSM**.
4. Select **Discovered type**: **Dell Server** > **Dell Server Discovery**.
5. Right-click **Dell Server Discovery**, and then click **Overrides** > **Override the Object Discovery** > **For a Group**.
   The **Select Object** wizard is displayed.
6. Select the **DellProxyMSGroup** group, and then click **OK**.

Unable to download Certificate Signing Request using Internet Explorer

Workaround: In Internet Explorer, select **Internet Options** > **Security**. For the Internet zone, click **Custom level**. In the Security Settings window, under **Downloads**, enable **File download**.

OMIMSSC Admin Portal displays exceptions after upgrading the appliance

Workaround: After upgrading the OMIMSSC appliance for SCOM, delete the browser cache and log in to the OMIMSSC Admin Portal.

Associated devices with the Dell EMC Alert Relay Server are not deleted from the Dell EMC OpenManage Integration Dashboard if there is a network issue

About this task

After you uninstall the Dell EMC Alert Relay Server Installer, the associated devices with the Alert Relay Server are automatically removed from the SCOM console. Selecting **Sync with SCOM MS** on the Dell EMC OpenManage Integration Dashboard home page to synchronize Alert Relay Server details, you might see network issue failure message and the associated devices will continue to be visible on the Dell EMC OpenManage Integration Dashboard.

Workaround

Manually delete the devices from the Dell EMC OpenManage Integration Dashboard.

Reference topics

Topics:

Monitoring features supported by OMIMSSC

The topics in this section describe the monitoring features that are supported by the OMIMSSC appliance for SCOM.

Dell EMC Server and Rack Workstation Monitoring (Licensed) Feature

Dell EMC Server and Rack Workstation Monitoring (Licensed) feature provides detailed or scalable inventory, based on your discovery method, and monitoring of the following devices:

*   12th, 13th generation, and iDRAC 9-based PowerEdge servers
*   PowerVault servers
*   Hardware monitoring of Dell EMC-branded or Dell EMC OEM Ready servers and Dell EMC Microsoft Storage Spaces Direct Ready nodes.
*   Dell Precision Racks

Inventory and monitoring of these devices could be done through iDRAC or iDRAC Service Module (iSM) installed on the managed Dell EMC Server or Rack Workstation through one of the following methods based on your monitoring preference:

*   iDRAC using WS-Man
*   iDRAC access via Host OS
*   iSM using WMI

This is a licensed feature. For the list of supported platforms for iSM, see the **iDRAC Service Module Installation Guide** on the support site.

Management Packs

Table 11. Management Packs required for the Dell EMC Server and Rack Workstations Monitoring (Licensed) feature

Feature	Default location of Management Packs	Management Packs
Dell EMC Server and Rack Workstation Monitoring (Licensed)	**Library** `C:\Program Files\Dell Management Packs\Server Mgmt`	**Library** • Dell.Connections.HardwareLibrary.mp • Dell.OperationsLibrary.Server.mp

Table 11. Management Packs required for the Dell EMC Server and Rack Workstations Monitoring (Licensed) feature

Feature	Default location of Management Packs	Management Packs

	`Suite\<OMIMSSC_SCOM_Version>\Library`
	
	Scalable and detailed Management Packs
	
	`C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\Server Monitoring`
	`<OMIMSSC_SCOM_Version>` is the version of the OMIMSSC for SCOM appliance. For example, 7.2 or 7.3.
		Monitored Management Packs
		
		● For Dell EMC Servers or Rack Workstations that are discovered through iSM–WMI:
		  ○ Dell.ManagedServer.iSM.mp
		  ○ Dell.ManagedServer.Model.mp
		  ○ Dell.View.Server.mp
		● For Dell EMC Servers or Rack Workstations that are discovered through iDRAC–WS-Man:
		  ○ Dell.Model.Server.mp
		  ○ Dell.OperationsLibrary.Server.mp
		  ○ Dell.View.Server.mp
		● Dell.Model.Server.mp
		● Dell.Server.SDK.mp
		● Dell.View.Server.mp

Configuration prerequisites

● Ensure that iSM is installed.
  ○ WMI feature is enabled for discovering devices through iSM–WMI.
  ○ iDRAC access via Host OS in enabled for discovering devices through iDRAC access via Host OS.
● Ensure that there is WS-MAN (WS-Management) connectivity to iDRAC.
● Ensure that the SNMP ports on the firewall are enabled.
● To receive alerts in SCOM, enable the OS-to-iDRAC Passthrough setting in iDRAC.
● Ensure that the Dell Device Helper is installed.
● Ensure that `MaxEnvelopeSizekb` value in WinRM setting is higher (for Windows Server 2008 R2 only).

Management Server (MS) requirements

● Microsoft System Center—Operations Manager 2012 and later: Dell EMC Server and Rack Workstation Monitoring (Licensed) feature is available only on management servers running Operations Manager 2012 and later.
● SMASH Library MPB from Microsoft: Dell EMC Server and Rack Workstation Monitoring (Licensed) feature requires SMASH library MPB from Microsoft to discover Dell EMC PowerEdge Servers. See Install Web Services Management (WS-Man) and SMASH device template.

Managed System requirements

● Required iSM version is installed on the Dell EMC device. Based on your monitoring requirements, the following features must be enabled through the iDRAC console:
  ○ Windows Management Instrumentation (WMI) feature to monitor through iSM–WMI.
  ○ iDRAC access via Host OS (Experimental feature) to monitor through iDRAC using host IP.
● iDRAC7 or later.
  ⓘ **NOTE:** If you are using iDRAC firmware version 2.40.40.40 or later, Transport Layer Security (TLS) versions 1.1 or later are enabled by default. Before installing Dell EMC Server Management Pack Suite version 7.2 for Microsoft System Center Configuration Manager, see support.microsoft.com/en-us/topic/update-to-enable-tls for more information about TLS updates. Based on your web browser, you may have to enable support for TLS 1.1 or later.

Feature management tasks

The following table lists the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature tasks available on the **Dell EMC Feature Management Dashboard**. Some tasks that are listed in the Feature Management tasks table appear only after you have imported the Dell EMC Server and Rack Workstation Monitoring (Licensed) 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.

Table 12. Feature management tasks

Tasks	Description
Enable Agent Proxying	Enables agent proxying for the Dell EMC PowerEdge Servers running the supported iSM version and also triggers discovery of these servers.
Set to Scalable Feature (Licensed)	If the detailed feature is running on the system, the **Dell EMC Feature Management Dashboard** switches from the detailed feature to the scalable feature for this monitoring method. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set to Detailed Feature (Licensed)	If the scalable feature is running on the system, the **Dell EMC Feature Management Dashboard** switches from the scalable feature to the detailed feature for this monitoring method. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set as Preferred Monitoring Method (Licensed)	Enables the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature as the preferred monitoring method for your Dell EMC Servers and Rack Workstations, when these devices are monitored through both the Dell EMC Server and Rack Workstation Monitoring feature and Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.
Enable Event Auto-Resolution	Enables the Event Auto-Resolution feature.
Disable Event Auto-Resolution	Disables the Event Auto-Resolution feature.
Associate Run-As Account	This task associates the Run As Account that is used for the SMASH discovery with all Dell Server objects, which are required for health monitoring. For more information, see Associate Run-As Account task-Dell EMC Server and Rack Workstation Monitoring feature.
Remove Monitoring Feature (Licensed)	Removes the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.
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.

Dell EMC Chassis Monitoring feature

The Dell EMC chassis monitoring feature supports discovery and monitoring of Dell EMC Chassis Management Controller/ OpenManage Enterprise Modular (CMC/OME-M) on PowerEdge MX7000, PowerEdge FX2/ FX2s chassis, PowerEdge VRTX chassis, PowerEdge M1000E chassis, and Dell OEM Ready chassis using:

- SNMP and/or WS-Man protocol
- Redfish

Dell EMC Chassis monitoring feature also supports Detailed monitoring of individual chassis components in the supported Microsoft System Center—Operations Manager.

Management Packs

Table 13. Management Packs required for the Dell EMC chassis monitoring feature

Feature	Default location of Management Packs	Management Packs
Dell EMC Chassis Monitoring	**Library** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\Library` **Monitored Management Packs** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\Chassis Monitoring` `<OMIMSSC_SCOM_Version>` is the version of the OMIMSSC for SCOM appliance. For example, 7.2 or 7.3.	**Library** - Dell.Connections.HardwareLibrary.mp - Dell.OperationsLibrary.Common.mp **Monitored Management Packs** - Dell.CMC.SDK.mp - Dell.Model.CMC.mp - Dell.View.SDKCMC.mp

Configuration prerequisites

- Ensure that SNMP ports on firewall are enabled.
- Ensure that Dell Device Helper is installed.
- Ensure that there is WS-Man connectivity between the Management Server and the Managed Node.

Dell EMC Chassis Monitoring requirements

- For slot discovery and correlation to work, ensure that you have Dell Device Helper utility installed.
- To monitor Chassis controller, IO Module, IO Module Group, Power Supply, and Power Supply Group components.
- To monitor the health of Chassis devices, associate the community string Run As account with the SNMP Monitoring Account with the target as Dell Modular Chassis class or respective Chassis object (if you have different Run As accounts for different Chassis devices).
- To discover Chassis Slots and Chassis Slot Summary for Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M), create Run As Accounts and associate it to the profiles — Dell CMC Login Account Run As Profiles. Also, enable the CMC Slot Discovery from the SCOM console.
- To perform Chassis Detailed monitoring, create Run As Accounts with WS-Man credentials that are required for accessing the Dell EMC CMC/OME-Ms, and associate it to the profiles — Dell CMC Login Account Run As Profiles.
- (i) **NOTE:** If you are using AD domain credentials for Dell EMC CMC/OME-M, then, enter the credentials in the following format: **username@domainname.com**

Configuring Dell EMC Chassis Management Controller/ OpenManage Enterprise Modular (CMC/ OME-M) feature for correlating Server Modules with the Chassis Slot summary

To configure Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M) feature for correlating server modules, create Run As Accounts and associate it to Run As Profiles to populate chassis slot summary.

1. Create a Run As Account of type Simple Authentication that has privileges to connect to the CMC/OME-M on the chassis. Also, use the Basic or Digest Run As Account types for configuring the user credentials.
2. Select the More Secure or Less Secure option in the Run As Account configuration, so that you can selectively distribute the configuration to specific management servers.
3. Associate the created Run As Accounts with the Dell CMC Login Account profile and select the appropriate class, group, or object on which you can configure the profile. `To enable slot summary discovery for CMC/OME-M, override the enable property to True in Dell CMC Slot Discovery. It is disabled by default.`

   (i) **NOTE:** Add the Server Management Action account to the SCOM administrator group.

   (i) **NOTE:** After the slot discovery, if you remove the link between Run As Account with Run As Profile, or disable the slot-discovery workflow, the discovered slots remain with old data.

Feature management tasks

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

(i) **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.

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

Table 14. Feature management tasks

Tasks	Description
Set to Scalable Monitoring	If the Detailed feature is running on the system, the **Dell EMC Feature Management Dashboard** switches from the detailed feature to the scalable feature. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set to Detailed Monitoring	If the scalable feature is running on the system, the **Dell EMC Feature Management Dashboard** switches from the scalable feature to the detailed feature.
Refresh Node Count	Updates the node count.
Refresh Dashboard	Updates the **Dell EMC Feature Management Dashboard**. (i) **NOTE:** The **Refresh dashboard** task may not update the dashboard immediately. It might take a few minutes to update the dashboard contents.

Dell EMC Chassis Modular Server Correlation Feature

Chassis Modular Server Correlation feature supports:

- Correlation of discovered Modular Servers using the licensed or license-free monitoring feature with Chassis slots.
  (i) **NOTE:** Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME-M) slot discovery is disabled by default. Hence, enable CMC/OME-M slot discovery for the correlation feature to work.

● Correlation of Chassis Shared Storage components with Dell EMC PowerEdge Servers.

    ⓘ **NOTE:** Imports Dell EMC Chassis detailed monitoring for the correlation of chassis shared components with Dell EMC PowerEdge Servers.

Management Packs

Table 15. Management Packs required for the Dell EMC Chassis Modular Server Correlation monitoring feature

Feature	Default location of Management Packs	Management Packs
Dell EMC Chassis Modular Server Correlation	**Library** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\Library` **Monitored Management Packs** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\ChassisModular ServerCorrelation` `<OMIMSSC_SCOM_Version>` is the version of the OMIMSSC for SCOM appliance. For example, 7.2 or 7.3.	**Library** ● Dell.Connections.HardwareLibrary.mp ● Dell.OperationsLibrary.Common.mp **Monitored Management Packs** ● Dell.ChassisModularServer.Correlation.mp

Management Server (MS) requirements

Chassis Blade correlation in distributed SCOM environment

To enable the proxy agent:

1. In the SCOM console, click **Administration**.
2. In the **Administration** pane, expand **Administration** > **Device Management** > **Management Servers**.
3. Select the management server where you have discovered the chassis devices.
4. Right-click and select **Properties**.
5. In **Management Server Properties**, click **Security**.
6. Select **Allow this server to act as a proxy and discover managed objects on other computers**.
7. Click **OK**.

Feature management tasks

The following table lists the Dell EMC Chassis Modular Server Correlation feature tasks available on the **Dell EMC Feature Management Dashboard**. Some tasks that are listed in the Feature Management tasks table appear only after you have imported the Dell EMC Chassis Modular Server Correlation 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 running another task using the Dell EMC Feature Management Dashboard.

Table 16. Feature management tasks

Tasks	Description
Refresh Node Count	Updates the node count.
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.
Upgrade Chassis Modular Server Correlation Feature	Upgrades to the latest version of the Dell EMC Chassis modular server correlation feature.
Remove Chassis Modular Server Correlation Feature	Removes the Dell EMC Chassis modular server correlation feature

Dell EMC Network Switch monitoring feature

The Dell EMC Network Switch monitoring feature supports discovery and monitoring of the network switches including M-Series, Z-Series, N-Series, and S-Series switches. In the network switch monitoring feature, SNMP-based communication is performed.

The Dell EMC Network Switch monitoring feature also supports detailed level of monitoring of individual switch components in the supported Microsoft System Center—Operations Manager.

Management Packs

Table 17. Management Packs required for the Dell EMC Network Switch monitoring feature

Feature	Default location of Management Packs	Management Packs
Dell EMC Network Switch Monitoring	**Library** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\Library` **Monitored Management Packs** `C:\Program Files\Dell Management Packs\Server Mgmt Suite\<OMIMSSC_SCOM_Version>\NetworkSwitch Monitoring` `<OMIMSSC_SCOM_Version>` is the version of the OMIMSSC for SCOM appliance. For example, 7.2 or 7.3.	**Library** ● Dell.Connections.HardwareLibrary.mp ● Dell.OperationsLibrary.Common.mp **Monitored Management Packs** ● Dell.NetworkSwitch.mp ● Dell.View.NetworkSwitch.mp

Feature management tasks

The following table lists the Dell EMC Network Switch monitoring tasks available on the **Dell EMC Feature Management Dashboard**. Some tasks that are listed in the Feature Management tasks table appear only after you have imported the network switch 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 running another task using the Dell EMC Feature Management Dashboard.

Table 18. Feature management tasks

Tasks	Description
Refresh Node Count	Updates the node count.
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.
Set to Scalable Monitoring	If the Detailed Edition is running on the system, the Dell EMC Feature Management Dashboard switches to the Scalable Edition. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.
Set to Detailed Monitoring	If the Scalable Edition is running on the system, the Dell EMC Feature Management Dashboard switches to the Detailed Edition. On upgrading from the previous version, run this task to use the latest version for this monitoring feature.

Configuring the monitoring features of OMIMSSC by using the Feature Management Dashboard

The **Dell EMC Feature Management Dashboard** provide options to configure monitoring features using the OMIMSSC appliance to monitor the various Dell EMC devices—PowerEdge Servers, PowerEdge Storage Spaces Direct Ready nodes, Dell EMC Precision Racks, Dell Remote Access Controllers (DRAC), Dell EMC Network Switches, Dell EMC OEM servers and Dell EMC Chassis including PowerEdge FX2, PowerEdge VRTX, PowerEdge M1000E, PowerEdge MX7000. 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 OMIMSSC monitoring features and then configure them automatically for importing, upgrading, and removing the management packs required by a feature.

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 13. 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**.
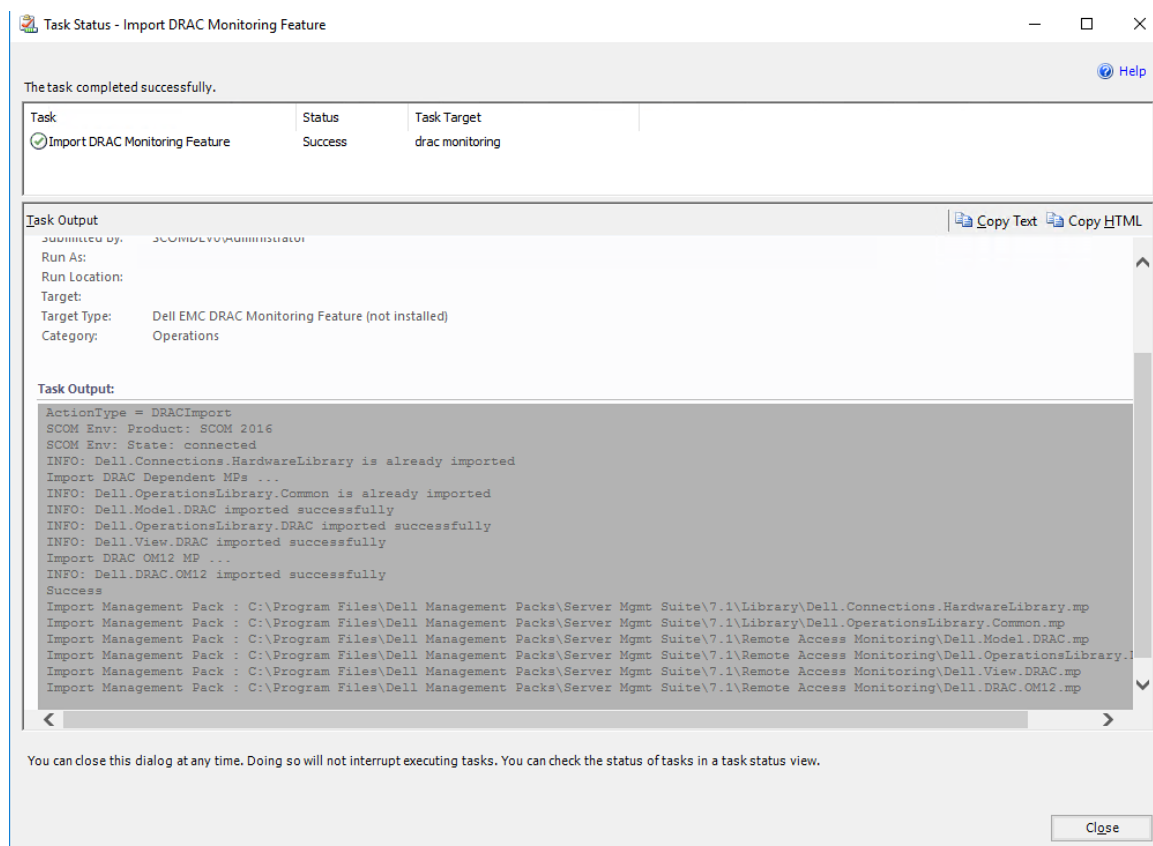
Figure 14. Task status of Import Monitoring Feature

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 the OMIMSSC appliance, 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**.

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

Table 19. Customizing OMIMSSC 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.
Dell EMC Server and Rack Workstation Monitoring (Licensed)	● Inventory up to individual components. ● Health monitoring at server, rack workstation, and component group level.	● Inventory and health monitoring of individual components. ● View metrics for power, temperature, network interface cards processor, memory, Computer Usage per Second (CUPS), the PCIeSSD wear level, and IO performance metrics.
Dell EMC Chassis Monitoring	● Chassis inventory ● Chassis slots summary ● Health monitoring of chassis	Inventory and health monitoring of individual chassis components.
DRAC Monitoring	● iDRAC inventory ● iDRAC health monitoring	Not Applicable.
Dell EMC Chassis Modular Server Correlation	Correlate Modular servers with Chassis—view inventory and health from chassis up to components inside the Modular server.	Not Applicable.
Dell EMC Network Switch Monitoring	● Network switch inventory ● Health monitoring of network switches	Inventory and health monitoring of individual network switch components.

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.

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.

Run tasks on the SCOM console

Steps

1. In the left pane of SCOM, 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.

Override properties to customize the device discovery process

About this task

You can customize the discovery of Dell EMC devices by overriding their discovery parameters, performance, and health metrics. To override discovery parameters, performance, and health metrics, do the following on the OpenManage Integration Dashboard:

Steps

1. In the left pane of SCOM, click **Monitoring**.
2. Click **Dell EMC** > **Dell EMC OpenManage Integration Views** > **Dell EMC OpenManage Integration Dashboard**.
3. Enter the credentials to log in to OpenManage Integration Dashboard. Enter the username in the format: `domain\username`.
4. In the left pane, click **Profiles and Configuration**.
5. Select **Profiles and Configuration**.
   The **Discovery, Monitoring and Performance Overrides** page is displayed. The discovery type and monitoring intervals set on the available device types is displayed in the table.
6. Click **Edit**.
   The **Override discovery, monitoring and performance intervals** dialog box is displayed.
7. Customize the monitoring settings by selecting or entering data in the fields:
   a. Select the check box corresponding to the device type whose monitoring properties must be overridden.
   b. Enter the time frequency for automatically running the device discovery and health status jobs.
   c. To enable collection of metrics, select **Yes** from the drop-down menu, and then enter the interval after which metrics must be collected.
   d. Click **Apply**.

Next steps

The recommended default intervals set by the OMIMSSC appliance for the different operations are:

● Discovery Interval—86400 seconds (24 hours)
● Health Interval—21600 seconds (6 hours)
● Metrics Interval—21600 seconds (6 hours)

It is recommended that these intervals are not changed to avoid any possible performance issues. However, if you want to change these intervals, ensure that sufficient resources are reserved, and correct SQL Server design and sizing considerations are followed. For more information, see the respective Microsoft documentation.

Key features of licensed monitoring of PowerEdge servers in OMIMSSC

System configuration lockdown mode in iDRAC9 PowerEdge servers

The System Configuration Lockdown mode feature is available for iDRAC9—based PowerEdge servers that lock the system's configuration, including firmware updates. After the System Configuration Lockdown Mode is enabled:

● You cannot change the system's configuration. This feature is intended to protect the system from unintentional changes. Using the iDRAC console, you can enable or disable the System Configuration Lockdown mode.
● You cannot configure the trap destination information in the servers. Therefore, alerts are not generated for monitoring. In such a case, you are notified with a critical alert indicating that System Configuration Lockdown mode is enabled, and trap destination information for alerts is not configured.

> (i) **NOTE:** Dell Technologies recommends you to update the "Dell OM : System configuration lockdown alert rule interval" immediately after the server discovery interval is updated or modified. This ensures that the System Lockdown mode alert is generated after the completion of server discovery with a certain interval.

You can view information about the System Configuration Lockdown mode in the Detail View pane of the Dell EMC Diagram View. For more information about this feature, see the **iDRAC9 Version 3.00.00.00 User's Guide** available on the support site. This feature is available for servers that are discovered by using iDRAC and iSM methods of Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.

iDRAC Group Manager in iDRAC9 PowerEdge servers

The iDRAC Group Manager feature is available for iDRAC9—based PowerEdge servers to offer simplified basic management of iDRAC, and associated servers on the same local network. Group Manager feature enables one-to-many console experience without requiring a separate application. Using the iDRAC Group Manager, you can view information about a set of servers by permitting more powerful management than by inspecting servers visually for faults and other manual methods.

You can view information about the iDRAC Group Manager, iDRAC Group Manager Status, and iDRAC Group Name under the iDRAC object in the Detail View pane of the Diagram View. For more information about this feature, see the **iDRAC9 Version 3.00.00.00 User's Guide** available on the support site. This feature is available for servers that are discovered by using the iDRAC and iSM methods of Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.

Event auto resolution

This section describes the automatic resolution or acknowledgment of the Dell device events using the Event Auto Resolution feature.

Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for Microsoft System Center Operations Manager receives and processes the events from the Dell devices. These events can be broadly classified as issue, information, and resolution events. All these events remain on the console until they are manually closed. Even after the issue gets resolved at the node, the issue event, and the corresponding resolution event remains in the console until they are manually acknowledged. Event Auto Resolution feature automatically resolves or acknowledges such Dell device events.

The auto resolution of events can be classified as:

● Problem to problem—One problem event resolves another problem event. For example, a temperature sensor sends a warning event when it crosses the warning threshold. If there is no action, after certain time, the same sensor sends critical event when it crosses the critical event. In this case, there is no importance of the warning event, because it does not exist. The warning event is acknowledged, and only critical event is displayed on the console.

● Problem to resolution—One resolution or a normal event resolves a problem event. For example, a temperature sensor sends a warning event when it crosses the warning threshold. When the administrator takes appropriate action, the same sensor sends the resolution event or normal event after certain time. In this case, there is no importance of the warning event, because it does not exist. The warning event is acknowledged, and only normal event is displayed on the console.

This feature is available only for servers that are discovered through iDRAC WS-Man. By default, the Event Auto Resolution disabled. Enable this feature by using the Enable Event Auto Resolution task. The tasks such as Enable Event Auto Resolution and Disable Event Resolution, are available under **Dell EMC** > **Dell EMC Feature Management Dashboard** > **Dell EMC Server and Rack Workstation Monitoring (Licensed)** > **Dell EMC Monitoring Feature Tasks**.

Capacity planning of PowerEdge servers discovered through iDRAC and iSM

You can monitor if the server's utilization has exceeded the configured capacity threshold value using the Dell Server Capacity Check unit monitor. The unit monitor—Dell Server Capacity Check monitors the average system or CUPS usage for the last one day of each server against the configured capacity threshold value. By default, this unit monitor is disabled. To enable the Dell Server Capacity Check unit monitor, see Enable performance and power monitoring unit monitors.

The minimum threshold value is 1, and the maximum threshold value is 99. The default threshold value is 60. You can configure the threshold values within the specified range. That is, 1–99. In case, you provide a threshold value other than the specified ranges, that threshold is reset to its default value.

A warning event per server is generated when the average system or CUPS usage for the last one day exceeds the configured threshold value. The warning event is auto resolved when the average system or CUPS usage for the last one day returns within the configured threshold value.

You can view the details of the warning alert in the Alert Details pane under Monitoring.

Detect and restore the status of a failed CMC or OpenManage Enterprise-Modular

Using the "iDRAC detection of a failed Dell EMC Chassis Management Controller/OpenManage Enterprise Modular (CMC/OME- M)" feature, iDRAC of a Rack Style Management (RSM) enabled modular server detects a failed or an unavailable CMC. By using this feature, you can take immediate remedial action to bring the failed Dell EMC CMC/OME-M to a normal state.

The Dell Chassis Controller Sensor indicates the presence or failure of a Dell EMC CMC/OME-M. You can view the health state that is obtained from the unit monitor by clicking **Dell EMC Diagram Views** > **Dell Chassis Controller Sensor** under Sensors.

> (i) **NOTE:**
> ● The Dell Chassis Controller Sensor is available in both the Scalable and Detailed Management Pack editions.
> ● iDRAC detection of failed Dell EMC CMC/OME-M is supported for YX3X and iDRAC9-based PowerEdge FX2 Chassis.

Port connection information of PowerEdge servers discovered through iDRAC and iSM

> (i) **NOTE:** This feature is supported for iDRAC9-based PowerEdge servers only.

Server port connection information feature provides information about the physical mapping of switch ports to server ports, and iDRAC dedicated port connections. This feature enables you to reduce cabling error debugging by identifying switch ports that are connected to a server's network ports, and iDRAC dedicated port. You can view the information about the Server port connection under iDRAC NIC and NIC objects in the Detail View pane of the Dell EMC Diagram View. Along with the inventory information of each NIC, chassis ID information of the switch and the port ID information is populated. This feature is available for Dell EMC PowerEdge servers that are discovered through both the iDRAC and iSM methods of Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.

Hardware components of servers and rack workstations monitored by OMIMSSC

The following table provides information about the monitored hardware components that are supported in Scalable and Detailed feature for Dell EMC devices that are discovered through iDRAC–WS-Man or iSM-WMI in OMIMSSC.

Table 20. Monitored hardware components of servers and rack workstations—Scalable and Detailed feature

Hardware components	Server and Rack Workstation monitoring feature using iDRAC WS-Man		Server and Rack Workstation monitoring feature using iSM-WMI	
	Scalable	Detailed	Scalable	Detailed
BIOS	No	No	No	No
Battery Sensor Group	No	Yes	Yes	Yes
Battery Sensor	No	Yes	No	Yes
Current Sensor Group	No	Yes	No	No
Current Sensor	No	Yes	No	No
Fan Sensor Group	No	Yes	Yes	Yes
Fan Sensor	No	Yes	No	Yes
Host NIC Group	No	Yes	Yes	Yes
Host NIC	No	Yes	No	Yes

Table 20. Monitored hardware components of servers and rack workstations—Scalable and Detailed feature (continued)

Hardware components	Server and Rack Workstation monitoring feature using iDRAC WS-Man		Server and Rack Workstation monitoring feature using iSM-WMI	
	Scalable	**Detailed**	**Scalable**	**Detailed**
iDRAC Network Interface	Yes	Yes	Yes	Yes
iDRAC	No	No	No	No
iDRAC License	No	No	No	Yes
iDRAC License Group	No	No	Yes	Yes
Intrusion Sensor Group	No	Yes	Yes	Yes
Intrusion Sensor	No	Yes	No	Yes
License Group	Yes	No	-	-
License	No	Yes	-	-
Memory	Yes	No	No	Yes
Memory Instance	Yes	Yes	-	-
Physical Network Interface	No	Yes	No	Yes
Physical Network Interface Group	Yes	Yes	Yes	Yes
Processors Group	Yes	No	Yes	Yes
Processor	Yes	No	No	Yes
Power Supply Group	Yes	Yes	Yes	Yes
Power Supply	No	Yes	No	Yes
PCIeSSD Extender	No	Yes	No	Yes
PCIeSSD backplane	No	Yes	No	Yes
PCIeSSD Physical Disk	No	Yes	No	Yes
Server Sensors	No	Yes	-	-
Server Storage	Yes	Yes	-	-
Storage Controller Connector	No	Yes	-	-
Storage Controller	No	Yes	No	Yes
Storage Controller Sensor	No	Yes	No	Yes
Storage Controller Battery Group	No	Yes	No	Yes
Storage Controller Battery	No	Yes	No	Yes
Storage Virtual Disk Group	No	Yes	No	Yes
Storage Virtual Disk	No	Yes	No	Yes
Storage Controller Physical Disk Group	No	Yes	-	-

Hardware components	Server and Rack Workstation monitoring feature using iDRAC WS-Man		Server and Rack Workstation monitoring feature using iSM-WMI	
	Scalable	Detailed	Scalable	Detailed
Storage Controller Physical Disk	No	Yes	-	-
Storage Controller Enclosure	No	Yes	No	Yes
Storage Controller Enclosure EMM	No	Yes	No	Yes
Storage Controller Enclosure Fan Sensor Group	No	Yes	No	Yes
Storage Controller Enclosure Fan Sensor	No	Yes	No	Yes
Storage Controller Enclosure Power Supply Group	No	Yes	No	Yes
Storage Controller Enclosure Power Supply	No	Yes	No	Yes
Storage Controller Enclosure Temperature Sensor Group	No	Yes	No	Yes
Storage Controller Enclosure Temperature Sensor	No	Yes	No	Yes
Storage Controller Enclosure Sensor	No	Yes	No	Yes
Storage Connector Internal/external/direct attached physical disk group	-	-	No	Yes
Storage Connector Internal/external/direct attached physical disk instance	-	-	No	Yes
SD Card Group	No	Yes	Yes	Yes
SD Card	No	Yes	No	Yes
Temperature Sensor Group	No	Yes	Yes	Yes
Temperature Sensor	No	Yes	No	Yes
Voltage Sensor Group	No	Yes	Yes	Yes
Voltage Sensor	No	Yes	No	Yes

Hardware components of chassis monitored by OMIMSSC

The following table provides information about the monitored hardware components supported in Scalable and Detailed feature.

Table 21. Monitored chassis hardware components—Support for Scalable and Detailed features.

Hardware Components	PowerEdge MX7000		PowerEdge M1000e		PowerEdge FX2		PowerEdge VRTX	
	Scalable	Detailed	Scalable	Detailed	Scalable	Detailed	Scalable	Detailed
CMC/OME-M Slot Information	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CMC/OME-M Slot	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fan Group	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IO Module Group	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Power Supply Group	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fan	No	Yes	No	Yes	No	Yes	No	Yes
IO Module	No	Yes	No	Yes	No	Yes	No	Yes
Power Supply	No	Yes	No	Yes	No	Yes	No	Yes
PCIe Device Group	No	No	Yes	Yes	Yes	Yes	Yes	Yes
PCIe Device	No	No	No	No	No	Yes	No	No
Storage	No	No	No	No	No	No	Yes	Yes
Storage Controller	No	No	No	No	No	No	No	Yes
Storage Controller Virtual Disk Group	No	No	No	No	No	No	No	Yes
Storage Controller Virtual Disk	No	No	No	No	No	No	No	Yes
Storage Controller Physical Disk Group	No	No	No	No	No	No	No	Yes
Storage Controller Physical Disk	No	No	No	No	No	No	No	Yes
Storage Enclosure	No	No	No	No	No	No	No	Yes

Hardware components of network switches monitored by OMIMSSC

The following table provides information about the monitored network switches hardware components that are supported in Scalable and Detailed feature:

Table 22. Monitored network switches hardware components—Scalable and Detailed feature

Hardware Components	Discovery mode	
	Scalable	Detailed
Switch	Yes	Yes
Fan Group	Yes	Yes
Fan unit	No	Yes
Power supply Group	Yes	Yes
Power supply Unit	No	Yes

Hardware Components	Discovery mode	
	Scalable	Detailed
Interfaces	Yes	No
User Port Group	Yes	No
User Port instances	No	Yes

View options provided by the OMIMSSC monitoring features

Table 23. View options provided by the OMIMSSC monitoring features

View types	OMIMSSC monitoring features			
	Server and Rack Workstation (Licensed) using iDRAC WS-Man	Server and Rack Workstation (Licensed) using iSM-WMI	Chassis	Network Switches
Alert View	Yes	Yes	Yes	Yes
Diagram View	Yes	Yes	Yes	Yes
Performance and Power Monitoring View	Yes	Yes	Yes	Yes
State View	Yes	Yes	Yes	Yes

For more information about the views supported by Server and Rack Workstation monitoring feature using OMSA (agent-based), see the *Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for Microsoft System Center Operations Manager User's Guide* on the support site.

Diagram views displayed by different monitoring features of OMIMSSC

Table 24. Diagram views displayed by different monitoring features of OMIMSSC

Diagram View Type displayed on the SCOM console	OMIMSSC monitoring features			
	Server and Rack Workstation (Licensed)	Server and Rack Workstation (Licensed) using iSM-WMI	Chassis	Network Switches
Complete Diagram View	Yes	Yes	No	Yes
Rack Workstation Diagram View	Yes	Yes	No	No
Modular Server Diagram View	Yes	Yes	No	No
Monolithic Server Diagram View	Yes	Yes	No	No
Sled Server Diagram View	Yes	Yes	No	No
Unit Diagram View	Yes	Yes	No	No

Table 24. Diagram views displayed by different monitoring features of OMIMSSC (continued)

Diagram View Type displayed on the SCOM console	OMIMSSC monitoring features			
	Server and Rack Workstation (Licensed)	Server and Rack Workstation (Licensed) using iSM–WMI	Chassis	Network Switches
Remote Access Controller Group Diagram View	No	No	No	No
CMC Group Diagram View	No	No	Yes	No
Chassis Diagram View	No	No	Yes	No
Network Switch Diagram View	No	No	No	Yes

Complete Diagram View supported by OMIMSSC

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.
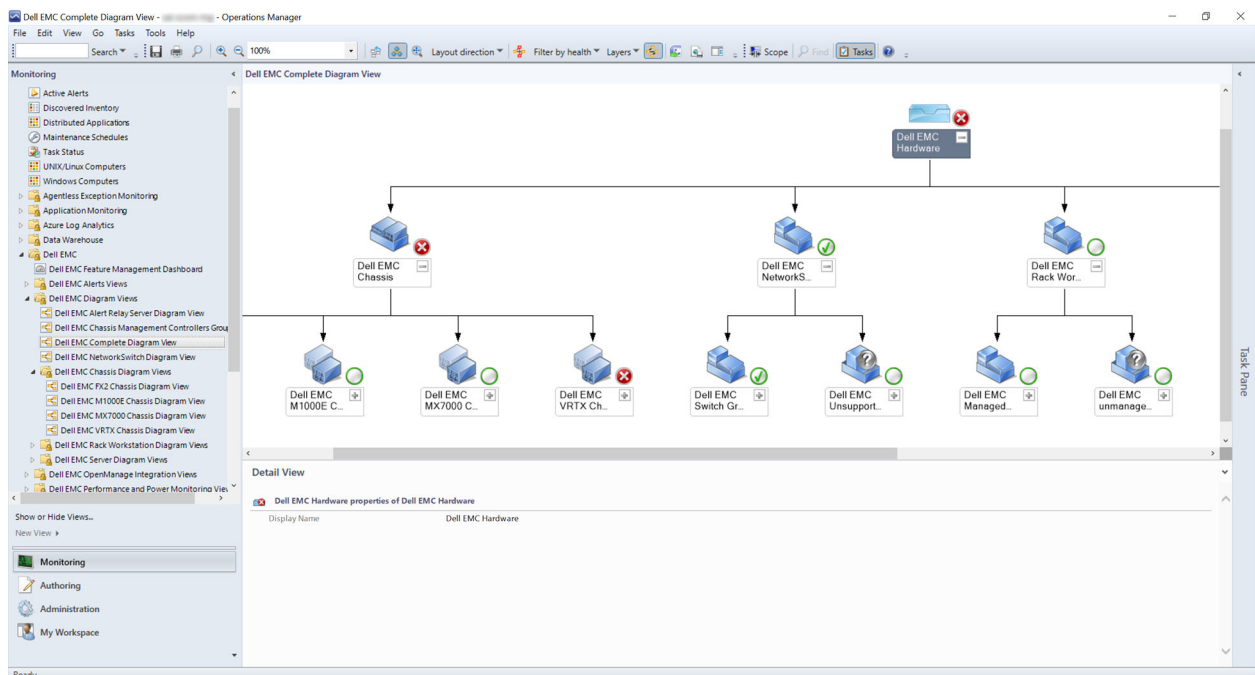
A Complete Diagram view displayed by the monitoring features has information about the following:

● Dell EMC Modular and Monolithic servers
● Dell EMC Sled Group
● Dell EMC Rack Workstations Group
● Dell EMC Rack Workstations
● Chassis Management Controllers
● Remote Access Controllers
● Dell EMC unmanaged systems

Rack Workstation Diagram View

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

Component data displayed by the Modular and Monolithic Diagram Views	OMIMSSC monitoring feature	
	Server and Rack Workstation (Licensed)	Server and Rack Workstation (Licensed) using iSM-WMI
Physical network interfaces	Yes	Yes
Memory	Yes	Yes
PSU	Yes	Yes
Sensors	Yes	Yes
Processors	Yes	Yes
Storage Components	Yes	Yes
BIOS (Inventory only)	Yes	Yes
BIOS	No	No
iDRAC NIC	Yes	Yes
Host NIC	Yes	Yes
SD Card	Yes	Yes
Network Interfaces Group	No	No
License	Yes	Yes
Memory Group	No	No
PSU Group	No	No
Sensor Group	No	No
Processor Group	No	No
Storage Component Group	No	No
Host NIC Group	No	No
iDRAC	No	No
iDRAC License Group	No	No
PCIe/SSD Group	No	No
SD Card Group	No	No

Modular Systems Diagram View supported by OMIMSSC

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.

Monolithic Servers Diagram View supported by OMIMSSC

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.

Sled Servers Diagram View supported by OMIMSSC

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.

PowerEdge server Unit Diagram View supported by OMIMSSC

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 OMIMSSC monitoring feature.

Remote Access Controllers Group Diagram view supported by OMIMSSC

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.

State views displayed by different monitoring features of OMIMSSC

Table 26. State views displayed by different monitoring features of OMIMSSC

State View Type displayed on the SCOM console	OMIMSSC monitoring feature			
	Server and Rack Workstation (Licensed)	Server and Rack Workstation (Licensed) using iSM-WMI	Chassis	Network Switches
Servers and Rack Workstation State View	No	No	No	No
Managed Rack Workstation State View	No	No	No	No
FM Servers State View	Yes	No	No	No
Sled Servers State View	No	No	No	No
Server (iSM) State View	No	Yes	No	No
Sled Server (iSM) State View	No	Yes	No	No
DRAC State View	No	No	No	No
Server and Rack Workstations (Licensed) State View	Yes	No	No	No
Managed Workstation (Licensed) State View	Yes	No	No	No
Sled Servers (Licensed) State View	Yes	No	No	No

Table 26. State views displayed by different monitoring features of OMIMSSC (continued)

State View Type displayed on the SCOM console	OMIMSSC monitoring feature			
	Server and Rack Workstation (Licensed)	Server and Rack Workstation (Licensed) using iSM-WMI	Chassis	Network Switches
Unmanaged Servers (Licensed) State View	Yes	No	No	No
FX2 Chassis State View	No	No	Yes	No
MX1000E Chassis State View	No	No	Yes	No
MX7000 Chassis State View	No	No	Yes	No
VRTX Chassis State View	No	No	Yes	No
Network Switch State View	No	No	No	Yes

Performance and power monitoring views displayed by different monitoring features of OMIMSSC

The performance view allows you to customize how you want to view performance data collected from performance objects and counters. This includes the ability to view historical and current operational data together. You must select Show in the Details pane to display data from a rule in the graph in the Results pane.

Performance and power monitoring view in the licensed monitoring feature of OMIMSSC for PowerEdge servers and workstations

The following OMIMSSC performance and power monitoring views are displayed for PowerEdge servers and workstations:

- Dell Performance View
- Disk Performance - iSM

(i) **NOTE:** By default, all performance metric rules are disabled for the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature.

(i) **NOTE:** Dell Performance View is available only when the Detailed feature of the Dell EMC Server and Rack Workstation Monitoring (Licensed) feature is installed, and you have selected Metrics Monitoring as Yes while overriding the metrics parameters.

As a part of the OMIMSSC performance and power monitoring view for servers and rack workstations, the following System Board Usage views are displayed:

- CPU Usage (%)
- IO Usage (%)
- Memory Usage (%)
- Overall System Usage (%)

(i) **NOTE:**
- System Board Usage metrics are supported only on some of the 13th generation of the PowerEdge servers. By default, the Dell Server Performance rule is set to Disabled.
- The Dell EMC Performance View displays the performance index of CPU, Memory and I/O utilization index, and system level CUPS index in a graphical format.

Performance and power monitoring view in the licensed monitoring feature of OMIMSSC for chassis

The following OMIMSSC performance and power monitoring view is displayed for Dell EMC chassis:

● Dell EMC Chassis Performance View

(i) **NOTE:** Dell EMC Chassis Performance View is available only when the Detailed feature of the Dell EMC Chassis Monitoring feature is installed, and you have selected Metrics Monitoring as Yes while overriding the metrics parameters.

OMIMSSC 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. 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.

Unit monitors in the licensed monitoring feature of OMIMSSC and Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack Version 7.3 for System Center Operations Manager for PowerEdge servers and workstations

All the following unit monitors provided by the licensed version (iDRAC WS-Man) of OMIMSSC are of **Periodic** type:

● Dell EMC PowerEdge Server
  ○ Dell Server Run As Account Association
  ○ Dell Server Unit Monitor
● Dell Server Power Supply
  ○ Dell Server Power Supply Unit
● Dell Server Processor Group
  ○ Dell Server Processor Group
● Dell Server Chassis Controller Sensor
  ○ Dell Server Chassis Controller Sensor
● Dell Storage Controller
  ○ Dell Server Storage Controller
● Dell Server Controller Battery
  ○ Dell Server Controller Battery Unit
● Dell Battery Sensor
  ○ Dell Server Battery Sensor Health
● Dell Battery Sensor Group
  ○ Dell Server Battery Group Sensor Health
● Dell Current Sensor
  ○ Dell Server Current Sensor Health
● Dell Fan Sensor
  ○ Dell Server Fan Sensor Health
● Dell Fan Sensor Group
  ○ Dell Server Fan Group Sensor Health
● Dell Intrusion Sensor
  ○ Dell Server Intrusion Sensor Health

- Dell Modular Blade Server With Operating System
  - Dell Server Run As Account Association
  - Dell Server Unit Monitor
- Dell Modular Blade Server Without Operating System
  - Dell Server Run As Account Association
  - Dell Server Unit Monitor
- Dell Monolithic Server With Operating System
  - Dell Server Run As Account Association
  - Dell Server Unit Monitor
- Dell Monolithic Server Without Operating System
  - Dell Server Run As Account Association
  - Dell Server Unit Monitor
- Dell Network Interfaces Group
  - Dell Server Network Interface Group
- Dell iDRAC Network Interface
  - Dell Server iDRAC Network Interface Unit
- Dell Server Capacity Threshold Check
  - Dell Server Capacity Threshold Check
- Dell Server Host NIC
  - Dell Server Host NIC
- Dell Server License
  - Dell Server License
- Dell Server License Group
  - Dell Server License Group
- Physical Network Interface
  - Dell Server Network Interface Unit
- PCIe SSD backplane
  - Dell Server PCIeSSD backplane
- PCIe SSD Extender
  - Dell Server PCIeSSD Extender
- PCIe SSD Physical Disk
  - Dell Server PCIeSSD Physical Disk Predictive Failure Disk
  - Dell Server PCIeSSD Physical Disk Primary Status
- Dell Server SD Card
  - Dell Server SD Card
  - Dell Server SD Card Group
- Dell Server Connector Enclosure
  - Dell Server Connector Enclosure
- Dell Storage Controller Enclosure EMM
  - Dell Server Enclosure EMM
- Dell Storage Controller Enclosure Fan Sensor
  - Dell Server Enclosure Fan Sensor
- Dell Storage Controller Enclosure Physical Disk
  - Dell Server Enclosure External Physical Disk
- Dell Storage Controller Enclosure Power Supply
  - Dell Server Enclosure Power Supply
- Dell Storage Controller Enclosure Temperature Sensor
  - Dell Server Temperature Sensor
- Dell Storage Controller Internal Physical Disk
  - Dell Server Internal Physical Disk Unit
- Dell Storage Controller Physical Disk
  - Dell Server Controller Direct Attached Physical Disk
- Dell Storage Group
  - Dell Server Storage
- Dell Storage Virtual Disk
  - Dell Server Controller Virtual Disk Unit

- Dell Temperature Sensor
  - Dell Server Temperature Sensor Health
- Dell Temperature Sensor Group
  - Dell Server Temperature Sensor Group Health
- Dell Voltage Sensor
  - Dell Server Voltage Sensor Health
- Dell Voltage Sensor Group
  - Dell Server Sensors Voltage Group

Unit monitors for Dell EMC Chassis Monitoring feature

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

- Dell EMC CMC/OME-M
  - Dell Chassis Run as Account Association
  - Dell CMC Status
- Dell Chassis Overall Health
  - Dell Chassis Overall Health Unit Monitor
- Dell Chassis IO Module
  - Dell Chassis IO Module Health Poll Based Unit Monitor
- Dell Modular Chassis Fan
  - Dell Chassis Fan Health Poll Based Unit Monitor
- Dell Chassis Modular Controller
  - Dell Chassis CMC Health Poll Based Unit Monitor
- Dell Chassis Modular Controller Group
  - Dell Chassis CMC Group Health Poll Based Unit Monitor
- Dell Chassis Modular Power Supply
  - Dell Chassis Power Supply Health Poll Based Unit Monitor
- Dell Chassis Modular Power Supply Group
  - Dell Chassis Power Supply Group Health Poll Based Unit Monitor
- Dell Chassis Modular PCIe Device
  - Dell Chassis PCIe Device Health Poll Based Unit Monitor
- Dell Chassis Storage Enclosure
  - Dell Chassis Storage Enclosure Health Poll Based Unit Monitor
- Dell Chassis Storage Controller
  - Dell Chassis Storage Controller Health Poll Based Unit Monitor
  - Dell Chassis Storage Controller Battery Health Poll Based Unit Monitor
- Dell Chassis Storage Controller Virtual Disk
  - Dell Chassis Storage Virtual Disk Health Poll Based Unit Monitor
- Dell Chassis Storage Controller Enclosure Internal Physical Disk
  - Dell Chassis Storage Internal Physical Disk Primary Health Status Poll Based Unit Monitor
  - Dell Chassis Storage Internal Physical Disk Predictive Failure Health Status Poll Based Unit Monitor
- Dell Chassis Storage Controller Enclosure External Physical Disk
  - Dell Chassis Storage External Physical Disk Primary Health Status Poll Based Unit Monitor
  - Dell Chassis Storage External Physical Disk Predictive Failure Health Status Poll Based Unit Monitor

Unit monitors for Dell EMC Network Switches Monitoring feature

All the following unit monitors provided by the network switches monitoring feature are of **Periodic** type:

- Dell EMC Network Switch
  - Dell EMC Network Switch Status
- Dell EMC Network Switch Fan Group
  - Dell EMC Network Switch Fan group Overall Health Unit Monitor
- Dell EMC Network Switch Fan units
  - Dell EMC Network Switch Fan Health Poll Based Unit Monitor

- Dell EMC Network Switch User port group
  - Dell EMC Network Switch user port group Health Poll Based Unit Monitor
- Dell EMC Network Switch User port units
  - Dell EMC Network Switch user port Health Poll Based Unit Monitor
- Dell EMC Network Switch Power Supply units
  - Dell EMC Network Switch power supply Health Poll Based Unit Monitor
- Dell EMC Network Switch Power Supply Group
  - Dell EMC Network Switch power supply Group Health Poll Based Unit Monitor
- Dell EMC Network Switch Interfaces
  - Dell EMC Network Switch Interfaces overall Health Unit Monitor

Event rules used by different monitoring features of OMIMSSC

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 OMIMSSC provide information the relevant event rules information to the administrators.

Event rules processed by the licensed (iDRAC WS-Man) monitoring feature of OMIMSSC for PowerEdge servers and workstations

Dell Systems Event Processing Rules

OMIMSSC processes rules from Dell EMC PowerEdge Servers.

Dell EMC PowerEdge Servers through iDRAC–WS-Man

All informational, warning, and critical SNMP traps for Dell EMC PowerEdge Servers discovered using Dell EMC Server and Rack Monitoring (Licensed) feature, have a corresponding SNMP trap rule. Each of these rules is processed based on the following criteria:

- Source Name = Dell Server IP
- OID = Actual trap ID of the trap event
- Data Provider = SNMP trap event provider

Event rules processed by the licensed (iSM-WMI) monitoring feature of OMIMSSC for PowerEdge servers and workstations

The following section lists the rules specific to the Dell EMC Server and Rack Workstation Monitoring feature using iSM-WMI.

- Dell Systems Event Processing Rules—OMIMSSC processes rules from Dell EMC PowerEdge Servers.
- Dell EMC PowerEdge Servers through iSM-WMI—All informational, warning, and critical events for Dell EMC PowerEdge Servers discovered using this feature, have a corresponding event rule. Each of these rules is processed based on the following criteria:
  - Source Name = "Lifecycle controller Log"
  - Event no= Actual event ID of the event
  - Data Provider = Windows System event log

Event rules processed by the licensed Chassis monitoring feature of OMIMSSC

- Dell Systems Event Processing Rules—OMIMSSC appliance processes rules from Chassis traps.
- Dell EMC Chassis devices—All informational, warning, and critical SNMP traps for the chassis devices have a corresponding SNMP trap rule. Each of these rules is processed based on the following criteria:
  - Source Name = DRAC/CMC name or IP

- OID = Actual trap ID of the DRAC or 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.

Additional resources

Table 27. Additional resources

Document	Description	Availability
Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) Release Notes	Provides information about new features, known issues, and workaround in the OMIMSSC appliance for SCOM.	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 Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager User's Guide	Provides information about installing, configuring, using, and troubleshooting Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager.	
Dell EMC Windows Server Agent-based and iDRAC7 or iDRAC8 SNMP Management Pack for System Center Operations Manager 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 System Center Operations Manager.	
Scalability with Dell EMC OpenManage Integration with Microsoft System Center (OMIMSSC) for System Center Operations Manager (SCOM) technical white paper	Provides information to scale up your monitoring capabilities by adding Dell EMC Alert Relay Servers in to your OMIMSSC environment.	

22

Accessing support content from the Dell support site

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

- Direct links:
  - OpenManage Integration for VMware vCenter
  - Dell OpenManage Enterprise
  - iDRAC
  - Dell Serviceability tools
- Dell support site:
  1. Go to Dell Support site.
  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.

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.

(i) **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.

A

Glossary

Table 28. Terms used in this guide

Term	Description
Alert Relay Server	Dell EMC Alert Relay Servers (previously known as Proxy Management Servers) helps to scale up monitoring capabilities in your OMIMSSC environment.
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 feature that is offered by OMIMSSC 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.
Dell EMC Servers and Rack Workstation monitoring (Licensed)	This is a license-based feature that is offered by OMIMSSC to discover and monitor 12th, 13th generation and iDRAC 9-based PowerEdge servers, PowerVault servers, supported Dell Precision Racks in a data center. The hardware monitoring of Dell EMC branded or Dell EMC OEM Ready servers and Dell EMC Microsoft Storage Spaces Direct Ready Nodes is also supported.
FMD	Dell EMC Feature Management Dashboard
iSM	iDRAC Service Module is a lightweight software that runs on the server and complements iDRAC with monitoring information from the operating system. For more information about iSM and the supported platform, see the **iDRAC Service Module Installation Guide** at Dell.com/support.
MS	Management Server
MP	Management Pack
OMIMSSC	Dell EMC OpenManage Integration for Microsoft System Center—Operations Manager
PowerEdge servers	PowerEdge monolithic servers, PowerEdge modular servers, PowerVault devices, supported Rack Workstations, Dell branded OEM servers, and Dell OEM Ready servers, unless otherwise specified.
SCOM	Microsoft System Center for Operations Manager.

Additional topics

Topics:

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

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

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

   (i) **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.

   (i) **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.
   > (i) **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 learn.microsoft.com/en-us.

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 microsoft.com/en-in/download/confirmation.aspx, 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.**