OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager

Unified User’s Guide

September 2020
Rev. A01

Notes, cautions, and warnings

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

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

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

Contents

Introduction to OMIMSSC

This document is an unified user's guide which contains all the information related to usage, installation, and best practices of OMIMSSC.

OpenManage Integration for Microsoft System Center (OMIMSSC) is an appliance-based integration into System Center suite of products. OMIMSSC enables full lifecycle management of Dell EMC PowerEdge servers by using integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC).

OMIMSSC offers operating system deployment, Storage Spaces Direct cluster creation, hardware patching, firmware update, and maintenance of servers and modular systems. Integrate OMIMSSC with Microsoft System Center Configuration Manager (SCCM) for managing the Dell PowerEdge servers in traditional data center, integrate OMIMSSC with Microsoft System Center Virtual Machine Manager (SCVMM) for managing The Dell PowerEdge servers in virtual and cloud environments.

For information about SCCM and SCVMM, see the Microsoft documentation.

ⓘ **NOTE:** The associated Dell EMC Deployment Tool Kit (DTK) version 6.4 is made available for latest iDRAC9 X5 based PowerEdge Servers, to be used with the OMIMSSC Pack only.

ⓘ **NOTE:** DTK is End of Life product from Dell EMC. This version of DTK is supported for use only with OMIMSSC version 7.2.1.

Topics:

What’s new?

- Support for System Center Configuration Manager (SCCM) version 1910.
- Support for System Center Configuration Manager (SCCM) version 2002.
- Support for System Center Virtual Machine Manager (SCVMM) 2016 UR8.
- Support for System Center Virtual Machine Manager (SCVMM) 2016 UR9.
- Support for System Center Virtual Machine Manager (SCVMM) 2019 UR1.
- Simplified user document. (Installation guide, User's guide, and Troubleshooting information consolidated in a single unified document).
- Reduced installer file size to support faster appliance download.
- Security fixes for Improper Authentication, Information disclosure for appliance logs, and Use of Hard-coded Cryptographic Key vulnerabilities have been implemented. For additional details on the security fixes, refer https://www.dell.com/support/security.
- Support for latest iDRAC9 based PowerEdge servers.

2

OMIMSSC components

The following is the list of the OMIMSSC components and their names that have been used in this guide:

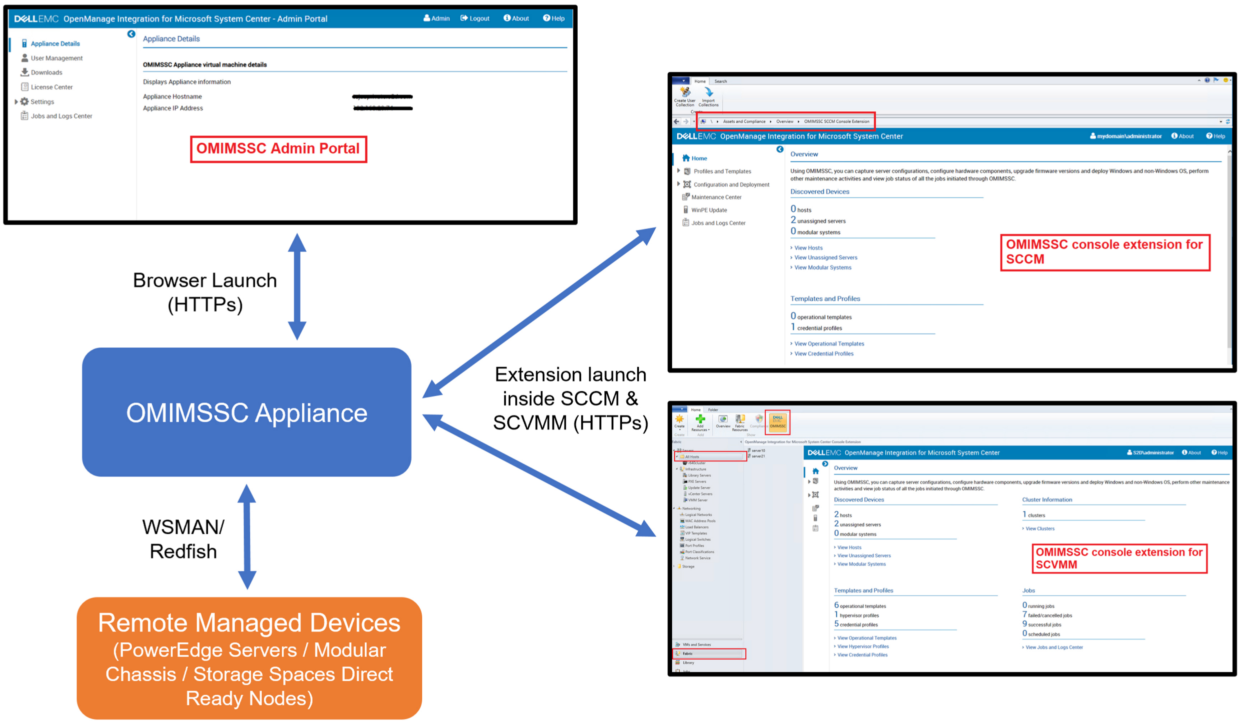
Table 1. Components in OMIMSSC

Components	Description
OpenManage Integration for Microsoft System Center Appliance virtual machine, also known as OMIMSSC Appliance.	Host the OMIMSSC Appliance on a Hyper-V as a virtual machine based on CentOS and performs the following tasks: ● Interacts with the Dell EMC servers through iDRAC by using Web Services Management (WSMan) commands. ● Interacts with Dell EMC PowerEdge MX7000 devices through OpenManage Enterprise Module (OME-Modular) by using REST API commands. ● Enables you to administer the OMIMSSC Appliance through the OMIMSSC admin portal.
OpenManage Integration for Microsoft System Center console, also known as the OMIMSSC console.	Same console extension is used on SCCM and SCVMM consoles, it is also known as: ● OMIMSSC console extension for SCCM ● OMIMSSC console extension for SCVMM

Management Systems are systems on which OMIMSSC and its components are installed.

Managed Systems are the servers that are managed by OMIMSSC.

OMIMSSC architecture


OMIMSSC Admin Portal
Browser Launch (HTTPs)
OMIMSSC Appliance
Extension launch inside SCCM & SCVMM (HTTPs)
OMIMSSC console extension for SCCM
OMIMSSC console extension for SCVMM
WSMAN/ Redfish
Remote Managed Devices
(PowerEdge Servers / Modular Chassis / Storage Spaces Direct Ready Nodes)

System requirements for OMIMSSC

Topics:

Support Matrix

All the available support matrix for OMIMSSC are as follows:

OMIMSSC **Supported System Center**

- Microsoft System Center Configuration Manager (SCCM) 2012 SP1
- Microsoft System Center Configuration Manager (SCCM) 2012 SP2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2 SP1
- Microsoft System Center Configuration Manager (SCCM) 1610
- Microsoft System Center Configuration Manager (SCCM) version 1809
- Microsoft System Center Configuration Manager (SCCM) version 1810
- Microsoft System Center Configuration Manager (SCCM) version 1902
- Microsoft System Center Configuration Manager (SCCM) version 1906
- Microsoft System Center Configuration Manager (SCCM) version 1910
- Microsoft System Center Configuration Manager (SCCM) version 2002
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 SP1
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR8
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR9
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR1
- Microsoft System Center Virtual Machine Manager (SCVMM) SAC version 1807

Table 2. Supported Devices

Dell EMC System	Supported Version
iDRAC 9 based PowerEdge Servers	● OS Driver Pack for supported AMD platforms: ○ R6515, R7515, C6525, and R6525 - 19.12.08 ○ R7525 - 19.12.07 ● Lifecycle Controller Version and Integration Dell EMC Remote Access Controller Version for supported AMD platforms: **SCCM** ○ R6515 and R7515 - 3.40.40.40 or higher ○ C6525 and R6525 - 3.42.42.42 or higher ○ R7525 - 4.10.10.10 or higher **SCVMM**

Table 2. Supported Devices (continued)

Dell EMC System	Supported Version
	○ R6515, R7515, C6525, R6525, and R7525 - 4.30.30.30 or higher ● Dell EMC OpenManage Deployment Tool kit Version - 6.4 **NOTE:** Operating system deployment for ESXi is not supported. **NOTE:** Operating system deployment with boot to vFlash \ stage to vFLash method and server profile backup features are not supported.
PowerEdge Servers 14th Generation	● OS Driver Pack: 17.05.21 ● Lifecycle Controller Version-3.00.00.00 or higher ● Integration Dell EMC Remote Access Controller Version -3.00.00.00 or higher ● Dell EMC OpenManage Deployment Tool kit Version - 6.3
PowerEdge Servers 13th Generation	● OS Driver Pack: 16.08.13 ● Lifecycle Controller Version-2.40.40.40 or higher ● Integration Dell Remote Access Controller Version-2.40.40.40 or higher ● Dell EMC OpenManage Deployment Tool kit Version - 6.3
PowerEdge Servers 12th Generation	● OS Driver Pack: for servers R220 & FM120 - 16.08.13 ● Other supported Platforms OS Driver Pack: 15.07.07 ● Lifecycle Controller Version 2.40.40.40 or higher ● Integration Dell Remote Access Controller Version 2.40.40.40 or higher ● Dell OpenManage Deployment Tool kit Version - 6.3
Chassis Management Console (CMC)	● FX2 1.4 or higher ● M1000e 5.2 or higher ● VRTX 2.2 or higher
Dell EMC OpenManage Enterprise-Modular	● PowerEdge MX7000 Chassis 1.0

NOTE: Support for 11th generation of PowerEdge servers is deprecated from OMIMSSC version 7.2.1 release onwards.

Table 3. Supported Operating Systems (Deployment):

Operating Systems	Supported Version
Microsoft Windows	● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2 ● Windows Server 2012 SP1
Linux Operating System	● RHEL 7.3, 7.4, 7.5 ● RHEL 7.2 ● RHEL 6.9
VMWare ESXi	● ESXi 6.0 - A02 ● ESXi 6.0 U3 - A15 ● ESXi 6.5 - A03 ● ESXi 6.5 U1 - A11 ● ESXi 6.7 - A06 **NOTE:** Download the image from https://www.dell.com/support/, refer to Drivers and Downloads page of the specific server model in accordance to OMIMSSC supported versions.

OMIMSSC Supported Clusters

- Creation and management of Windows 2016 and 2019 S2D enabled clusters on SCVMM console
- Management of Windows 2012 R2, 2016, and 2019 hyper-V host clusters on SCVMM console

Account privileges

All the required account privileges to use OMIMSSC are as follows:

Account privileges for OMIMSSC console extension for SCCM is that the user is a member of the following groups in SCCM:

Table 4. User accounts with required privileges

Users	Privileges/Roles
For enrollment	● Account used to enroll the SCCM console with OMIMSSC should be a full admin or an administrator in SCCM. ● Account used to enroll the SCVMM console with OMIMSSC should be a member of administrator role in SCVMM. ● Domain user. ● Member of Local Administrator group in system center machine.
For logging in to console extensions	● Account used to enroll the SCCM console with OMIMSSC should be a full admin or an administrator in SCCM. ● Account used to enroll the SCVMM console with OMIMSSC should be a delegated admin or an administrator in SCVMM. ● Domain user. ● Member of Local Administrator group in system center machine.

Common system requirements for OMIMSSC

Before installing OMIMSSC, ensure that you complete the following software prerequisite installations based on the three listed OMIMSSC components:

- OMIMSSC Appliance:
  - Install Windows Server, and enable the Hyper-V role.
  - You can now enroll any number of SCCM, or SCVMM consoles with one OMIMSSC Appliance, as OMIMSSC supports multiconsole enrollment. Based on number of consoles you plan to enroll, the following are the hardware requirements:

Table 5. Hardware requirements

Components	For one SCCM or SCVMM console	For N number of SCCM or SCVMM consoles
RAM	8 GB	8 GB*N
Processor counts	4	4*N

- Install one of the following versions of Windows operating system:
  - Windows Server 2019
  - Windows Server 2016
  - Windows server 2012 R2
  - Windows Server 2012
- OMIMSSC admin portal:

  Install any of the following supported browsers:
  - Internet Explorer 10 or later
  - Mozilla Firefox 30 or later
  - Google Chrome 23 or later

- Microsoft Edge

To follow specific OMIMSSC system requirements, you can now follow the requirements that are mentioned in bellow link as per the console you use:

- System requirements of OMIMSSC console extension for SCCM
- System requirements of OMIMSSC console extension for SCVMM

System requirements of OMIMSSC console extension for SCCM

To install OMIMSSC console extension for SCCM:

- Install the same versions of SCCM admin console and SCCM site server.

System requirements of OMIMSSC console extension for SCVMM

To install OMIMSSC console extension for SCVMM:

- Install the same versions of SCVMM admin console and SCVMM server.
- Failover clustering feature is enabled on SCVMM server.
- Enrolled user should have administrative rights on SCVMM server.
- Enrolled user should have administrative rights on the managed cluster.

Network requirements

Ports used in OMIMSSC Appliance:

Various OMIMSSC components use the following list of ports, and hence, include these ports in the firewall exception list:

Table 6. Ports information

Usage	Protocol	Port Number
iDRAC communication	WSMan	—
Modular Systems	REST	—
Autodiscovery	HTTPS	—
iDRAC—These ports are enabled for iDRAC to access the CIFS share that is created by the installer or users.	HTTPS	135 through to 139, and 445

4

Deploy OMIMSSC

Topics:

Downloading OMIMSSC from web

To download OMIMSSC, from https://www.dell.com/support perform the following steps:

1. Click **Browse all products** > **Software** > **Enterprise Systems Management** > **OpenManage Integration for Microsoft System.**
2. Select the required version of OMIMSSC.
3. Click **Drivers & downloads** tab.
4. Download OMIMSSC vhd file.
5. Extract the vhd file and then Set up OMIMSSC Appliance.
   The vhd file size will be about 5GB, hence the deployment will take about five to ten minutes to complete.
6. Specify the location to unzip the files and click unzip button to extract files:
   - **OMIMSSC_v7.2.1.2610_for_VMM_and_ConfigMgr**
   - **DellEMC_OpenManage_Deployment_Toolkit_Windows_6.4.0**

     ⓘ **NOTE:** The DTK version 6.4 is supported for use only with OMIMSSC version 7.2.1.

Setting up OMIMSSC Appliance

Ensure that the following requirements are met on the Hyper-V where you are setting up OMIMSSC Appliance:

- Virtual switch is configured and available.
- Allocate memory for OMIMSSC Appliance VM based on number of Microsoft consoles you plan to enroll. For more information, see the Common requirements.

To set up OMIMSSC Appliance:

1. Deploy the OMIMSSC Appliance VM by performing the following steps:
   a. In **Windows Server**, in **Hyper-V Manager**, from the **Actions** menu, select **New** and click **Virtual Machine Manager**. The **New Virtual Machine Wizard** is displayed.
   b. In **Before You Begin**, click **Next**.
   c. In **Specify Name and Location**, provide a name for the virtual machine.

      If you want to store the VM in a different location, and then select **Store the virtual machine in a different location**, click **Browse**, and traverse to the new location.
   d. In **Specify Generation**, select **Generation 1**, and then click **Next**.
   e. In **Assign Memory**, assign the memory capacity that is mentioned in the prerequisite.
   f. In **Configure Networking**, in **Connection**, select the network that you want to use, and then click **Next**.
   g. In **Connect Virtual Hard Disk**, select **Use an existing virtual hard disk**, traverse to the location where the **OMIMSSC_v7.2.1_for_VMM_and_ConfigMgr** VHD file is present, and select the file.

      The vhd file size will be about 5GB, hence the deployment will take about five to ten minutes to complete.
   h. In **Summary**, confirm the details that you have provided and click **Finish**.
   i. Set the **Number of virtual processors** count value to 4, since by default the processor count is set to 1.

      To set the processor count:

   i. Right-click OMIMSSC Appliance, and select **Settings**.
   ii. In **Settings**, select **Processor**, and set **Number of virtual processors** to **4**.

2. Start the OMIMSSC Appliance VM and perform the following tasks:
3. Perform the following tasks once OMIMSSC Appliance starts:

   ⓘ **NOTE:** It is recommended that you wait for five minutes before you log in as an **Admin** so that all services are initiated.

   a. In **localhost login**: Type admin.
   b. In **Enter new Admin password**: Type a password.

      ⓘ **NOTE:** Dell EMC recommends to configure and use strong passwords to authenticate appliance `admin` user and console extension.

   c. In **Please confirm new Admin password**: retype the password, and press **Enter** to continue.
   d. In the options listed, select **Configure Network**, press **Enter**, and perform the following substeps:
      - In **NetworkManagerTUI**, select **Set system hostname** provide the OMIMSSC Appliance name and click **OK**.

        For example, `Hostname.domain.com`

        ⓘ **NOTE:** You can change the IP address of OMIMSSC Appliance by selecting **Configure Network** option. You cannot change the IP address or host name of OMIMSSC Appliance after this point.
      - If you are providing a static IP address, select **Edit a connection**, and select **Ethernet0**.

        Select **IPv4 CONFIGURATION**, select **Manual**, and click **Show**. Provide the IP configuration address, gateway address, DNS server IP, and click **OK**.

   e. Note the OMIMSSC admin portal URL from OMIMSSC Appliance.

      ⓘ **NOTE:** Add the OMIMSSC Appliance IP and FQDN in Forward Lookup Zones and Reverse Lookup Zones in DNS.

      ⓘ **NOTE:** Appliance logs are accessible for non admin users. However, these logs do not carry sensitive information. As a workaround protect the appliance URL.

Enrolling multiple Microsoft consoles

Manage OMIMSSC Appliance resources when multiple Microsoft consoles are enrolled with OMIMSSC.

Based on number of Microsoft consoles you plan to enroll with OMIMSSC Appliance, ensure that the hardware requirements are met. For more information, see Common system requirements for OMIMSSC.

To configure resources for multiple Microsoft consoles, perform the following steps:

1. Launch and login to OMIMSSC Appliance.
2. Navigate to **Configure Enrollment Parameters**, and click **Enter**.
3. Provide the number of consoles you plan to enroll with OMIMSSC Appliance.
   The required resources are listed.

Launching OMIMSSC admin portal to download OMIMSSC components

1. Launch a browser and log in to the OMIMSSC admin portal by using the same credentials that were used while logging in to OMIMSSC Appliance

   Format: `https://<IP address or FQDN>`

   ⓘ **NOTE:** Add OMIMSSC admin portal's URL in **Local Intranet Site**. For more information, see Adding OMIMSSC IP address in browser
2. Click **Downloads**, and click **Download Installer** to download the required console extension.

Installing OMIMSSC console extension for SCCM

- Ensure that you install the OMIMSSC on the SCCM site server before using it in the SCCM admin console.
- It is recommended that you close Configuration Manager before installing, upgrading, or uninstalling the OMIMSSC console extension for SCCM.

1. Double-click `OMIMSSC_SCCM_Console_Extension.exe`.
   The **Welcome** screen is displayed.
2. Click **Next**.
3. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Destination Folder** page, by default an installation folder is selected. To change the location, click **Change** and traverse to a new location, and then click **Next**.
5. On the **Ready to Install the Program** page, click **Install**.

   The following folder is created after installing the console extension:
   - Log—this folder consists of console-related log information.
6. In **Installation Completed Successfully**, click **Finish**.

Installing OMIMSSC console extension for SCVMM

- Install OMIMSSC console extension on SCVMM management server and SCVMM console. Only after installing OMIMSSC console, you can import the console extension to SCVMM.

1. Double-click the `OMIMSSC_SCVMM_Console_Extension.exe` .
   The **Welcome** screen is displayed.
2. Click **Next**.
3. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Destination Folder** page, by default an installation folder is selected. To change the location, click **Change** and traverse to a new location, and then click **Next**.
5. On the **Ready to Install the Program** page, click **Install**.

   The following folders are created after installing the console extension:
   - Log—this folder consists of console-related log information.
   - OMIMSSC_UPDATE—This folder consists of all the activities that are required for Cluster Aware Update (CAU). This folder has read and write permissions only for CAU operations. Windows Management Instrumentation (WMI) permissions are configured for this folder. For more information, see Microsoft documentation.
6. In **InstallShield Wizard Completed** page, click **Finish**.
7. Import the OMIMSSC console extension for SCVMM in to SCVMM console. For more information see, Importing OMIMSSC console extension for SCVMM.

5

OMIMSSC licensing

OMIMSSC has two types of licenses:

- Evaluation license—this is a trial version of the license containing an evaluation license for five servers (hosts or unassigned) which is auto imported after the installation. This is applicable only for 11th and later generations of the Dell EMC servers.
- Production license—you can purchase production license from Dell EMC for any number of servers to be managed by OMIMSSC. This license includes product support and OMIMSSC Appliance updates.

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital Locker. If you are unable to download your license key(s), contact Dell Support by going to `dell.com/support/softwarecontacts` to locate the regional Dell Support phone number for your product.

You can discover servers in OMIMSSC using a single license file. If a server is discovered in OMIMSSC a license is used. And, if a server is deleted, a license is released. An entry is made in the activity log of OMIMSSC for the following activities:

- license file is imported
- server is deleted from OMIMSSC and license is relinquished.
- license is consumed after discovering a server.

After you upgrade from an evaluation license to a production license, the evaluation license is overwritten with the production license. The **Licensed Nodes** count is equal to the number of production licenses purchased.

Topics:

Options after uploading licenses

Following are the options supported for license feature in OMIMSSC

License file for new purchases

When you place an order for purchasing a new license, an email is sent from Dell about the order confirmation, and you can download the new license file from the Dell Digital store. The license is in an .xml format. If the license is in a .zip format, extract the license .xml file from the .zip file before uploading.

Stacking licenses

You can stack multiple production licenses to increase the number of supported servers to the sum of the servers in the uploaded licenses. An evaluation license cannot be stacked. The number of supported servers cannot be increased by stacking, and requires the use of multiple OMIMSSC Appliances.

If there are already multiple licenses uploaded, the number of supported servers are the sum of the servers in the licenses at the time the last license was uploaded.

Replacement of licenses

If there is a problem with your order, or when you try to upload a modified or corrupt file, an error message is displayed for the same. You can request for another license file from the Dell Digital Locker. Once you receive a replacement license, the replacement license contains the same entitlement ID of the previous license. When you upload a replacement license, the license is replaced if a license was already uploaded with the same entitlement ID.

Reimporting licenses

If you try to import the same license file, an error message is displayed. Purchase a new license, and import the new license file.

Importing multiple licenses

You can import multiple license files with different entitlement ID to increase the number of discovering, and maintaining servers in OMIMSSC.

Enforcement

Upgrading licenses

You are allowed to work with OMIMSSC with the existing license file for all the supported server generations. If the license file does not support the latest server generation, then purchase new licenses.

Evaluation License

When an evaluation license expires, several key areas cease to work, and an error message is displayed.

License consumption in OMIMSSC after server discovery

When you attempt to add a host or discover a bare-metal server, you are warned about your usage and it is recommended to purchase new licenses under the following circumstances:

- If the number of licensed servers exceed beyond the number of licenses purchased
- If you have discovered servers equal to the number of licenses purchased
- If you exceed the number of licenses purchased, then you are given a grace license.
- If you have exceeded the number of licenses purchased, and all the grace licenses.

ⓘ **NOTE:** Grace license is 20 percent of the total number of license purchased. So the actual licenses you can use in OMIMSSC is total licenses purchased plus the grace license.

Importing license in to OMIMSSC

After purchasing a license, import it in to OMIMSSC by performing the following steps:

1. In OMIMSSC admin portal, click **License Center**.
2. Click **Import License** and browse to select the license file downloaded from the Dell Digital store.

   ⓘ **NOTE:** You can import only valid license files. If the file is corrupt, or tampered, then an error message is displayed accordingly. Download the file again from the Dell Digital store or contact a Dell representative to get a valid license file.

Viewing license details

1. Open a browser, and provide the OMIMSSC Appliance URL.

   The OMIMSSC Admin Portal login page is displayed.
2. Click **License Center**.

   The page displays the following information.

   License Summary—displays the license details for OMIMSSC.

   - **Licensed nodes**—total number of licenses purchased

- **Nodes in use**—number of servers discovered and have used up the license
- **Nodes Available**—remaining licensed nodes that you can discover in OMIMSSC.

Managing Licenses—displays each license file imported along with the details such as entitlement ID, product description, date when the license file was imported, date from when the license file is valid, and list of all the server generations supported by the license.

6

Enrolling Microsoft console in OMIMSSC

- For SCCM users, OMIMSSC console extension for SCCM console is installed.
- For SCVMM users, OMIMSSC console extension for SCVMM is installed.

Ensure the following information is available:

- User credentials of the system on which Microsoft is set up, see required account privileges.
- FQDN of SCCM or FQDN of SCVMM.

To enroll an SCCM or SCVMM console with OMIMSSC, perform the following steps:

1. Open a browser, and provide OMIMSSC Appliance URL.
   The OMIMSSC admin portal login page is displayed.
2. Click **Settings**, click **Console Enrollment**, and then click **Enroll**.
   The **Enroll a Console** page is displayed.
3. Provide a name and description for the console.
4. Provide the FQDN of SCCM site server, or SCVMM server, and the credentials.
5. (Optional) Click **Create New** to create a Windows type credential profile to access SCCM or SCVMM console.
   - Select the **Credential Profile Type** as **Windows Credential Profile**.
   - Provide a profile name and description.
   - In **Credentials**, provide the user name and password.
   - Provide the domain details in **Domain**.

   ⓘ **NOTE:** Provide the domain name with Top Level Domain (TLD) details while creating the credential profile for console enrollment.

   For example, if the domain name is `mydomain`, and the TLD is `com`, provide the domain name in credential profile as: `mydomain.com`.
6. To verify the connections between OMIMSSC Appliance and Microsoft console, click **Test Connection**.
7. To enroll the console after a successful test connection, click **Enroll**.

   ⓘ **NOTE:** After enrollment, OMIMSSC creates an account in SCVMM with the name **OMIMSSC SCVMM Console Extension Registration Profile**. Ensure that this profile is not deleted, because you cannot perform any operations in OMIMSSC if this profile is deleted.

   ⓘ **NOTE:** Enroll the SCCM site server to use OMIMSSC console extension on SCCM admin console.

Topics:

Launching OMIMSSC from enrolled Microsoft console

Launch OMIMSSC from enrolled SCCM or SCVMM console.

Adding OMIMSSC FQDN address in browser

Before launching OMIMSSC, add the FQDN address of OMIMSSC as a prerequisite into the **Local Intranet** site list by performing the following steps:

1. Click **IE Settings**, and click **Internet Options**.
2. Click **Advanced**, and under **Settings**, search for the **Security** section.
3. Clear the **Do not save encrypted pages to disk** option, and click **OK**.

Launching OMIMSSC console extension for SCCM

View the user privileges table mentioned in Account privileges.

In SCCM console, click **Assets and Compliance**, click **Overview**, and then click the **OMIMSSC console extension for SCCM**.

> **NOTE:** If you are connecting to SCCM console using Remote Desktop Protocol (RDP), and then the OMIMSSC session may be logged out if the RDP is closed. Hence, log in again after reopening the RDP session.

Launching OMIMSSC console extension for SCVMM

To launch OMIMSSC console extension for SCVMM:

1. Import the console extension to SCVMM. For more information, see Importing OMIMSSC console extension for SCVMM.
2. Launch the console extension in SCVMM. For more information, see Launching OMIMSSC console extension from SCVMM.

Importing OMIMSSC console extension for SCVMM

To import the OMIMSSC console extension for SCVMM, perform the following steps:

1. Launch the SVMM console either by using Administrator privilege or as a Delegated Admin.
2. Click **Settings**, and then click **Import Console Add-in**.
   The **Import Console Add-in Wizard** is displayed.
3. Click **Browse** and select the .zip file from `C:\Program Files\OMIMSSC\VMM Console Extension`, click **Next**, and then click **Finish**.
   Ensure that the add-in is valid.

Launching OMIMSSC console extension for SCVMM

1. In SCVMM console, select **Fabric**, and then select the **All Hosts** server groups.

   > **NOTE:** To launch OMIMSSC, you can select any host group that you have permissions to access.

2. In **Home** ribbon, select **DELL EMC OMIMSSC** in the ribbon.

7

Managing OMIMSSC and its components

Topics:

Viewing OMIMSSC Appliance details

1. Launch the OMIMSSC admin portal from a browser.
2. Log in to OMIMSSC admin portal by using the same credentials that were used while logging in to OMIMSSC Appliance VM, and click **Appliance Details**. The IP address and host name of OMIMSSC Appliance is displayed.

Viewing OMIMSSC user management

1. Launch the OMIMSSC admin portal from a browser.
2. Log in to the OMIMSSC admin portal by using the same credentials that were used while logging in to OMIMSSC Appliance VM, and click **OMIMSSC User Management**. Status of users, previously logged in to SCCM or SCVMM is displayed.

Viewing or refreshing enrolled consoles

You can view all the enrolled Microsoft consoles with OMIMSSC by performing the following steps:

1. In OMIMSSC admin portal, click **Settings**, and then click **Console Enrolment**.

   All the enrolled consoles are displayed.
2. To view the latest list of enrolled consoles, click **Refresh**.

Changing OMIMSSC Appliance password

To change the password of OMIMSSC Appliance VM, perform the following steps:

1. Launch OMIMSSC Appliance VM, and login using the old credentials.
2. Navigate to **Change Admin Password**, and press **Enter**.
   The screen to change password is displayed.
3. Provide your present password, and then provide a new password matching the listed criteria. Re-enter the new password and press **Enter**.
   The status after changing the password is displayed.
4. To come back to home page, press **Enter**.

   NOTE: Appliance will reboot after changing the password.

Repairing or modifying installers

To repair any of the installer files, see the following topics:

- Repairing OMIMSSC console extension for SCCM
- Repairing OMIMSSC console extension for SCVMM

Repairing OMIMSSC console extension for SCCM

To repair the OMIMSSC files in case they are corrupt, perform the following steps:

1. Run the OMIMSSC console extension for SCCM installer.
   The **Welcome** screen is displayed.
2. Click **Next**.
3. In **Program Maintenance**, select **Repair**, and then click **Next**.
   The **Ready to Repair the Program** screen is displayed.
4. Click **Install**.
   A progress screen displays the progress of installation. After installation is complete, the **InstallShield Wizard Completed** window is displayed.
5. Click **Finish**.

Repairing OMIMSSC console extension for SCVMM

To repair the OMIMSSC files in case they are corrupt, perform the following steps:

1. Run the **OMIMSSC console extension for SCVMM** installer.
2. In **Program Maintenance**, select **Repair**, and then click **Next**.
3. In **Ready to Repair or Remove the program**, click **Repair**.
4. When the repair task is complete, click **Finish**.

Modifying SCCM and SCVMM accounts in OMIMSSC admin portal

By using this option, you can change the passwords of SCCM, and SCVMM accounts in OMIMSSC console.

You can modify the SCCM, and SCVMM administrator passwords from OMIMSSC admin portal. This process is a sequential activity.

1. Modify the password of SCCM or SCVMM administrator account in Active Directory.
2. Modify the password in OMIMSSC.

Perform the following steps to change the SCCM or SCVMM administrator account in OMIMSSC:

1. In the OMIMSSC Admin Portal, click **Settings**, and then click **Console Enrollment**.

   The enrolled consoles are displayed.
2. Select a console to edit, and click **Edit**.
3. Provide the new password, and click **Finish** to save the changes.

After updating the password, relaunch the Microsoft console, and OMIMSSC console extensions using the new credentials.

Backup and Restore OMIMSSC Appliance

Using **Backup Appliance Data** option from OMIMSSC Appliance, save OMIMSSC information such as enrolled Microsoft consoles, discovered devices, profiles, update sources, Operational Templates, licenses and completed jobs in OMIMSSC console extensions.

Topics:

Backup OMIMSSC Appliance

This functionality enables OMIMSSC appliance database and important configurations to be backed up. The backup file will be stored on CIFS share path with an encrypted password provided by the user. It is recommended that the appliance data is backed up periodically.

Pre-requisites:

- Ensure that you create CIFS share with access credentials and allow read and write permissions.
- Ensure the same encryption password is used for both backup and restore. The encryption password cannot be recovered

Perform the following steps for backing up OMIMSSC Appliance data on CIFS share.

NOTE: This feature is available from OMIMSSC version 7.2.1 onwards and not available on black console.

1. From the OMIMSSC admin portal, click **Settings**, and then click **Backup Appliance**.
2. In **Backup Settings and Details** page, provide CIFS share path for backup in the `\\<IP address or FQDN>\<folder name>` format.
3. Select the **Credential Profile for CIFS share** from the drop-down menu.
4. Enter the encryption password in the **Password** and **Retype Password** fields.
5. Click **Test Connection** to verify connectivity between the OMIMSSC Appliance and CIFS share.
   Ensure the mentioned backup folder exists and is accessible
6. Click **Backup** to backup the OMIMSSC Appliance data.

Next steps

To reconfirm if the backup is successful, go to backup folder. There will be two files created in the backup folder in the following format:

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

NOTE: Date and time shown in backup files will indicate when the backup was taken. Do not rename the backup file.

Restore OMIMSSC Appliance

Install the console extension of OMIMSSC version 7.2.1 before restoring the appliance, see Launching OMIMSSC admin portal to download OMIMSSC components section.

Restore OMIMSSC Appliance data in any of the following scenarios:

- Before upgrading to a new version of OMIMSSC
- Before migrating from one OMIMSSC Appliance to another OMIMSSC Appliance

Restoring OMIMSSC Appliance

Pre-requisites:

Ensure that you restore the data before performing any operations on the new OMIMSSC Appliance.

Perform the following steps for restoring old OMIMSSC Appliance data on a fresh OMIMSSC Appliance:

1. From the OMIMSSC admin portal, click **Settings**, and then click **Restore Appliance**
2. There are two options available for restoring appliance data.
   - `Option 1: Restore using IP address`

     This option should be used to restore data from OMIMSSC versions 7.1, 7.1.1, and 7.2.

     In IP Address, provide the IP address of the old OMIMSSC appliance, and click Restore.

     ⓘ **NOTE:** Data is restored to the new OMIMSSC appliance.
   - Option 2: Restore using a custom CIFS share

     This option should be used to restore data from 7.2.1 release onwards

     ⓘ **NOTE:** CIFS share access credentials are stored in the database as credential profile. For added security measures, encryption password should be provided to decrypt the backed up file.

   a. Provide the CIFS share location path in the `\\<IP address or FQDN>\<folder name>\<filename>.tar.gz` format.

   b. Select the Credential Profile for CIFS share from the drop-down menu.

   c. Enter the file encryption password and click Restore.

   The **Restore** page will be logged out automatically.
3. To view the status of restore, after the OMIMSSC appliance restarts:

   It is recommended that you wait for few minutes before you log in so that all services are initiated.

   a. Log in to OMIMSSC admin portal.

   b. Expand **Settings**, and then click **Logs**.

   c. Download the `dlciappliance_main.log` file, and search for the following message for a successful restore:

   ```
   Successfully restored OMIMSSC Appliance
   ```

Perform the following after restoring the old OMIMSSC Appliance:

- It is recommended that you re-create the scheduled jobs after restoring old OMIMSSC Appliance.
- For the hypervisor profiles exported from earlier version of OMIMSSC, ensure that you edit the profile to provide the ISO file path and Windows credential profile.

9

Uninstalling OMIMSSC

To uninstall OMIMSSC:

1. De-enroll the OMIMSSC console from the OMIMSSC admin portal. For more information, see De-enrolling OMIMSSC console.
2. Uninstall the OMIMSSC console extension for the registered Microsoft console. For information, see Uninstalling OMIMSSC console extension for SCCM or Uninstalling OMIMSSC console extension for SCVMM.
3. Remove OMIMSSC Appliance VM. For more information, see Removing OMIMSSC Appliance VM.
4. Remove Appliance-specific accounts. For more information, see Other uninstallation tasks.

Topics:

De-enrolling Microsoft console from OMIMSSC

In case you have enrolled multiple Microsoft consoles with one OMIMSSC Appliance, you can de-enroll one console and still continue working with OMIMSSC. For complete uninstallation, see *OpenManage Integration for Microsoft System Center Installation Guide*.

To de-enroll a Microsoft console, perform the following steps:

1. In OMIMSSC, click **Console Enrollment**.
   All the consoles that are enrolled with OMIMSSC Appliance are displayed.
2. Select the console and click **De-enroll** to remove the registration of the console with Appliance.
3. Uninstall the console plugin.

   NOTE:

   - After de-enrolling and uninstalling a console, the host servers that are associated with the console are moved to unassigned server list in OMIMSSC.

4. (Optional) In case the console is not reachable, click **Yes** when promoted to forcefully de-enroll the console.
   - If an OMIMSSC console is already open during de-enrollment, ensure that you close the Microsoft console to complete the de-enrollment.
   - For SCVMM users:
     - If you forcefully de-enroll SCVMM console from OMIMSSC when the SCVMM server is not reachable, manually delete the **Application Profile** in SCVMM.

Uninstalling OMIMSSC console extension for SCCM

Double-click `OMIMSSC_SCCM_Console_Extension.exe`, select **Remove**, and follow the instructions on the screen.

Uninstalling OMIMSSC console extension for SCVMM

To uninstall the OMIMSSC console extension for SCVMM:

1. Remove the console extension from **Uninstall a Program**.
2. Remove the console extension from SCVMM console.

Removing OMIMSSC console extension for SCVMM

1. In **Control Panel**, click **Programs**, and then click **Uninstall a Program**.
2. Select **Console Add-in for SCVMM**, and then click **Uninstall**.

Removing OMIMSSC console extension in SCVMM

1. In the SCVMM console, click **Settings**.
2. Right-click **OMIMSSC** and select **Remove**.

Other uninstallation steps

To remove the OMIMSSC console extension from SCVMM, delete the following accounts and profiles:

- Appliance-specific RunAsAccounts
- OMIMSSC Application Profile

Deleting Appliance-specific RunAsAccounts

To delete the Appliance-specific RunAsAccounts from the SCVMM console.

1. In the SCVMM console, click **Settings**.
2. Click **Run As Accounts**.
3. From the list of accounts, delete Appliance-specific accounts.

   The Appliance-specific accounts are prefixed as `Dell_`.

Deleting OMIMSSC application profile

1. In the SCVMM console, click **Library**, **Profiles**, and then click the **Applications profiles**.
   All the application profiles used in SCVMM are displayed.
2. Select and delete the **OMIMSSC Registration Profile**.

Removing Appliance VM

To remove Appliance VM:

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

10

Upgrading OMIMSSC for SCVMM

After installing and setting up OMIMSSC if a service pack update is available, and then by using the Service Pack Update feature in OMIMSSCyou can install the latest updates.

NOTE: Service Pack upgrade from previous versions of OMIMSSC to OMIMSSC v7.2 or v7.2.1 is not available.

To upgrade from an earlier version of OMIMSSC, back up the data of your current version and restore it in OMIMSSC version 7.2 or 7.2.1 appliance.

For more information about backup and restore of OMIMSSC appliance, see the Back up OMIMSSC Appliance section and Restore OMIMSSC Appliance section.

Topics:

About service pack updates

Once OMIMSSC is released, it is required to share any critical defect fixes or feature additions that are available as an upgrade or extension to the existing OMIMSSC Appliance. You can update service packs and other updates for the OMIMSSC Appliance operating system and OMIMSSC.

- You can place 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, once applied you cannot roll them back.
- The service packs are cumulative, that is, the latest service pack has fixes from all the previous releases.

The two types of service packs by OMIMSSC:

- OMIMSSC Appliance service packs.
- Infrastructure service packs.

Service packs updates can be applied using two methods:

- Using offline package.
- Using ***linux.dell.com***.

To apply the service pack updates using offline package, perform the following steps:

1. Download the service pack from the Web. For more information, see . Downloading OMIMSSC from web
2. Check the list of prerequisites for service pack updates. For more information, see .Instructions for upgrading service packs
3. Copy the downloaded service pack update to repository. For more information, see Copying service pack updates to repository.
4. Provide the repository URL information in OMIMSSC admin portal. For more information, see Proving repository URL information.
5. Install the service pack updates. For more information, see Installing service pack updates.

To apply the service pack updates using online package, perform the following steps:

1. Provide the repository URL information in OMIMSSC admin portal. For more information, see Proving repository URL information.
2. Install the service pack updates. For more information, see Installing service pack updates.

Installation prerequisites

- Ensure OMIMSSC for SCCM and SCVMM version 7.1 or version 7.1.1 or version 7.2 is deployed before upgrading to OMIMSSC for SCCM and SCVMM version 7.2.1
- Ensure that no jobs are running. If running, wait till the jobs are completed.
- Backup the OMIMSSC appliance data.

ⓘ **NOTE:** For information about the backup procedure, see the **Backup OMIMSSC Appliance** section.

Instructions for upgrading service packs

To upgrade from an earlier version of OMIMSSC, backup the data of your current version, and then update by using a service pack.

1. In the OMIMSSC Admin Portal, click **Settings** > **Service Pack Updates**
2. In the **Repository URL** box, enter the URL of the location of the service pack repository using one of the following update methods:
    a. To update using the offline package, in the **Repository URL** box, provide the URL information of the location where the service pack is saved in the format http://<hostname or IP address>/OMIMSSC_v7.2_SP/RPM_Repository.
    b. To update using the linux.dell.com, in the **Repository URL** box, provide the URL information in the format http://linux.dell.com/repo/omimssc-sccm-scvmm/<Service Pack Version> and if required, provide proxy server details and credentials to access the proxy server, and then click **Save**.
3. Select **Check for Updates** check box. The current version of OMIMSSC and service pack are displayed.
4. Click **Apply**, and then click **OK**
5. Navigate to **Settings** > **Logs** > in the upgradelogs directory, to view or download the log files for the service pack upgrade, select the <service pack version number> directory, for example <folder name> directory to view or download the log files for the service pack upgrade.
6. Log in to the **Admin Portal**, and then delete the browser cache history.
7. After the service pack update is complete, reboot the appliance manually.

For more information about creating service pack update repositories, see the About service pack updates section.

Copying service pack updates to repository

- Save the downloaded service pack in a repository.
- Ensure all the files formats in the server pack are supported by the HTTP server. If not, check with HTTP administrator to add the support. The following file formats are supported:
    - .RPM
    - .XML
    - .TXT
    - .BZ2

To enable `.BZ2` file format:

1. Open the IIS Manager on the server where the repo files are saved.
2. Expand the host name. Click **Sites** and then **Default Web Site**.
3. In **Action** pane click **Add**.
   The **Add MIME Type** window is displayed.
4. Provide the **File name extension** as **.BZ2** and **MIME type** as **APP/BZ2** and click **OK**.

Preparing repository

1. Place the service packs files directly in the HTTP server.
2. Double-click the downloaded service pack, and unzip the files to a location.
3. Copy the unzipped files to the HTTP site.

Providing repository URL information for service pack updates

To update OMIMSSC, provide URL information where the service pack updates are located.

To update OMIMSSC, using service pack updates, perform the following steps:

1. In **OMIMSSC**, select **Settings** > **Service Pack Updates**.
2. To update using the offline package, in **Repository URL**, provide the URL information in the format `http://<servername>:<portname>/<repository path>` and if required, provide proxy server details and credentials to access the server, and then click **Save**.

   NOTE: Ensure the host name provided in the URL does not contain an underscore (_).

   To update using linux.dell.com, in **Repository URL**, provide the URL information in the format `http://linux.dell.com/repo/omimssc-sccm-scvmm/<service pack version>` and if required, provide proxy server details and credentials to access the server, and then click **Save.**

Installing service pack updates

Check to see if the repository's URL information is available and included in the **Service Pack Updates** page, for more information see, Providing repository URL information.

To install service pack updates:

1. Once the service pack is placed in the HTTP site, in **OMIMSSC Admin Portal** > **Settings** > **Service Pack Updates**, click **Check for Updates**.

   For OMIMSSC, the existing version and the service pack version available in the repository are displayed.

   If necessary, you can view the Release Notes.
2. Click **Apply**, and then click **OK**.
3. Once the upgrade activity is complete, log in to the OMIMSSC admin portal and then clear the browser's cache history.

Postinstall:

To verify the Service Pack update:

1. In OMIMSSC admin portal, in **About**, views the Service Pack update version details.
2. For more information, in OMIMSSC admin portal, select **Settings** > **Logs**.
3. In the **upgradelogs** directory, to view or download the log files for the service pack upgrade, select the **<service pack version number>** directory, for example 1.2.0.207 directory to view or download the log files for the service pack upgrade.
4. If the service pack update has failed, and then contact **dell.com/support**.
5. Reboot the appliance manually.

   NOTE: After the service pack update is complete,

   - Upgrade the OMIMSSC console extension for SCCM
   - Upgrade the OMIMSSC console extension for SCVMM

Upgrading OMIMSSC console extension for SCCM

Ensure that you backup the old OMIMSSC Appliance. For more information, see Back up OMIMSSC Appliance.

1. From the OMIMSSC admin portal, click **Download Installer** and save the installer to a location.
2. Run the OMIMSSC installer.
3. In the message prompting you to upgrade, click **Yes**.
4. On the OMIMSSC Welcome page, click **Next**.
5. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Ready to Install the Program** page, click **Install**.
7. On the **InstallShield Wizard Completed** page, click **Finish** to complete the installation.

Upgrading OMIMSSC console extension for SCVMM

Ensure that you backup the old OMIMSSC Appliance. For more information, see Back up OMIMSSC Appliance.

1. From the OMIMSSC admin portal, click **Download Installer** and save the installer to a location.
2. Run the OMIMSSC installer.
3. In the message prompting you to upgrade, click **Yes**.
4. On the OMIMSSC Welcome page, click **Next**.
5. On the **License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
6. On the **Ready to Install the Program** page, click **Install**.
7. On the **InstallShield Wizard Completed** page, click **Finish** to complete the installation.
8. Delete the OMIMSSC console extension for SCVMM, and reimport the console extension. For information about removing the console, see Removing OMIMSSC console extension for SCVMM.

11

Rebooting OMIMSSC Appliance

To reboot OMIMSSC Appliance, perform the following steps:

1. Launch and login to OMIMSSC Appliance VM.
2. Navigate to **Reboot this Virtual Appliance**, and press **Enter**.
3. To confirm, click **Yes**.
   The OMIMSSC Appliance is restarted along with all the required services.
4. Log in to OMIMSSC Appliance after the VM restarts.

Logging out of OMIMSSC Appliance

1. Launch and login to OMIMSSC Appliance VM.
2. Navigate to **Log out**, and press **Enter**.

13

Managing profiles

Profiles contain all the data that is required for performing any operations in OMIMSSC.

Topics:

About credential profile

Credential profiles simplify the use and management of user credentials by authenticating the role-based capabilities of the user. Each credential profile contains a user name and password for a single user account.

OMIMSSC uses credential profiles to connect to the managed systems' iDRAC. Also, you can use credential profiles to access the FTP site, resources available in Windows shares, and to work with different features of iDRAC.

You can create four types of credential profiles:

- Device Credential Profile—used to log in to iDRAC or CMC. Also, you can use this profile to discover a server, resolve synchronization issues, and deploy operating system. This profile is specific to a console. You can use and manage this profile only in a console where it is created.
- Windows Credential Profile—used for accessing share folders in Windows operating system
- FTP Credential Profile—used for accessing an FTP site
- Proxy Server Credentials—used for providing proxy credentials for accessing any FTP sites for updates.

  ⓘ **NOTE:** All profiles other than device profile are shared resources. You can use and manage these profiles from any of the enrolled consoles.

Predefined credential profile

SYSTEM DEFAULT FTP account is a predefined credential profile available in OMIMSSC. The predefined credential profile is of type FTP, having **User Name**, and **Password** as **anonymous**. Use this profile to access `ftp.dell.com`

Creating credential profile

When creating a credential profile, consider the following points:

- During auto discovery, if a default credential profile is not available for iDRAC, and then the default iDRAC credentials is used. The default iDRAC user name is `root`, and password is `calvin`.
- To get information about the modular systems, the modular server is accessed with default CMC profile. The default CMC profile user name is `root` and password is `calvin`.
- (Only for SCVMM users) When a device type credential profile is created, an associated **RunAsAccount** is created in **SCVMM** to manage the device, and the name of the **RunAsAccount** is `Dell_CredentialProfileName`.
- Ensure that you do not edit, or delete the **RunAsAccount** in SCVMM.

1. In OMIMSSC, perform any of the following steps to create a **Credential Profile**:
   - In OMIMSSC dashboard, click **Create Credential Profile**.
   - In the navigation pane, click **Profiles** > **Credential Profile**, and then click **Create**.
2. In **Credential Type**, select the credential profile type that you want to use.
3. Provide a profile name and description.

   ⓘ **NOTE: Default Profile for** option is applicable only for a Device type credential profile.

4. In **Credentials**, provide the user name and password.

- If you are creating a **Device Credential Profile**, select to make this profile as the default profile to log in to iDRAC or CMC by selecting the **Default Profile for** option. Select **None**, if you choose not to set the profile as a default profile.
- If you are creating a **Windows Credential Profile**, provide the domain details in **Domain**.

  NOTE: While creating the credential profile for console enrollment, if the NETBIOS name is configured in Active Directory (AD), provide the NETBIOS name as a Domain. If NETBIOS name is not configured in the AD, provide the domain name with Top Level Domain (TLD) details.

  For example, if the domain name is `mydomain`, and the TLD is `com`, provide the domain name in credential profile as: `mydomain.com`
- If you are creating a **Proxy Server Credentials**, provide the proxy server URL `http://hostname:port` or `http://IPaddress:port` format in **Proxy Server URL**.

5. To create the profile, click **Finish**.

NOTE: When you create a device type credential profile in SCVMM, it creates a corresponding **RunAsAccount** with name that is prefixed with, **Dell_**. Ensure that the enrolled user has access to the corresponding **RunAsAccount** for operations such as Operating System deployment, which consumes the created device credential profile.

Modifying credential profile

Consider the following before modifying a credential profile:

- After creating, you cannot modify the type of a credential profile. However, you can modify other fields.
- You cannot modify a credential profile, if it is in use.

NOTE: The steps to modify any type of credential profile are the same.

1. Select the credential profile that you want to modify, click **Edit**, and update the profile.
2. To save the changes made, click **Save**.

To view the changes made, refresh the **Credential Profile** page.

Deleting credential profile

Consider the following when you are deleting a credential profile:

- When a device type credential profile is deleted, the associated **RunAsAccount** from SCVMM is also deleted.
- When **RunAsAccount** in SCVMM is deleted, the corresponding credential profile is not available in OMIMSSC.
- To delete a credential profile that is used in discovering servers, delete the discovered server and then delete the credential profile.
- To delete a device type credential profile that is used for deployment, first delete the servers that are deployed in the SCVMM environment and then delete the credential profile.
- You cannot delete a credential profile if it is used in an update source.

NOTE: The steps to delete any type of credential profile are the same.

Select the credential profile that you want to delete, and then click **Delete**.

To view the changes made, refresh the **Credential Profile** page.

About hypervisor profile (for SCVMM users)

A hypervisor profile contains a customized WinPE ISO (WinPE ISO is used for hypervisor deployment), host group, and host profile taken from SCVMM, and LC drivers for injection. Only OMIMSSC console extension for SCVMM users, can create and manage hypervisor profiles.

Creating hypervisor profile

Create a hypervisor profile and use the profile to deploy hypervisors.

- Update the WinPE ISO image, and have access to the share folder where the image is saved. For information about updating the WinPE image, see WinPE update.
- Create a host group, and host profile or physical computer profile, in SCVMM. For information about creating host groups in SCVMM, see Microsoft documentation.

1. In OMIMSSC, perform any one of the following tasks:
   - In the OMIMSSC dashboard, click **Create Hypervisor Profiles**.
   - In the left navigation pane, click **Profiles and Templates**, **Hypervisor Profile**, and then click **Create**.

   The **Hypervisor Profile Wizard** is displayed.
2. In the **Welcome** page click **Next**.
3. In **Hypervisor Profile**, provide a name and description of the profile, and then click **Next**.
4. In the **SCVMM Information** page,
   a. For **SCVMM Host Group Destination**, select an SCVMM host group from the drop-down menu to add the host into this group.
   b. From **SCVMM Host Profile/Physical Computer Profile**, select a host profile or physical computer profile from SCVMM that includes configuration information to be applied on servers.

      In SCVMM, select one of the following disk partition methods in a **Physical Computer Profile**:
      - When booting to UEFI mode, select **GUID Partition Table (GPT)** option.
      - When booting to BIOS mode, select **Master Board Record (MBR)** option.
5. In **WinPE Boot Image Source**, provide the following details, and click **Next**.
   a. For **Network WinPE ISO Name**, provide the share folder path having the updated WinPE file name. For updating WinPE file, see WinPE update.
   b. For **Credential Profile**, select the credentials having access to share folder having the WinPE file.
   c. (Optional) To create a windows credential profile, click **Create New**. For information about creating credential profile, see Creating credential profile.
6. (Optional) To enable LC driver injection, perform the following steps:

   > **NOTE:** Ensure that you select **Enable Dell Lifecycle Controller Drivers Injection** check-box, because the latest operating system driver packs for NIC cards are available in the latest operating system drivers.

   a. Select the operating system that you want to deploy so that the relevant drivers are selected.
   b. Select **Enable LC Drivers Injection**.
   c. Select the hypervisor version **Hypervisor Version**.
7. In **Summary**, click **Finish**.

To view the changes made, refresh the **Hypervisor profile** page.

Modifying hypervisor profile

Consider the following when you are modifying a hypervisor profile:

- You can modify host profile, host group, and drivers from Lifecycle Controller.
- You can modify the WinPE ISO name. However, you cannot modify the ISO image.

1. Select the profile that you want to modify and click **Edit**.
2. Provide the details, and click **Finish**.

To view the changes made, refresh the **Hypervisor profile** page.

Deleting hypervisor profile

Select the hypervisor profile that you want to delete, and click **Delete**.

To view the changes made, refresh the **Hypervisor profile** page.

14

Discovering devices and synchronizing servers with MSSC console

Discovery is the process of adding supported modular systems and PowerEdge bare-metal servers or host servers or nodes in to OMIMSSC.

Synchronization with MSSC console is the process of adding host servers from registered Microsoft console (SCCM or SCVMM) in to OMIMSSC. Hence, using any one of the processes, you can add devices in to OMIMSSC . Only after discovering the devices, you can manage them in OMIMSSC.

Topics:

Discovering devices in OMIMSSC

Discover MX7000 Modular Systems, hosts, and unassigned servers in OMIMSSC. Information about discovered devices is saved in OMIMSSC Appliance.

Using the following methods, you can discover Dell EMC servers using their iDRAC IP address:

- Discovering servers using auto discovery
- Discovering servers using manual discovery

> **NOTE:** The discovered device is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS that are required to work with OMIMSSC. For information about supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.

Discover Modular Systems with device IP address using Discovering modular systems using manual discovery method.

Device discovery in OMIMSSC console extension for SCCM

Discover devices in OMIMSSC console extension for SCCM. After discovering a server, the server is added to a predefined group in OMIMSSC, and one of the following SCCM predefined groups or collections—**All Dell Lifecycle Controller Servers collection** and **Import Dell Server collection** that are created under the **Device Collections**.

If the discovered server is not present in SCCM, or if there are no predefined groups or collections in SCCM, the predefined collections are created and the discovered server is and then added to the respective group.

Device discovery in OMIMSSC console extension for SCVMM

Discover Modular Systems, hyper-V hosts, and unassigned servers in OMIMSSC console extension for SCVMM. After discovery, the devices are added to respective predefined update groups.

System requirements for managed systems

Managed systems are the devices that are managed using OMIMSSC. The system requirements for discovering servers using OMIMSSC console extensions are as follows:

- OMIMSSC console extension for SCCM supports modular, monolithic, and tower server models on 12th and later generations of servers.
- OMIMSSC console extension for SCVMM supports modular and monolithic server models on 12th and later generations of servers.
- For source configuration and destination configuration, use same type of disks—only Solid-state Drive (SSD), SAS, or only Serial ATA (SATA) drives.
- For successful hardware profile RAID cloning, for destination system disks, use same or greater size and number of disks as present in the source.
- RAID sliced virtual disks are not supported.
- iDRAC with shared LOM is not supported.
- RAID configured on external controller is not supported.
- Enable Collect System Inventory on Restart (CSIOR) in managed systems. For more information, see iDRAC documentation.

Discovering servers using auto discovery

To automatically discover servers, connect servers to the network and power on the servers. OMIMSSC auto discovers the unassigned servers by using the remote enablement feature of iDRAC. OMIMSSC works as a provisioning server and uses iDRAC reference to auto discover servers.

1. In OMIMSSC, create a device type credential profile by providing the iDRAC credentials and make it as default for servers. For information about creating a credential profile, see Creating a credential profile.
2. Disable the existing Administrator account in iDRAC settings in the managed device.

   NOTE: It is recommended that you have a guest user account with operator privileges to log in to iDRAC in case auto discovery fails.

3. Enable the auto discovery feature in managed device's iDRAC settings. For more information, see iDRAC documentation.
4. In managed device's, iDRAC Settings, provide OMIMSSC Appliance IP in **provision server IP**, and then restart the server.

Discovering servers using manual discovery

To manually discover PowerEdge servers by using an IP address or an IP range. To discover servers, provide the iDRAC IP address and the device type credentials of a server. When you are discovering servers by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of a server.

Ensure that a default credential profile is available.

1. In OMIMSSC console, perform any one of the following steps:
   - In the dashboard, click **Discover Servers**.
   - In the navigation pane, click **Configuration and Deployment**, click **Server View**, and then click **Discover**.
2. In the **Discover** page, select the required option:
   - **Discover Using an IP Address**—to discover a server using an IP address.
   - **Discover Using an IP Range**—to discover all servers within an IP range.
3. Select the device type credential profile, or click **Create New** to create a device type credential profile.

   The selected profile is applied to all the servers.
4. In **iDRAC IP address**, provide the IP address of the server that you want to discover.
5. In **Discover Using an IP Address or IP Address Range**, do any of the following:
   - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
   - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.
6. Provide a unique job name, description for the job, and click **Finish**.

To track this job, the **Go to the Job List** option is selected by default.

The **Jobs and Logs Center** page is displayed. Expand the discovery job to view the progress of the job in **Running** tab.

After discovering a server, the server is added to **Hosts** tab, or **Unassigned** tab in the **Server View** page of **Configuration and Deployment** section.

- When you discover a server with an operating system that is deployed on it, and the server is already present in SCCM or SCVMM console, and then the server is listed as a host server under the **Hosts** tab.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, and then the server is listed as an unassigned server under the **Unassigned** tab in all the OMIMSSC console extensions, in case of multiple Microsoft consoles enrolled to single OMIMSSC Appliance.

After discovering a server, the server is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS to work with OMIMSSC. To view the firmware versions of the server components, hover the hover over the **Hardware Compatibility** column against the server row. For information about the supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.

A license is consumed for each discovered server. The **Licensed Nodes** count in **License Center** page decreases as the number of servers are discovered.

NOTE: To work with the servers discovered in the prior versions of OMIMSSC Appliance, rediscover the servers.

NOTE: When you log in to OMIMSSC as a delegated admin, you can view all the host servers and unassigned servers that are not specific to the logged in user. Hence, you cannot perform any operations on such servers. Make sure that you have the required privileges before performing any operations on such servers.

Discovering MX7000 by using manual discovery

To manually discover PowerEdge MX7000 Modular System by using an IP address or an IP range, provide a Modular System's IP address and device type credentials of the Modular System. When you are discovering Modular Systems by using an IP range, specify an IP (IPv4) range within a subnet by including the start and end range and the device type credentials of the Modular Systems.

Ensure that the default credential profile of a Modular System you want to discover is available.

To discover Modular Systems, perform the following steps:

1. In OMIMSSC, click **Configuration and Deployment**, click **Modular Systems View**, and then click **Discover**.
2. In the **Discover** page, select the required option:
    - **Discover Using an IP Address**—to discover a Modular System using an IP address.
    - **Discover Using an IP Range**—to discover all Modular Systems within an IP range.
3. Select the device type credential profile, or click **Create New** to create a device type credential profile.

    The selected profile is applied to all the servers.
4. In **IP address**, provide the IP address of the Modular System that you want to discover.
5. In **Discover Using an IP Address or IP Address Range**, do one of the following:
    - In **IP Address Start Range**, and **IP Address End Range**, provide the IP address range that you want to include, which is the starting and ending range.
    - Select **Enable Exclude Range** if you want to exclude an IP address range and in **IP Address Start Range** and **IP Address End Range**, provide the range that you want to exclude.
6. In **Modular Systems Discovery Methods**, select one of the following:
    - **Shallow discovery**—discovers Modular Systems and also number of servers in the Modular System.
    - **Deep discovery**—discovers Modular Systems and devices present in the Modular System such as Input Output Modules (IOM) and storage devices.

        NOTE: To deep discover MX7000 and its components, ensure that PowerEdge MX7000 and all its components are enabled with IPv4 address.
7. Provide a unique job name, and click **Finish**.

    To track this job, the **Go to the Job List** option is selected by default.

    To view the progress of the job in the **Running** tab, expand the discovery job in **Jobs and Logs Center**.

Synchronization of OMIMSSC console extension with enrolled SCCM

You can synchronize all servers (hosts and unassigned) from enrolled SCCM to OMIMSSC. Also, you get the latest firmware inventory information about the servers after synchronization.

Before synchronizing OMIMSSC and the enrolled SCCM console, ensure that the following requirements are met:

- Have details of default iDRAC credential profile for servers.
- Update the **Dell Default Collection** before synchronizing OMIMSSC with SCCM. However, if an unassigned server is discovered in SCCM, it is added to **Import Dell server collection**. To add this server in **Dell Default Collection**, add the server's iDRAC IP address in the **OOB** page.
- Ensure that there are no duplicate entries of devices in SCCM.

After synchronizing OMIMSSC with SCCM, if the device is not present in SCCM, and then the **All Dell Lifecycle Controller Servers** collection and the **Import Dell server** collection under **Device Collections** is created and the server is added to that respective group.

Synchronization of OMIMSSC console extension with enrolled SCVMM

You can synchronize all hyper-V hosts, hyper-V host clusters, modular hyper-V hosts, and unassigned servers from SCVMM consoles with OMIMSSC console extension for SCVMM. Also, you get the latest firmware inventory information about the servers after synchronization.

Consider the following before synchronizing OMIMSSC with SCVMM:

- Have details of default iDRAC credential profile for servers.
- If the host server's Baseboard Management Controller (BMC) is not configured with the iDRAC IP address, and then you cannot synchronize the host server with OMIMSSC. Hence, configure BMC in SCVMM (for more information, see MSDN article at `technet.microsoft.com`), and then synchronize OMIMSSC with SCVMM.
- SCVMM supports numerous hosts in the environment, due to which synchronization is a long running task.

Synchronizing with enrolled Microsoft console

To add servers managed in Microsoft console to OMIMSSC, perform the following step:

In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Synchronize with OMIMSSC** to synchronize all the hosts that are listed in enrolled MSSC with the OMIMSSC Appliance.

Resolving synchronization errors

The servers that are not synchronized with OMIMSSC are listed with their iDRAC IP address and host name.

NOTE: All servers that are not synchronized due to issues such as invalid credentials, or the iDRAC IP address, or connectivity, or other issues; ensure that you resolve the issues first, and then synchronize.

NOTE: During resynchronization, host servers that are deleted from the enrolled MSSC environment are moved to the **Unassigned Servers** tab in the OMIMSSC console extensions. If a server is decommissioned, and then remove that server from the list of unassigned servers.

To resynchronize servers with credential profile issues:

1. In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Resolve Sync Errors**.
2. Select the servers for resynchronization, and select the credential profile, or to create a credential profile click **Create New**.
3. Provide a job name, and if necessary select the **Go to the Job List** option to view the job status automatically once the job is submitted.
4. Click **Finish** to submit the job.

Viewing System Lockdown Mode

The System Lockdown Mode setting is available in iDRAC for 14th generation of servers and later. The setting when turned on locks the system configuration including firmware updates. After the System Lockdown mode is enabled, users cannot change any configuration settings. This setting is intended to protect the system from unintentional changes. To perform any operations on the managed servers, ensure that you disable the setting on it's iDRAC console. In OMIMSSC console, the System Lockdown mode status is represented with a lock image before the iDRAC IP address of the server.

- A lock image is displayed along with the servers's iDRAC IP if the setting is enabled on that system.
- An unlocked image is displayed along with the servers's iDRAC IP if the setting is disabled on that system.

NOTE: Before launching the OMIMSSC console extensions, verify the iDRAC System Lockdown Mode setting on the managed servers.

For more information about iDRAC System Lockdown Mode, see iDRAC documentation available at `dell.com/support`.

Deleting servers from OMIMSSC

To delete a server, perform the following steps:

Consider the following points before deleting a server:

- After you delete a server, the consumed license is relinquished.
- You can delete a server that is listed in OMIMSSC based on the following criteria:
    - An unassigned server that is listed in the **Unassigned servers** tab.
    - If you delete a host server that is provisioned in enrolled SCCM or SCVMM and present in OMIMSSC under the **Hosts** tab, first delete the server in SCCM or SCVMM, and then delete the server from OMIMSSC.

1. In the OMIMSSC console, click **Configuration and deployment**, and then click **Server View**:
    - To delete unassigned servers—in the **Unassigned Servers** tab, select the server, and click **Delete**.
    - To delete host servers—in the **Host Servers** tab, select the server, and click **Delete**.
2. In the confirmation dialog box, click **Yes**.

Deleting Modular Systems from OMIMSSC

To delete a Modular System, perform the following steps:

1. In OMIMSSC console, click **Configuration and deployment**, and then click **Modular Systems View**.
2. Select the Modular Systems, and click **Delete**.

15

Views in OMIMSSC

View all the devices discovered in OMIMSSC in **Configuration and Deployment** page along with their hardware and firmware inventory information. Also, view all the jobs with status in **Jobs and Logs Center** page.

Topics:

Launching Server View

The **Server View** page lists all unassigned and host servers that are discovered in OMIMSSC under **Unassigned Servers** and **Hosts** tabs.

In **Unassigned Servers** tab, view the iDRAC IP address, service tag, model, generation, processor speed, memory of the server, template compliance status for assigned Operational Template, Modular System's service tag if it is a modular server, and hardware compatibility information. On hovering over the **Hardware Compatibility** column, you can view the versions of BIOS, iDRAC, LC, and driver packs of the device. For more information about hardware compatibility, see About firmware update.

In **Hosts** tab, view host name, iDRAC IP address, service tag, model, generation, processor speed, memory of the server, Modular System's service tag if it is a modular server, cluster's Fully Qualified Domain Name (FQDN) if the server is part of a cluster, template compliance status for assigned Operational Template, and hardware compatibility information. On hovering over the **Hardware Compatibility** column, you can view the versions of BIOS, iDRAC, LC, and driver packs of the device. For more information about hardware compatibility, see About firmware update.

You can perform the following tasks on **Server View** page:

- Discover servers
- View updated information, by refreshing the page.
- Delete servers from OMIMSSC.
- Synchronize with enrolled Microsoft console.
- Resolving synchronization errors.
- Assign Operational Template and run Operational Template compliance.
- Deploy Operational Template
- Correlate servers to cluster group and the Modular System to which the server belongs to.
- Launch iDRAC console

To view servers:

1. In OMIMSSC console extension, click **Configuration and Deployment**, and then click **Server View**.
2. To view bare-metal servers, click **Unassigned Servers** tab.
3. To view host servers, click **Hosts** tab.
    a. To view host groups in nested format as grouped in SCCM or SCVMM, click **Select Console Hosts** drop-down menu.

    The **Select Console Hosts** drop-down menu lists all the host groups present in SCCM along with an internal group name. If you select the internal group name, all the hosts that are discovered and managed in SCCM and OMIMSSC are displayed.

After discovering servers, consider the following points:

- The **Operational Template** column is displayed as **Not Assigned**, after the servers are discovered. To update firmware and deploy operating system on these servers, assign and deploy Operational Templates. For more information, see Managing Operational Templates.
- The discovered servers are added to predefined groups in OMIMSSC. You can create custom update groups based on functional requirements. For more information, see About update groups.
- When you log in to OMIMSSC as a delegated admin, you can view all the host and unassigned servers that are not specific to this user. Hence, ensure that you have the required privileges before performing any operations on the servers.
- If there are multiple Microsoft consoles enrolled in OMIMSSC, and then host servers are specific to the Microsoft console where they are managed. And the unassigned servers are common to all consoles.

Launching Modular Systems view

The **Modular Systems View** page lists all the Modular Systems that are discovered in OMIMSSC.

View the CMC IP address, service tag, model, firmware version, template compliance status of Modular System for an assigned Operational Template, number of servers, Input/Output (I/O) Modules, and storage devices present on that Modular System. Configure the hardware and update Modular System firmware, by deploying the Operational Template.

You can perform the following tasks on **Modular Systems View** page:

- Discover Modular Systems using manual discovery
- Delete Modular System
- To view latest inventory information, refresh the page.
- Assign Operational Template for Modular System
- Deploy Operational Template for Modular System
- View I/O modules
- Launching I/O modules

To view Modular System discovered in OMIMSSC:

1. In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**.
   All the Modular Systems discovered model names are displayed.
2. To view a specific Modular System, click a model name under **Modular Systems View**.

   All the Modular Systems of that model are displayed with their service tag.
3. To view all devices present in that Modular System, click service tag.

   All the servers, Input Output modules, and storage devices along with their details are displayed.

   NOTE: Only after a deep discovery of a Modular System, all devices in the Modular System and their information are displayed.

   - By default the **Servers** tab is displayed.

     All the servers that are discovered in this Modular System are displayed.
   - To view all the Input Output Modules present in a Modular System, click **I/O Modules** tab.
   - To view all the storage devices present in the Modular System, click **Storage Devices** tab.

After discovering Modular Systems, consider the following points:

- The **Operational Template** column is displayed as **Not Assigned**, after the Modular Systems are discovered. To update firmware and deploy operating system on these Modular Systems, assign and deploy Operational Templates. For more information, see Managing Operational Templates.
- View the count of Input/Output, storage devices, and servers present in Modular Systems after a shallow discovery. Perform a deep discovery, to view more details about the components in a Modular System.

Launching OpenManage Enterprise Modular console

To launch OpenManage Enterprise Modular console, perform the following steps:

1. In OMIMSSC, expand **Configuration and Deployment**, and click **Modular Systems**.
2. Click **Device IP** of the Modular System.

Input/Output Modules

All the network Input/Output Modules along with their IP address, service tag, Input/Output type, model, firmware version and slot information are displayed.

Launch I/O Modules console from Input/Output Modules page.

To view information about Input/Output Modules, perform the following steps:

1. In OMIMSSC, click **Configuration and Deployment**, and then click **Modular Systems View**. Expand the **Modular Systems View**, and click service tag.

   All service tag of that model are displayed.
2. To view the Input/Output module, click **I/O Modules** tab.

Launching Input Output Modules console

To launch Input Output Module console, perform the following steps:

1. In OMIMSSC, expand **Configuration and Deployment**, click **Modular Systems View**. Expand the model to individual devices level.

   All devices under that model are displayed.
2. Click **I/O Modules** tab.
3. Click **IP address** of the device.

Launching Cluster View

The **Cluster View** page lists all the clusters that are discovered in OMIMSSC. View cluster's Fully Qualified Name (FQDN), service tag, and number of servers present in that cluster. Also, create a logical switch for clusters, and then create Storage Spaces Direct clusters using the predefined Operational Template.

You can perform the following tasks on **Cluster View** page:

- Creating logical switch (only for SCVMM 2016 and 2019 users)
- Creating Storage Spaces Direct clusters (only for SCVMM 2016 and 2019 users)
- Launching iDRAC console
- To view latest clusters discovered, refresh the page.

To view cluster groups discovered in OMIMSSC:

1. In OMIMSSC, click **Configuration and Deployment**, and then click **Cluster View**.
   All the different types of clusters are grouped and listed.
2. To view information about specific type of clusters, expand the cluster type.
   All the clusters of this type are listed on the left pane.
3. To view servers present in a cluster, click a cluster name.

Launching iDRAC console

To launch iDRAC console, perform the following step:

In OMIMSSC, expand **Configuration and Deployment**, and select one of the following:

- Click **Server View**. Based on the server (if it is a host or an unassigned server), click **Unassigned Servers** or **Hosts** tab, and click the **iDRAC IP** address of the server.

  The **Unassigned Servers** tab is displayed by default.

  To view the hosts tab, click **Hosts**.
- Click **Cluster View**. Expand the cluster type and expand cluster group to server level.

  The **Server** tab is displayed.

Launching Maintenance Center

The **Maintenance Center** page lists all the discovered devices in groups and the resources that are required for maintaining devices in OMIMSSC. To view S2D cluster groups in **Maintenance Center** page, ensure that you have chosen **All update groups** from the **Update Group** drop-down menu. View the device firmware inventory, manage the devices by keeping their firmware up-to-date as per the recommendations, revert the server to an earlier state if it has failed, bring up a replaced component to the same configuration of the old component, and export server logs for troubleshooting any issues. In **Update Settings** page view all the update sources, polling and notifications for latest updates from default update source, update groups of devices that require similar management, and all the protection vaults required for server configurations.

ⓘ **NOTE:** By default, OMIMSSC is packaged with a catalog file that displays an earlier version of the comparison report for predefined FTP, HTTP, and HTTPS update source. Hence, download the latest catalog to display the latest comparison report. To download the latest catalog, edit and save the FTP, HTTP, and HTTPS update sources.

ⓘ **NOTE:** Baseline version of a specific component of a device is marked as not available if the update is not present in the selected update source catalog.

You can perform the following tasks on **Maintenance Center** page:

- Create update source
- Set polling frequency
- Select predefined update groups or Create custom update groups.
- View and refresh firmware inventory
- Upgrade and downgrade firmware versions using run update method
- Create protection vaults
- Export server profiles
- Import server profiles
- Exporting inventory

To view **Maintenance Center** page:

In OMIMSSC, click **Maintenance Center**.
The **Maintenance Center** page is displayed.

Launching Jobs and Logs Center

View information about jobs initiated in OMIMSSC along with status of job's progress, and its subtask. Also, you can filter and view jobs of a particular job category.

You can view jobs that are initiated from OMIMSSC, in OMIMSSC Admin Portal and OMIMSSC console extension.

- OMIMSSC Admin portal—displays jobs that are initiated from all OMIMSSC consoles and users
- OMIMSSC console—displays jobs specific to a user and a console

Job names are either generated by the system or provided by users, and the subtasks are named after the IP address or hostname of the managed systems. Expand the subtask to view the activity logs for that job. Jobs are classified under four groups:

- **Running**—displays all the jobs that are currently running and in-progress state.
- **History**—displays all the jobs run in the past with its job status.
- **Scheduled**—displays all the jobs that are scheduled for a future date and time. Also, you can cancel these scheduled jobs.
- **Generic Logs**—displays OMIMSSC Appliance-specific, common log messages that are not specific to a task, and other activities. Every job is displayed with a user name and a console FQDN from where it was initiated.
  - **Appliance Log Messages**—displays all OMIMSSC Appliance-specific log messages such as restarting OMIMSSC Appliance. You can view this category of messages only from OMIMSSC Admin Portal.
  - **Generic Log Messages**—displays log messages that are common across different job categories that are listed in **Running**, **History**, and **Scheduled** tabs. These logs are specific to a console and a user.

    For example, if a firmware update job is in-progress for a group of servers, the tab displays log messages that belong to creating the Server Update Utility (SUU) repository for that job.

The various states of a job that is defined in OMIMSSC are as follows:

- **Canceled**—job is manually canceled, or after OMIMSSC Appliance restarts.
- **Successful**—job is completed successfully.

- **Failed**—job is not successful.
- **In Progress**—job is running.
- **Scheduled**—job has been scheduled for a future date and time.

  > **NOTE:** If multiple jobs are submitted simultaneously to the same device, the jobs fail. Hence, ensure that you schedule jobs for same device at different times.
- **Waiting**—job is in a queue.
- **Recurring Schedule**—job is scheduled at regular intervals.

1. In OMIMSSC, click **Jobs and Log Center**.
2. To view a specific category of jobs, such as **Scheduled**, **History**, or **Generic**, click the required tab.

   Expand a job to view all the devices included in that job. Expand further to view the log messages for that job.

   > **NOTE:** All the job-related generic log messages are listed under the **Generic** tab and not under the **Running** or **History** tab.
3. (Optional) Apply filters to view different groups of jobs and status of job in **Status** column.

16

Managing Operational Templates

Operational Templates contain complete device configuration and are used for deploying operating system and update firmware for PowerEdge servers and Modular Systems within Microsoft environment.

Operational Template replicates hardware and firmware of a reference server (golden server) on to many other servers while provisioning for operating systems. It contains firmware, hardware, and operating system components with its attribute set with current value of the reference server. These values can be modified before applying this template across devices. Also, you can check the compliance status against an assigned Operational Template and view the compliance report in a summary page.

Only these components that are available in the reference server would be retrieved and displayed as Operational Template components dynamically. For example, if the server does not have an FC component, the same is not displayed in the Operational Template.

For information about reference server and reference Modular System, see About reference server configuration and About reference Modular System configuration.

The following table describes the components that are listed in Operational Template and viewing and deploying capabilities of each component:

Table 7. Functionality of Operational Template

Component	Deploy Configuration	Firmware update	View Configuration	Operational Template compliance status
BIOS	Yes	Yes	Yes	Yes
iDRAC	Yes	Yes	Yes	Yes
NIC/CNA	Yes	Yes	Yes	Yes
RAID	Yes	Yes	Yes	Yes
FC	Yes	Yes	Yes	Yes
Windows	Yes	—	No	—
RHEL	Yes	—	No	—
ESXI	Yes	—	No	—
Management Module	Yes	Yes	Yes	Yes

Topics:

Predefined Operational Templates

Predefined templates have all the configurations that are required to create Storage Spaces Direct clusters or Windows Server Software-Defined (WSSD). OMIMSSC supports creating clusters on R740XD, R740XD2, and R640 Storage Spaces Direct Ready Node models along with their specific network adapters.

Table 8. List of predefined Operational Templates

Operational Template name	Description
R740XD_Mellanox_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having Mellanox card.
R740XD2_Mellanox_S2D_Template	Use this template for R740XD2 Storage Spaces Direct Ready Node models having Mellanox card.
R740XD_QLogic_S2D_Template	Use this template for R740XD Storage Spaces Direct Ready Node models having QLogic card.
R740XD2_QLogic_S2D_Template	Use this template for R740XD2 Storage Spaces Direct Ready Node models having QLogic card.
R640_Mellanox_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having Mellanox card.
R640_QLogic_S2D_Template	Use this template for R640 Storage Spaces Direct Ready Node models having QLogic card.

Consider the following points before deploying an Operational Template:

- The predefined templates are available only for management systems running SCVMM 2016 and 2019.
- The predefined Storage Spaces Direct template shows NIC card in slot 1. However, while deploying the Operational Template the NIC configuration is applied on the right slot. And if there are multiple NIC cards on the device, all the NIC cards are configured with the same configuration that is specified in the Operational Template.

About reference server configuration

A server configuration with a preferred boot sequence, BIOS, RAID settings, hardware configuration, firmware update attributes, and operating system parameters that is ideally suited for an organization is called reference server configuration.

Discover a reference server and capture the reference server settings in an Operational Template, and replicate it across different servers with same hardware configuration.

Creating Operational Template from reference servers

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a reference server by using the **Discovery** feature. For information about discovering servers, see Discovering servers using manual discovery.
- For SCCM users:
  - Create a task sequence. For more information, see Creating task sequence.
  - For non-Windows operating system deployment, have a device type credential profile. For more information, see Creating credential profile.
- For SCVMM users:
  - Create a hypervisor profile. For information about creating hypervisor profile, see Creating hypervisor profile.
  - For Windows deployment, have a device type credential profile. For more information, see Creating credential profile.
- If you are not using the default update source, and then create an update source. For more information, see Creating update source.

You can create an Operational Template by capturing the configuration of the reference server. After capturing the configuration, you can directly save the template, or edit the attributes for update source, hardware configuration, and Windows component as per your requirement. Now you can save the template, which can be used on PowerEdge homogeneous servers.

1. In OMIMSSC, do any of the following to open an Operational Template:
   - In the OMIMSSC dashboard, click **Create Operational Template**.
   - In the navigation pane, click **Profiles** > **Operational Template**, and then click **Create**.

   The **Operational Template** wizard is displayed.
2. Enter a name and description for the template.
3. Select the type of device, and enter the IP address of reference device, and then click **Next**.

   > ⓘ **NOTE:** You can capture the configuration of reference server with iDRAC 2.0 and later.

4. In **Device Components**, click a component to view the available attributes and their values.

   The components are as follows:
   - Firmware update
   - Hardware components, which are RAID, NIC, and BIOS.

     > ⓘ **NOTE:** In **iDRAC Embedded 1** component, following are the privileges and their values for **User Admin Privilege** attribute.
     >
     > **Table 9. Privilege value table**
     >
     > | Value | Privilege |
     > |---|---|
     > | 1 | Login |
     > | 2 | Configure |
     > | 4 | Configure Users |
     > | 8 | Logs |
     > | 16 | System Control |
     > | 32 | Access Virtual Console |
     > | 64 | Access Virtual Media |
     > | 128 | System Operations |
     > | 256 | Debug |
     > | 499 | Operator Privileges |

   - Operating system—select either Windows, or ESXi, or RHEL.
5. Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
6. Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.

   > ⓘ **NOTE:** Irrespective of the selection made in the check box against each component, all the configurations are captured in the template.

   In **Operating System** component, perform the steps in either of the following options, as per your requirement:
   - For Windows operating system deployment on SCCM, see Windows component for the OMIMSSC console extension for SCCM.
   - For Windows operating system deployment on SCVMM, see Windows component for the OMIMSSC console extension for SCVMM.
   - OMIMSSC
   - For non-Windows operating system deployment, see Non-Windows component for the OMIMSSC console extensions.
7. To save the profile, click **Finish**.

Windows OS component for OMIMSSC console extension for SCCM

While creating or editing Operational Template for server, perform the following steps for windows component:

1. Select a task sequence and deployment method.

   ⓘ **NOTE:** Only the task sequences deployed on collections are listed in the drop-down menu.

   For information about task sequence, see Task sequence.

2. Select one of the following options for the **Deployment method**:
   - **Boot to network ISO**—reboots specified ISO.
   - **Stage ISO to vFlash and Reboot**—downloads the ISO to vFlash and reboots.
   - **Reboot to vFlash**—reboots to vFlash. Ensure that the ISO is present in the vFlash.

     ⓘ **NOTE:** To use the **Reboot to vFlash** option, the label name of the partition that is created on vFlash must be **ISOIMG**.
3. (Optional) To use the image present in the network share, select the **Use Network ISO as Fallback** option.
4. enter an LC boot media image file.
5. Select the drivers required for the operating system.

Windows component for OMIMSSC console extension for SCVMM

While creating or editing Operational Template for server, perform the following steps for windows component:

Select **Hypervisor Profile**, **Credential Profile**, and **Server IP from**.

ⓘ **NOTE:** **Host Name**, and **Server Management NIC** are always pool values. For server management NIC, provide the MAC address of the network port through which you want the operating system to communicate to SCVMM.

If you select **Server IP from** as **Static**, and then ensure that you have configured the logical network in SCVMM, and the following fields are pool values:

- **Console Logical Network**
- **IP Subnet**
- **Static IP Address**

Non-Windows component for OMIMSSC console extensions

While creating or editing Operational Template for server, perform the following steps for non-windows component:

Select a non-windows operating system, operating system version, type of share folder, ISO file name, location of the ISO file and the password for the root account of the operating system.

(Optional) Select a Windows type credential profile for accessing the CIFS share.

Host name is a pool value and if you disable DHCP option, and then the following fields are pool values:

- **IP Address**
- **Subnet Mask**
- **Default Gateway**
- **Primary DNS**
- **Secondary DNS**

ⓘ **NOTE:** Network File System (NFS) and Common Internet File System (CIFS) share types are supported for non-Windows operating system deployment.

Creating Operational Template from reference Modular Systems

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a Modular System by using the **Discovery** feature. For information about discovering Modular Systems, see Discovering Modular System using manual discovery.
- If you are not using the default update source, and then create an update source. For more information, see Creating update source.

You can create an Operational Template by capturing the configuration of the reference Modular Systems. After capturing the configuration, you can directly save the template, or edit the attributes for update source and hardware configuration as per your requirement. Now you can save the template, that can be used to configure other Modular Systems of the same model.

NOTE: If you want to configure Active Directory (AD) users on other MX7000 devices ensure that you create an Operational Template from an MX7000 Modular System where all the AD users are configured.

NOTE: User account's passwords are not captured in Operational Template, from reference Modular System for security reasons. Edit the Operational Template to add a new user account and password, and then apply the Operational Template on the managed Modular Systems. Else, you can apply the Operational Template without any changes to user accounts, and the same passwords that are used in the reference Modular System are applied on the managed Modular System.

1. In OMIMSSC, do any of the following to open an Operational Template:
   - In the OMIMSSC dashboard, click **Create Operational Template**.
   - In the navigation pane, click **Profiles** > **Operational Template**, and then click **Create**.

   The **Operational Template** wizard is displayed.
2. Enter a name and description for the template.
3. In **Device Components**, click a component to view the available attributes and their values.

   The components are as follows:
   - Firmware update
   - Management Module Embedded

     NOTE: Ensure that the **Web Server** attribute is enabled. If this component is not enabled, and then the MX7000 Modular Systems cannot be accessed through OMIMSSC after deploying the Operational Template.

     NOTE: For **SNMP Configuration** and **Syslog Configuration**, ensure that you select all four configurations available in each attribute, to apply them on managed devices.
4. Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
5. Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.
6. To save the profile, click **Finish**.

Viewing Operational Template

To view Operational Templates created:

In OMIMSSC console, click **Profiles and Templates**, and then click **Operational Template**. All the templates that are created are listed here.

Modifying Operational Template

You can modify the update source, hardware configurations, and operating system of an operational template.

Consider the following before modifying an Operational Template:

- The values of few attributes depend on the values of other attributes. When you change attribute values manually, ensure that you also change the interdependent attributes. If these interdependent values are not changed appropriately, and then applying the hardware configurations may fail.
- Creation of Operational Template fetches all hardware configurations from the specified reference server which may contain attributes that are system-specific. For example, static IPv4 address, asset tag. To configure system-specific attributes, see Configuring system specific values using Operational Template
- Attributes in Operational Template are assigned with current values of the reference server. Operational Templates also lists other applicable values for the attributes.
- To modify predefined Operational Templates and custom created Operational Templates perform the following steps:

> **NOTE:** (For SCVMM users and servers only) All the mandatory attributes. (Mandatory attributes that are captured in the Operational Template are the Dell EMC recommended attributes for S2D cluster) required for Storage Spaces Direct are read-only attributes in the predefined Storage Spaces Direct template. However, you can edit the name of the template, operating system components, and non-mandatory hardware configuration attributes

1. Select the template that you want to modify and click **Edit**.
   The Operational Template page is displayed.
2. (Optional) Edit the name and description of the template, and then click **Next**.
3. To view the available attributes and their values in **Device Components**, click a component.
4. Modify the values of the available attributes.

   > **NOTE:** Select the check box against each component since only the selected component's configurations are applied on the managed system, when the Operational Template is applied.

   > **NOTE:** When editing Operational Template, few Advanced Host Controller Interface (AHCI) component attributes that are read-only are listed as editable. However, when these read-only attributes are set and the Operational Template is deployed, there are no changes that are made to the device.

   - For MX7000 Modular Systems:
     - Configurations are applied only if all the attributes for a group are selected. Hence, ensure that you select all the attributes in a group, even if you want to change one of the attributes in the group.
     - To add a new user through an Operational Template, select all the attributes of existing users that were exported when capturing the Operational Template, select the recently added user groups, and save the Operational Template.
     - To provide the time zone values, see Appendix.
5. For the operating system component, perform either of the following tasks depending on your requirement:
   - For Windows operating system deployment on SCCM, see Windows component for the OMIMSSC console extension for SCCM.
   - For Windows operating system deployment on SCVMM, see Windows component for the OMIMSSC console extension for SCVMM.
   - OMIMSSC
   - For non-Windows operating system deployment, see Non-Windows component for the OMIMSSC console extensions.
6. To save the profile, click **Finish**.

Configuring system specific values (Pool values) using Operational Template on multiple servers

OMIMSSC will retrieve as is configuration of the device. Attributes which are specific to a system, for example: Static IPv4 address for iDRAC will be displayed as a Pool Value in the Operational Template. Pool Value attributes which are dependent attributes are not selected by default and other attributes are selected by default.

1. Select the template that you want to modify and click Edit.
   The Operational Template page is displayed.
2. (Optional) Edit the name and description of the template, and then click **Next**.
3. To view the available attributes and their values in **Device Components**, click a component.
4. Expand the **Attribute Group**. If the value of the attribute is pool value, the attribute is identified to be system specific attribute.

5. Input to these system specific attributes can be given for multiple servers through a .CSV file using **Export Pool Attributes** while deploying Operational Template, see Deploying Operational Template on servers.
6. If you do not want to apply these system specific attributes, identify these attributes (mentioned in step 3) and unselect them while editing Operational Template.

Deleting Operational Template

To delete an Operational Template, perform the following steps:

Before deleting an Operational Template, ensure that:

- The selected Operational Template is not associated with any server or Modular System. If it is associated with a device, and then, unassign the template and then delete the template.
- No jobs that are associated with Operational Template are running.
- You have not selected a predefined Operational Template, since you cannot delete a predefined template.
- The steps to delete any type of Operational Template are the same.

Select the templates that you want to delete and click **Delete**. To confirm, click **Yes** .

Assigning Operational Template and running Operational Template compliance for servers

Assign an Operational Template to a server, and run the Operational Template compliance. Only after assigning an Operational Template to a server, you can view its Operational Template compliance status. You can compare a server's configuration with an Operational Template by assigning the template to a server. Once you assign an Operational Template, the compliance job runs and the Operational Template status is displayed on completion.

To assign an Operational Template, perform the following steps:

1. In OMIMSSC click **Configuration and Deployment**, and then click **Server View**. Select the required servers and click **Assign Operational Template and Run Compliance**.

   The **Assign Operational Template and Run Compliance** page is displayed.
2. Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

   The Operational Template drop-down lists templates, of the same type as that of the devices selected in the previous step.

   If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

   If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

   If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

   To view a detailed report, perform the following steps:

   a. Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.
      - Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.
      - Red color box—represents that the component is not present on the device.

Deploying Operational Template on servers

For deploying operating system on managed servers, ensure that you have the 4093492 KB article or later installed on your management system and on the operating system image that is used for deployment.

You can deploy Windows and non-Windows operating system—ESXi and RHEL by deploying the Operational Template assigned to servers.

NOTE: Download and install appropriate drivers from `Dell.com/support` if a yellow bang is displayed under Device Manager after you deploy Windows 2016 or Windows 2019 operating system on 12th generation of the servers.

NOTE: Deploying Operational Template on servers would be blocked if lock-down mode is enabled in the servers.

NOTE: When you deploy Windows to a UEFI-based device, format the hard drive that includes the windows partition by using a GUID Partition Table (GPT) file system. For more information, see UEFIGPT based hard drive partitions section of Microsoft documentation.

1. In OMIMSSC, click **Configuration and Deployment**, and click **Server View**. Select the servers on which you want to deploy a template on, and then click **Deploy Operational Template**.
   The **Deploy Operational Template** page is displayed.

   NOTE: If you see the prompt *`Press any key to boot to CD \ DVD .....`* while booting to the Task Sequence Media. For information on removing the prompt and automatically boot to Task Sequence Media, see Installing Windows to an EFI-Based Computer section of Microsoft documentation.
2. (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.

   Before exporting the pool values, add the IP address of the OMIMSSC Appliance where the OMIMSSC console extension is installed, to the local intranet site.
3. If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.

   The format of a .CSV file is `attribute-value-pool.csv`

   NOTE: Ensure that you select a .CSV file which has all proper attributes and the iDRAC IP or iDRAC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the iDRAC IP or iDRAC credentials changes and is marked as failed though the job may be successful in iDRAC.
4. Enter a unique job name, description for the job, and click **Deploy**.

   To track this job, the **Go to the Job List** option is selected by default.

Assigning Operational Template for Modular Systems

Assign an Operational Template to a Modular System and run the Operational Template compliance. This operation compares the configuration of a Modular System and an Operational Template by assigning the selected template to a Modular System. After you assign an Operational Template, the compliance job runs and the compliance status is displayed on completion.

To assign an Operational Template for Modular Systems, perform the following steps:

1. In OMIMSSC click **Configuration and Deployment**, and click **Modular Systems View**. Select the required Modular System and click **Assign Operational Template** .

   The **Assign Operational Template** page is displayed.
2. Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

   If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

   If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

   NOTE: The Operational Template compliance status excludes any changes that are made to user attributes.

   If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

   To view a detailed report, perform the following steps:

   a. Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.
      - Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.

- Red color box—represents that the component is not present on the device.

Deploying Operational Template for Modular System

You can configure Modular System components, and update the Modular System firmware versions by deploying the assigned Operational Template.

ⓘ **NOTE:** In a Multi-Chassis Management (MCM), if lead chassis is configured with **Propagation to member chassis**, and then configuring and updating lead chassis and member chassis from OMIMSSC will override the changes done through propagation.

1. In OMIMSSC, click **Configuration and Deployment**, and click **Modular Systems View**. Select the Modular System on which you have assigned the template, and then click **Deploy Operational Template**.
   The **Deploy Operational Template** page is displayed.
2. (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.
3. If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.

   The format of a .CSV file is `attribute-value-pool.csv`

   ⓘ **NOTE:** Ensure that you select a .CSV file which has all proper attributes and the CMC IP or CMC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the CMC IP or CMC credentials changes.
4. Enter a unique job name, description for the job, and click **Deploy**.

   ⓘ **NOTE:** There are no supported system-specific pool value attributes for Modular System. Hence, there are no pool values to be exported.

   To track this job, the **Go to the Job List** option is selected by default.

Unassigning Operational Template

1. In OMIMSSC, perform any one of the following tasks:
   - Click **Configuration and Deployment**, and click **Server View**.
   - Click **Configuration and Deployment**, and click **Modular System View**.

   Select the required devices and click **Assign Operational Template and Run Compliance**.

   The **Assign Operational Template and Run Compliance** page is displayed.
2. Select **Unassign** from **Operational Template** drop-down menu, and click **Assign**.
   Operational Template is unassigned to selected devices.

About reference Modular System configuration

A Modular System configuration with a preferred network configuration, user account, security, and alerts that is ideally suited for an organization is called reference Modular System configuration or reference chassis.

Discover a reference Modular System and capture the reference Modular System settings in an Operational Template, and replicate it across different Modular Systems of the same models.

17

Preparing for operating system deployment

Before deploying Windows operating system on the managed servers, update the WinPE image, create a task sequence, LC boot media file, and task sequence media bootable ISO file. The steps vary for SCCM and SCVMM console users. Refer the bellow section for more details. For deploying non-windows operating system remember the points mentioned in Preparing for non-Windows OS deployment section.

Topics:

About WinPE image

Windows Preinstallation Environment (WinPE) image is used for deploying operating system. Use an updated WinPE image for deploying operating system as the WinPE image available from SCCM or SCVMM may not contain the latest drivers. To create a WinPE image having all the required drivers, update the image using DTK. Ensure that relevant operating system-related driver packs are installed in Lifecycle Controller.

ⓘ **NOTE:** Do not change the filename of `boot.wim` file.

Providing WIM file for SCCM

Copy the `boot.wim` file from the following location `\\shareip\sms_sitecode\OSD\boot\x64\boot.wim`, and then paste it to a share folder accessible by OMIMSSC.
For example, location of shared path: `\\shareip\sharefolder\boot.wim`

Providing WIM file for SCVMM

Boot.WimPE base image to be provided for injecting in the latest boot critical Dell drivers from DTK is generated by installing PXE server in SCVMM.

1. Install and configure Windows Deployment Server (WDS) role on a server, and then add the PXE server to SCVMM.

   For information about adding the WDS role on a server, and adding a PXE server to SCVMM, see Provisioning a Hyper-V host or cluster from bare-metal computers section of Microsoft documentation.
2. Copy the `boot.wim` file from the PXE server present at the following location `C:\RemoteInstall\DCMgr\Boot\Windows\Images`, and then paste it to a share folder accessible by OMIMSSC.
   For example, location of shared path: `\\shareip\sharefolder\boot.wim`

WDS and PXE server is required only for generating the WinPE based boot.in image and not to be used in deployment scenarios.

Extracting DTK drivers

A DTK file contains the necessary firmware versions that are required for servers on which you are deploying the operating systems.

`To download DTK driver, launch` **https://www.dell.com/support**`/ -> Browse all products -> Servers -> PowerEdge -> Select the server type < C Series, Modular, Rack, or Tower> -> Select the server model -> Search for the keyword` **DTK** `and download the required version.`

ⓘ **NOTE:** While using the latest version of DTK for creating a WinPE ISO image, use the **Dell EMC OpenManage Deployment Toolkit for Windows** file. The **Dell EMC OpenManage Deployment Toolkit for Windows** file contains the necessary firmware versions that are required for systems on which you are deploying the operating systems. Use the latest version of the file, and do not use the **Dell EMC OpenManage Deployment Toolkit Windows Driver Cabinet** file for the WinPE update.

1. Double-click the DTK executable file.
2. To unzip the DTK drivers, select a folder.
   For example, `C:\DTK501`.
3. Copy the unzipped DTK folder to a share folder.
   For example, `\\Shareip\sharefolder\DTK\DTK501`

   ⓘ **NOTE:** If you are upgrading from SCVMM SP1 to SCVMM R2, and then upgrade to Windows PowerShell 4.0. and create a WinPE ISO image.

Updating WinPE image

A unique job name is assigned to each WinPE update job.

1. In OMIMSSC, select **WinPE Update**.
   The **WinPE Update** page is displayed.
2. In **Image Source**, for **Custom WinPE Image Path**, enter the WinPE image path along with the file name where the image is present.
   For example, `\\Shareip\sharefolder\WIM\boot.wim`.
3. Under **DTK Path**, for **DTK Drivers Path**, enter the location for the Dell EMC Deployment Toolkit drivers.
   For example, `\\Shareip\sharefolder\DTK\DTK501`
4. Under **Output File**, for **ISO or WIM File Name**, enter a name for the file along with the shared file path where the WinPE image will be generated.

   Enter one of the output file types:
   - WIM file for SCCM
   - ISO file for SCVMM

   ⓘ **NOTE:** Shared folder must be in the system center machine.
5. Under **Credential Profile**, for **Credential Profile**, enter the credentials that have access to the share folder where the WinPE image is saved.
6. (Optional) To view the job list, select **Go to the Job List**.

   A unique job name is assigned to each Windows Preinstallation Environment (WinPE) update.
7. Click **Update**.
   WinPE image with the file name that is provided in the preceding step is created under `\\Shareip\sharefolder\WIM`.

Preparing for operating system deployment on SCCM console

Before deploying operating system on managed servers discovered using OMIMSSC in SCCM console, create a Dell EMC specific or a custom task sequence, an LC boot media file, and task sequence media bootable ISO file.

Task sequence-SCCM

Task sequence is a series of commands that is used to deploy operating system on the managed system using SCCM.

Before creating Operational Template, Dell EMC recommends that you complete the following prerequisites.

- In Configuration Manager, ensure that the system is discovered and present under **Assets and Compliance** > **Device Collections** > **All Dell Lifecycle Controller Servers**. For more information, see Discover servers.
- Install the latest BIOS version on the system.
- Install the latest version of Lifecycle Controller on the system.
- Install the latest version of iDRAC firmware on the system.

ⓘ **NOTE:** Always launch the Configuration Manager console with administrator privileges.

Types of task sequence

You can create a task sequence in two ways:

- Create a Dell-specific task sequence using OMIMSSC Deployment template.
- Create a custom task sequence.

The task sequence goes to the next task sequence step irrespective of the success or failure of the command.

Creating Dell specific task sequence

To create a Dell-specific task sequence by using **OMIMSSC Server Deployment Template** option in SCCM:

1. Launch Configuration Manager.
   The Configuration Manager console screen is displayed.
2. In the left pane, select **Software Library** > **Overview** > **Operating Systems** > **Task Sequences**.
3. Right-click **Task Sequences**, and then click **OMIMSSC Server Deployment** > **Create OMIMSSC Server Deployment Template.**
   The **OMIMSSC Server Deployment Task Sequence Wizard** is displayed.
4. Type the name of the task sequence in the **Task Sequence Name** field.
5. Select the boot image that you want to use from the drop-down list.

   ⓘ **NOTE:** It is recommended that you use the Dell custom boot image that you created.

6. Under **Operating System Installation**, select the operating system installation type. The options are:
   - **Use an OS WIM image**
   - **Scripted OS install**
7. Select an operating system package from the **Operating system package to use** drop-down menu.
8. If you have a package with **unattend.xml**, and then select it from the **Package with unattend.xml info** menu, else select **<do not select now>**.
9. Click **Create.**
   The **Task Sequence Created** window is displayed with the name of the task sequence you created.
10. Click **Close** in the confirmation message box that is displayed.

Creating a custom task sequence

1. Launch the Configuration Manager.
   The Configuration Manager console is displayed.
2. In the left pane, select **Software Library** > **Overview** > **Operating Systems** > **Task Sequences**.
3. Right-click **Task Sequences**, and then click **Create Task Sequence**.
   The **Create Task Sequence Wizard** is displayed.
4. Select **Create a new custom task sequence**, and click **Next**.
5. Enter a name for the task sequence in the **Task sequence name** text box.
6. Browse for the Dell boot image that you had created, and click **Next**.
   The **Confirm the Settings** screen is displayed.
7. Review your settings and click **Next**.
8. Click **Close** in the confirmation message box that is displayed.

Editing a task sequence

ⓘ **NOTE:** While editing task sequence on SCCM 2016 and 2019, the missing objects references messages does not list **Setup windows and ConfigMgr** package. Add the package and then save the task sequence.

1. Launch the Configuration Manager.
   The Configuration Manager screen is displayed.

2. In the left pane, select **Software Library** > **Operating Systems** > **Task Sequence**.
3. Right-click the task sequence that you want to edit and click **Edit**.
   The **Task Sequence Editor** window is displayed.
4. Click **Add** > **Dell Deployment** > **Apply Drivers from Dell Lifecycle Controller.**
   The custom action for your Dell server deployment is loaded. You can now make changes to the task sequence.

   ⓘ **NOTE:** When editing a task sequence for the first time, the error message, **Setup Windows and Configuration Manager** is displayed. To resolve the error, create and select the Configurations Manager Client Upgrade package. For more information about creating packages, see the Configuration Manager documentation at **technet.microsoft.com**.

   ⓘ **NOTE:** When editing a task sequence on SCCM 2016 and 2019, the missing objects references messages do not list the Setup windows and ConfigMgr package. Hence, you must add the package and then save the task sequence.

Setting a default share location for the Lifecycle Controller boot media

To set a default share location for the Lifecycle Controller boot media:

1. In **Configuration Manager** , select **Administration** > **Site Configuration** > **Sites**
2. Right-click **<site server name>** and select **Configure Site Components**, and then select **Out of Band Management**.
   The **Out of Band Management Component Properties** window is displayed.
3. Click the **Lifecycle Controller** tab.
4. Under **Default Share Location for Custom Lifecycle Controller Boot Media**, click **Modify** to modify the default share location of the custom Lifecycle Controller boot media.
5. In the **Modify Share Information** window, enter a new share name and share path.
6. Click **OK**.

Creating a task sequence media bootable ISO

1. In Configuration Manager under **Software Library**, right-click **Task Sequences**, and select **Create Task Sequence Media**.

   ⓘ **NOTE:** Ensure that you manage and update the boot image across all distribution points before starting this wizard.

   ⓘ **NOTE:** OMIMSSC does not support the Standalone Media method to create Task Sequence Media.

2. From the **Task Sequence Media Wizard**, select **Bootable Media**, select **Allow unattended operating system deployment** option, and click **Next**.
3. Select **CD/DVD Set**, and click **Browse** and select the location to save the ISO image.
4. Click **Next**.
5. Clear the **Protect Media with a Password** check box and click **Next**.
6. Browse and select **PowerEdge server Deployment Boot Image**.

   ⓘ **NOTE:** Use the boot image created using DTK only.

7. Select the distribution point from the drop-down menu, and select the **Show distribution points from child sites** check box.
8. Click **Next**.
   The **Summary** screen is displayed with the task sequence media information.
9. Click **Next**.
   The progress bar is displayed.
10. On completion of creation of the image, close the wizard.

Preparing for non-Windows operating system deployment

Ensure that you remember the following points for deploying non-windows operating systems on managed systems:

- ISO file is available in either Network File System Version (NFS) or Common Internet File System (CIFS) share with read and write access.
- Confirm that virtual drive is available on the managed system.
- After deploying ESXi operating system, the server is moved to **Managed Lifecycle Controller (ESXi)** collection in SCCM.
- After deploying any type of non-windows operating system, the servers are moved to **Default Non-Windows Host Update Group**.
- It is recommended that the network adapter is connected to the network port in the server on which the operating system is being deployed.

18

Creating clusters using Operational Template

This chapter covers information about creating the Storage Spaces Direct clusters.

Topics:

Creating logical switch for Storage Spaces Direct clusters

Create logical switch from OMIMSSC in SCVMM.

ⓘ **NOTE:** The IP address that is entered in **Configuration for Management** section overrides the IP address that is entered in operating system component of Storage Spaces Direct predefined Operational Template.

1. In OMIMSSC, expand **Configuration and Deployment**, click **Cluster View**, and then click **Create logical switch** for Cluster.
2. Provide a name for the logical switch, and select the host group present in SCVMM for associating the logical switch.
3. Provide the following details, and click **Create**.
   a. In **Configuration for Management**, provide the **Subnet**, **Start IP**, **End IP**, **DNS Server**, **DNS Suffix**, and **Gateway** details.

      ⓘ **NOTE:** Provide the subnet information in Classless InterDomain Routing (CIDR) notation.

   b. In **Configuration for Storage**, provide the **VLAN**, **Subnet**, **Start IP**, and **End IP** details.
4. enter a unique job name, description for the job, and click **Create**.

   To track this job, the **Go to the Job List** option is selected by default.

To verify that the logical switch is created successfully, check for the logical switch name in the drop-down menu listed in **Create Cluster** page.

To view the details of the logical switch, perform the following steps in SCVMM:

1. To view the logical switch name, click **Fabric**, and in **Networking**, click **Logical Switches**.
2. To view the logical switch's Uplink Port Profile (UPP), click **Fabric**, and in **Networking**, click **Logical Switches**.
3. To view the logical switch's network, click **Fabric**, and in **Networking**, click **Logical Networks**.

Creating Storage Spaces Direct clusters

- Ensure that you create a logical network by using the **Create logical switch** for Cluster feature.
- Ensure that you are using SCVMM 2016 or 2019.
- Ensure that you are using Windows Server 2016 or 2019 Datacenter edition.
- Ensure that the managed servers configurations match the Storage Spaces Direct solution firmware and driver versions requirements. For more information, see *Dell EMC Storage Spaces Direct Ready Nodes PowerEdge R740XD , R740XD2, and PowerEdge R640 Support Matrix* documentation.
- For infrastructure and management details of Storage Spaces Direct, see *Dell EMC Microsoft Storage Spaces Direct Ready Node Deployment Guide for scalable hyper-converged infrastructure with R740xd, R740XD2, and R640 Storage Spaces Direct Ready Nodes* documentation.

  ⓘ **NOTE:** Storage Spaces Direct (S2D) is also referred as Windows Server Software-Defined (WSSD) and Azure Stack Hyper-converged Infrastructure (ASHCI).

Consider the following before creating Storage Spaces Direct clusters:

- You can create Storage Spaces Direct cluster in OMIMSSC by providing static IP address only.
- Virtual disk size is displayed as zero in the Storage Spaces Direct predefined Operational Template. But, after applying the Storage Spaces Direct predefined Operational Template, the virtual drive is created only of size equal to the full size of the M.2 physical storage media. For more information about the virtual drive space, see iDRAC User's Guide available at `dell.com/support`.
- You have to ensure that the IP address is configured in the operational template, if the operating system to iDRAC pass-through option is enabled.

To create Storage Spaces Direct cluster, perform the following steps:

1. In OMIMSSC, click **Configuration and Deployment** and then click **Cluster View**.
   The **Cluster View** page is displayed.
2. Provide a cluster name, and select the predefined Operational Template for creating Storage Spaces Direct clusters.
   - Unassigned servers that belong only to a specific server model and NIC card are displayed based on the Operational Template you select from **Operational Template** drop-down menu.
3. To add servers into a cluster, select the servers by using the check box.
4. To add system-specific pool values, click **Export Attribute Value Pool**.

   Edit and save the file so that you can provide the system-specific pool values. For more information, see Populating Pool Value CSV file.
5. (Optional) If you have to set system-specific values, in **Attribute Value Pool**, click **Browse** and select the edited .CSV file.
6. Provide a unique job name, and click **Create**.

   To track this job, the **Go to the Job List** option is selected by default.

   NOTE: When operating system deployment is in progress, you will see a host profile/physical computer profiles being cloned in SCVMM (name appended with server GUID) These profiles are consumed for individual server OSD.

To check if the clusters are created successfully:

1. Check for success status of cluster job creation.
2. View the cluster in **Cluster View** page.
3. View the cluster in SCVMM.

For more information, see Create a physical computer profile section section in Pre-requisites section of Microsoft documentation on Provisioning a Hyper-V host or cluster from bare-metal computers.

NOTE: It is recommended that cluster witness must be configured for a two node cluster. Cluster witness configuration helps maintain a cluster or storage quoram when a node or a network communication fails. For more information see Storage Spaces Direct deployment guide.

19

Firmware update in OMIMSSC

Maintain Dell EMC devices up-to-date by upgrading to the latest firmware to use security, issue fixes, and enhancements, using OMIMSSC. Update the firmware of devices using Dell EMC update repositories.

Updating firmware is supported only on hardware compatible devices. For using the features available in OMIMSSC on the managed devices, the managed devices must have the minimum required firmware versions of iDRAC, Lifecycle Controller (LC), and BIOS. Devices having the required firmware versions are hardware compatible.

Topics:

About update groups

Update groups are a group of devices that require similar update management. There are two types of update groups that are supported in OMIMSSC:

- Predefined update groups—You cannot manually create, modify, or delete the predefined update groups.
- Custom update groups—You can create modify and delete devices in these groups.

> **NOTE:** All server groups that exist in SCVMM are listed in OMIMSSC. However, the list of servers in OMIMSSC is not user-specific. Therefore, ensure that you have access to perform any operations on those devices.

Predefined update groups

After discovering a device, the discovered device is added to one of the following predefined groups.

- **Default host groups**—this group consists of servers that are deployed with Windows operating system or are synchronized with a registered Microsoft console.
- **Default unassigned groups**—this group consists of unassigned or bare-metal servers discovered.
- **Default non-windows host groups**—this group consists of servers that are deployed with non-windows operating systems.
- **Chassis update groups**—this group consists of modular servers and chassis or Modular Systems. 12th generation of servers and later are discovered along with their chassis information. By default, a group is created with the following name format, `Chassis-Service-tag-of-Chassis-Group`. For example, `Chassis-GJDC4BS-Group`. If a modular server is deleted from a cluster update group, and then the server is added to the chassis update group along with its CMC information. Even if there are no modular servers in the corresponding chassis update group, since all modular servers in the chassis are in a cluster update group, the chassis update group continues to exist, but displays only the CMC information.
- **Cluster update groups**—this group consists of **Windows Server Failover clusters**. If a 12th generation and later modular server is part of cluster, and then the CMC information is also added in the inventory in the **Maintenance Center** page.

Custom update groups

Create custom update groups of type **Generic update groups** by adding the discovered devices into groups that require similar management. However, you can add a device into a custom update group only from **Default unassigned update groups** and **Default host update groups**. To add the servers in custom update group, search for the required device using their service tag. After you add a device into a custom update group, the device is removed from the predefined update group and is available, only in the custom update group.

Viewing update groups

To view update groups:

1. In **OMIMSSC**, click **Maintenance Center** and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**.
   All the custom groups created are displayed with name, group type, and number of servers in the group.

Creating custom update groups

1. In OMIMSSC console, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, and then click **Create**.
   The **Firmware Update Group** page is displayed.
3. Provide a group name, description, and select the type of update group that you want to create.

   Custom update groups can have servers only from the following update group types:

   - Generic update group—consists servers from default unassigned update groups and default host update groups.
   - Host update group—consists servers from default host update groups.

   Also, you can have a combination of servers from the two types of server groups.
4. To add servers in the update group, search for the servers by using their service tag, and to add servers into the **Servers Included in the Update Group** table, click the right arrow.
5. To create the custom update group, click **Save**.

   Note: Custom update group is system center specific and will be visible to other users of same system center.

Modifying custom update groups

Consider the following points when you are modifying a custom update group:

- You cannot change the type of an update group after it is created.
- To move servers from one custom update group to another custom update group, you can:
  1. Remove the server from an existing custom update group. It is then automatically added into the predefined update group.
  2. Edit the custom group to add the server into, and then search for the server by using the service tag.

1. In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Edit** to modify the update group.

Deleting custom update groups

Consider the following points when you are deleting a custom update group in the following circumstances:

- You cannot delete an update group if it has a job that is scheduled, in-progress, or waiting. Hence, delete the scheduled jobs that are associated with a custom update group before deleting the server group.
- You can delete an update group even if servers are present in that update group. However, after deleting such an update group, the servers are moved to their respective predefined update groups.
- If a device that is present in custom update group, is deleted from MSSC, and you synchronize OMIMSSC with enrolled MSSC, the device is removed from the custom update group and is moved to the appropriate predefined group.

1. In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Settings**, click **Update Groups**, select the update group, and then click **Delete** to delete the update group.

About update sources

Update sources have reference to the catalog files that contain Dell EMC updates (BIOS, driver packs such as management components, network cards) and carry the self-contained executable file called Dell Update Packages (DUPs).

You can create an update source or a repository, and set it as a default update source for generating a comparison report, and receiving alerts when new catalog files are available at the repository.

Using OMIMSSC, you can keep the devices firmware up-to-date using online or offline update sources.

Online update sources are repositories that are maintained by Dell EMC.

Offline update sources are local repositories and used when there is no Internet connection.

It is recommended that you create custom repositories and place the network share in the local intranet of OMIMSSC Appliance. This would save the Internet bandwidth and also provide a secure internal repository.

Update firmware using one of the following update sources:

- **DRM repository**—is an offline repository. Export the inventory information of discovered devices from OMIMSSC Appliance to prepare a repository in DRM. For information about integration with DRM, and creating an update source through DRM, see Integration with DRM. After creating a repository in DRM, in OMIMSSC, select the update source that is created through DRM, relevant devices, and initiate an update on the devices. For information about DRM, see *Dell Repository Manager* documents available at `dell.com\support`.
- **FTP, HTTP, or HTTPS**—can be an online or offline repository. Update specific components of devices with respect to the latest update provided on FTP, HTTP, or HTTPS site. Dell EMC prepares a repository at every two months cadence and publishes the following updates through PDK catalogs:
  - Server BIOS and firmware
  - Dell EMC certified operating system driver packs—for operating system deployment

  NOTE: If you select an online update source, while deploying the Operational Template, the latest firmware versions are downloaded and applied on the managed devices. Hence, the firmware versions might differ between reference and deployed device.
- **Reference firmware inventory and comparison**—can be converted to an offline repository through DRM. Create a reference inventory file that contains the firmware inventory of the selected devices. The reference inventory file can contain inventory information of a device of the same type or model, or can have multiple devices of different types or models. You can compare the inventory information of devices present in OMIMSSC against the saved reference inventory file. To pass the exported file to DRM and create a repository, see *Dell Repository Manager* documents available at `dell.com\support`.

Predefined and default update source

OMIMSSC includes three predefined update sources that are available after a fresh installation, or upgrade. **DELL ONLINE FTP CATALOG** is a predefined update source of type FTP, **DELL ONLINE HTTP CATALOG** is a predefined update source of type HTTP, and **DELL ONLINE HTTPS CATALOG** is a predefined default update source of type HTTPS. However, you can create another update source and mark it as a default update source.

NOTE: If you are using proxy server, to access the repository, edit the update source to add the proxy details and save the changes.

Predefined and default update sources for Storage Spaces Direct clusters

OMIMSSC supports updating Storage Spaces Direct clusters through specific predefined update sources. These update sources have reference to catalog files that contain latest and recommended firmware versions of components for Storage Spaces Direct clusters. They are listed only on **Maintenance Center** page.

DELL ONLINE FTP S2D CATALOG is a predefined update source of type FTP, and is part of **DELL ONLINE FTP CATALOG**.

DELL ONLINE HTTP S2D CATALOG is a predefined update source of type HTTP, and is part of **DELL ONLINE HTTP CATALOG**.

DELL ONLINE HTTPS S2D CATALOG is a predefined default update source of type HTTPS, and is part of **DELL ONLINE HTTPS CATALOG**.

NOTE: Storage Spaces Direct (S2D) is also referred as Windows Server Software-Defined (WSSD) and Azure Stack Hyper-converged Infrastructure (ASHCI).

Predefined and default update sources for Modular Systems

OMIMSSC supports updating Modular Systems through specific predefined update sources. These update sources have reference to catalog files that contain latest and recommended firmware versions of components for Modular Systems. They are listed only on **Maintenance Center** page.

DELL ONLINE FTP MX7000 CATALOG is a predefined update source of type FTP, and is part of **DELL ONLINE FTP CATALOG**.

DELL ONLINE HTTP MX7000 CATALOG is a predefined update source of type HTTP, and is part of **DELL ONLINE HTTP CATALOG**.

DELL ONLINE HTTPS MX7000 CATALOG is a predefined default update source of type HTTPS, and is part of **DELL ONLINE HTTPS CATALOG**.

Validating data using test connection

To verify if the location of the update source is reachable by using the credentials that are mentioned while creating the update source, use **Test Connection**. Only after the connection is successful, you are enabled to create an update source.

Setting up local FTP

To set up local FTP:

1. Create a folder structure in your local FTP that is an exact replica of the online FTP, `ftp.dell.com`.
2. Download the `catalog.gz` file from online FTP and unzip the files.
3. Open the `catalog.xml` file and change the **baseLocation** to your local FTP URL, and compress the file with `.gz` extension.
   For example, change the **baseLocation** from `ftp.dell.com` to `ftp.yourdomain.com`.
4. Place the catalog file and the DUP files in your local FTP folder replicating the same structure as in `ftp.dell.com`.

Setting up local HTTP

To set up local HTTP:

1. Create a folder structure in your local HTTP that is an exact replica of `downloads.dell.com`.
2. Download the `catalog.gz` file from the online HTTP which is from the following location: `http://downloads.dell.com/catalog/catalog.xml.gz` and extract the files.
3. Extract the `catalog.xml` file and change the **baseLocation** to your local HTTP URL, and compress the file with `.gz` extension.
   For example, change the **baseLocation** from `downloads.dell.com` to host name or IP address such as `hostname.com`.
4. Place the catalog file with the modified catalog file, and the DUP files in your local HTTP folder replicating the same structure in `downloads.dell.com`.

Setting up local HTTPS

To set up local HTTPS:

1. Create a folder structure in your local HTTPS that is an exact replica of `downloads.dell.com`.
2. Download the `catalog.gz` file from the online HTTPS which is from the following location: `https://downloads.dell.com/catalog/catalog.xml.gz` and extract the files.
3. Extract the `catalog.xml` file and change the **baseLocation** to your local HTTPS URL, and compress the file with `.gz` extension.
   For example, change the **baseLocation** from `downloads.dell.com` to host name or IP address such as `hostname.com`.
4. Place the catalog file with the modified catalog file, and the DUP files in your local HTTPS folder replicating the same structure in `downloads.dell.com`.

Viewing update source

1. In **OMIMSSC**, click **Maintenance Center**.
2. In **Maintenance Center**, click **Maintenance Settings**, and then click **Update Source**.

   All the update sources created along with their description, source type, location, and credential profile name are displayed.

Creating update source

- Based on the update source type, ensure that a Windows or an FTP credential profile is available.
- Ensure that you install and configure DRM having Administrator roles, if you are creating a DRM update source.

1. In the OMIMSSC console, click **Maintenance Center** and then click **Maintenance Settings**.
2. In the **Update Source** page, click **Create New** and provide the update source name and description.
3. Select any of the following types of update source from the **Source Type** drop-down menu:
   - FTP Sources—select to create an online or local FTP update source.

     NOTE: If you are creating an FTP source, provide your FTP credentials along with proxy credentials if the FTP site is reachable by using proxy credentials.
   - HTTP Sources—select to create an online or local HTTP update source.

     NOTE: If you are creating an update source of type HTTP, provide the complete path of catalog with the catalog name and your proxy credentials to access the update source.
   - HTTPS Sources—select to create an online HTTPS update source.

     NOTE: If you are creating an update source of type HTTPS, provide the complete path of catalog with the catalog name and your proxy credentials to access the update source.

     DRM Repository—select to create a local repository update source. Ensure that you have installed DRM.

     NOTE: If you are creating a DRM source, provide your Windows credentials and ensure that the Windows shared location is accessible. In the location field, provide the complete path of the catalog file with the file name.
   - Inventory Output files—select to view the firmware inventory against reference server configuration.

     NOTE: You can view a comparison report by using **Inventory Output files** as an update source. The reference server's inventory information is compared against all other servers that are discovered in OMIMSSC.
4. In **Location**, provide the URL of the update source of an FTP or HTTP or HTTPS source and the Windows shared location for DRM.

   NOTE: The local FTP site must replicate the online FTP.

   NOTE: The local HTTP site must replicate the online HTTP.

   NOTE: Providing HTTP or HTTPS in the URL for an FTP source is not mandatory.
5. To access the update source, select the required credential profile in **Credentials**.
6. In **Proxy Credentials**, select the appropriate proxy credentials if proxy is required to access the FTP or HTTP source.
7. (Optional) To make the created update source as a default update source, select **Make this as default source**.
8. To verify that the location of the update source is reachable by using the mentioned credentials, click **Test Connection**, and then click **Save**.

   NOTE: You can create the update source only after the test connection is successful.

Modifying update source

Consider the following points before, modifying an update source:

- To edit **DELL ONLINE FTP S2D CATALOG, DELL ONLINE HTTP S2D CATALOG**, or **DELL ONLINE HTTPS S2D CATALOG** update source, edit the respective predefined update source, and save the changes. This update reflects in **DELL ONLINE FTP S2D CATALOG, DELL ONLINE HTTP S2D CATALOG**, or **DELL ONLINE HTTPS S2D CATALOG**update source.
- You cannot change the type of an update source and the location after the update source is created.

- You can modify an update source even if the update source is in use by an in-progress or a scheduled job, or if it is used in a deployment template. A warning message is displayed while modifying the in-use update source. Click **Confirm** to go to the changes.
- When a catalog file is updated in the update source, the locally cached catalog file is not automatically updated. To update the catalog file saved in cache, edit the update source or delete and re-create the update source.

Select the update source that you want to modify, click **Edit**, and then update the source as required.

Deleting update source

Consider the following points before, deleting an update source:

- You cannot delete a predefined update source.
- You cannot delete an update source if it is used in an in-progress, or a scheduled job.
- You cannot delete an update source if it is a default update source.

Select the update source that you want to delete, and click **Delete**.

Integration with Dell EMC Repository Manager(DRM)

OMIMSSC is integrated with DRM to create custom update sources in OMIMSSC. The integration is available from DRM version 2.2 onwards. Provide the discovered device information from OMIMSSC Appliance to DRM, and using the available inventory information, you can create a custom repository in DRM and set it as an update source in OMIMSSC for performing firmware updates and creating clusters on managed devices. For more information about creating a repository in DRM, see *Dell EMC Repository Manager* documents available at `Dell.com/support/home`.

Integrating DRM with OMIMSSC

This section describes the process to create a repository with integration.

NOTE: Consider factors such as testing on test environment, security updates, application recommendations, Dell EMC advisories, to prepare the required updates.

NOTE: To view the latest inventory information about discovered devices, after upgrading OMIMSSC, reintegrate DRM with OMIMSSC Appliance.

1. In the Home page, click **Add New Repository**. **Add New Repository** window is displayed.
2. Select the **Integration** tab, enter the **Repository Name** and **Description**.
3. Select **Custom** and click **Choose Systems** to select any specific system.
4. From the **Integration Type** drop-down menu, select the product with which you want to integrate. Based on the product selected the following options are displayed. The available options are:
   a. Dell OpenManage integration for Microsoft System Center - Provide Hostname or IP, Username, Password, and proxy server.

      NOTE: Ensure the password does not contain special characters such as, `<, >, ',", &`.

   b. Dell Console Integration - Provide URL https://<IP>/genericconsolerepository, Admin as Username, Password, and proxy server.

   NOTE: Dell Console Integration is applicable for consoles that have incorporated the web services such as OpenManage Integration for System Center Virtual Machine Manager (SCVMM).

5. After selecting the required option click **Connect**. The available system and model will be displayed in the **Integration Type** section.
6. Select **Add** to create the repository. The repository is displayed in the repository dashboard available in the home page.

   Note: While selecting bundle types or DUP formats, ensure to select Windows 64-bit and Operating System independent, if Dell PowerEdge MX7000 chassis is part of the inventory in OMIMSSC.

After integrating DRM with OMIMSSC, see *Obtain firmware catalog for Storage Spaces Direct Ready Nodes Using Dell Repository Manager* section from *Dell EMC Microsoft Storage Spaces Direct Ready Node Operations Guide for managing and monitoring Ready Node life cycle* at `dell.com/support`

Setting polling frequency

Configure polling and notifications, to receive alerts when there is a new catalog file available at the update source, that is selected as default. OMIMSSC Appliance saves a local cache of the update source. The color of the notification bell changes to orange color when there is a new catalog file available at the update source. To replace the locally cached catalog available in OMIMSSC Appliance, click the bell icon. After replacing the old catalog file with the latest catalog file, the bell color changes to green.

To set the polling frequency:

1. In OMIMSSC, click **Maintenance Center**, and then click **Polling and Notification**.
2. Select how frequently the polling should happen:
   - **Never**—this option is selected by default. Select to never receive any updates.
   - **Once a week**—select to receive updates about new catalogs available at update source on a weekly basis.
   - **Once every 2 weeks**—select to receive updates about new catalogs available at update source once every two weeks.
   - **Once a month**—select to receive updates about new catalogs available at update source on a monthly basis.

Viewing and refreshing device inventory

View comparison report for devices against an update source in **Maintenance Center** page. On selecting an update source, a report is displayed comparing existing firmware to the firmware present in the selected update source. The report is generated dynamically on changing the update source. Server inventory is compared with update source, and suggestive actions are listed. This activity takes considerable time based on the number of devices and device components present. You cannot perform other tasks during this process. Refreshing inventory refreshes the entire device's inventory even though you select a single component in that device.

Sometimes, the inventory of the device is updated, but the page does not display the latest inventory. Hence, use the refresh option to view the latest inventory information of the discovered devices.

NOTE: After upgrading to the latest version of OMIMSSC, if the connection to `ftp.dell.com` or `downloads.dell.com` fails, the default Dell online FTP, Dell HTTP, or Dell HTTPS update source cannot download the catalog file. Hence, the comparison report is not available. To view a comparison report for the default update source, edit the default Dell online FTP, the Dell HTTP, or the Dell HTTPS update source, (provide the proxy credentials if required), and then select the same from the **Select Update Source** drop-down menu. For more information about editing an update source, see Modifying update source.

NOTE: A local copy of the catalog file is in OMIMSSC when the product is delivered. Therefore, the latest comparison report is not available. To view the latest comparison report, update the catalog file. To update the catalog file, edit the update source and save it, or delete and re-create an update source.

NOTE: In SCCM, even after refreshing the inventory information, server details such as **Driver Pack Version**, and **Drivers Available For** operating system, are not updated in **Dell Out of Band Controllers** (OOB) properties page. To update the OOB properties, synchronize OMIMSSC with the enrolled SCCM.

NOTE: When you upgrade OMIMSSC, information about servers that are discovered in prior versions are not displayed. For the latest server information and correct comparison report, rediscover the servers.

To refresh and view firmware inventory of discovered devices:

1. In **OMIMSSC**, click **Maintenance Center**.
   The **Maintenance Center** page is displayed with a comparison report for all the devices that are discovered in OMIMSSC against the selected update source.
2. (Optional) To view a comparison report only for specific group of devices, select only the required devices.
3. (Optional) To view a comparison report, for another update source, change the update source by selecting an update source from **Select Update Source** drop-down list.
4. To view firmware information of device components such as current version, baseline version, and the update actions that are recommended by Dell EMC, expand the server group from **Device Group/Servers** to the server level, and then to the component level. Also, view the number of recommended updates for devices. Hover your cursor on the available updates icon to see the corresponding details of updates, such as number of critical updates, recommended updates.

The available updates icon indicator color is based on overall criticality of the updates and following are the critical update categories:

- The color is red even if there is a single critical update in the server or server group.
- The color is yellow if there are no critical updates.
- The color is green if the firmware versions are up-to-date.

Following update actions are suggested after populating the comparison report:

- Downgrade—an earlier version is available, and you can downgrade the existing firmware to this version.
- No Action Required—existing firmware is same as the one in update source.
- No Update Available—updates are not available for this component.

  > **NOTE:** There are no updates available for Power Supply Unit (PSU) components for MX7000 Modular Systems and servers in online catalogs. In case you want to update the PSU component for MX7000 Modular System, see *Updating Power Supply Unit component for Dell EMC PowerEdge MX7000 devices*. For updating PSU component for servers, contact Dell EMC support.
- Upgrade - Optional—updates are optional, and they consist of new features or any specific configuration upgrades.
- Upgrade - Urgent—updates are critical, and used for resolving security, performance, or break-fix situations in components such as BIOS.
- Upgrade - Recommended—updates are issue fixes, or any feature enhancements for components. Also, compatibility fixes with other firmware updates are included.

Applying filters

Apply filters to view selected information in the comparison report.

Filter the comparison report based on available server components. OMIMSSC supports three categories of filters:

- **Nature Of Update**—select to filter and view only the selected type of updates on servers.
- **Component Type** —select to filter and view only the selected components on servers.
- **Server Model** —select to filter and view only the selected server models.

> **NOTE:** You cannot export and import server profiles if the filters are applied.

To apply the filters:

In OMIMSSC, click **Maintenance Center**, click the filters drop-down menu, and then select the filters.

Removing filters

To remove filters:

In OMIMSSC, click **Maintenance Center**, and then click **Clear Filters**, or clear the selected check boxes.

Upgrading and downgrading firmware versions using run update method

Before applying updates on devices, ensure that the following conditions are met:

- An update source is available.

  > **NOTE:** Select Storage Spaces Direct update source or MX7000 update sources, for applying firmware updates on Storage Spaces Direct clusters or MX7000 Modular Systems since, these update sources see a modified reference to catalog that contains recommended firmware versions of components for Storage Spaces Direct clusters and Modular Systems.
- iDRAC or Management Module (MM) job queue is cleared before applying the updates, on the managed devices.

Apply updates on selected device groups which are hardware compatible with OMIMSSC. Updates can be applied immediately, or scheduled. The jobs that are created for firmware updates are listed under the **Jobs and Logs Center** page.

Consider the following points before upgrading or downgrading firmware:

- When you start this task, the task takes considerable time based on the number of devices and device components present.

- You can apply firmware updates on a single component of a device, or to the entire environment.
- If there are no applicable upgrades or downgrades for a device, performing a firmware update on the devices cause no action on the devices.
- For updating chassis, see *Updating CMC firmware* section in *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide*.
  - For updating chassis firmware in VRTX, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide*.
  - For updating chassis firmware in FX2, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide*.

1. In OMIMSSC, click **Maintenance Center**, select the servers or Modular System groups, and an update source, and then click **Run Update**.
2. In **Update Details**, provide the firmware update job name and description.
3. To enable downgrading the firmware versions, select the **Allow Downgrade** check-box.

   If this option is not selected, and then there is no action on the component that requires a firmware downgrade.
4. In **Schedule Update**, select one of the following:
   - **Run Now**—select to apply the updates immediately.
   - Select a date and time to schedule a firmware update in future.
5. Select any one of the following methods, and click **Finish**.
   - **Agent-free staged updates**—updates that are applicable without a system restart are applied immediately, and the updates that require a restart are applied when the system restarts. To check if all the updates are applied, refresh the inventory. The entire update job fails, if the operation fails on even one device.
   - **Agent-free updates**—updates are applied and the system restarts immediately.

     NOTE: OMIMSSC supports only **Agent-free updates** for MX7000 Modular Systems.

   NOTE: Cluster-Aware Updating (CAU)—automates the update process by using Windows CAU feature on cluster update groups to maintain server's availability. Updates are passed to cluster update coordinator that is present on the same system where the SCVMM server is installed. The update process is automated to maintain server's availability. The update job is submitted to Microsoft Cluster-Aware-Update (CAU) feature, irrespective of the selection made from the **Update Method** drop-down menu. For more information, see Updates using CAU.

   NOTE: After submitting a firmware update job to iDRAC, OMIMSSC interacts with iDRAC for the status of the job and displays it in the **Jobs and Logs** page in the OMIMSSC Admin Portal. If there is no response from iDRAC about the status of the job for a long time, and then the status of the job is marked as failed.

Updates using CAU

Updates on servers (that are part of cluster) happen through cluster update coordinator which is present on the same system where SCVMM server is installed. The updates are not staged and are applied immediately. Using Cluster Aware Update (CAU), you can minimize any disruption or server downtime enabling continuous availability of the workload. Hence, there is no impact to the service provided by the cluster group. For more information about CAU, see Cluster-Aware Updating Overview section at `technet.microsoft.com`.

Before applying the updates on cluster update groups, verify the following:

- Ensure that the enrolled user has administrator privileges for updating clusters through CAU feature.
- Connectivity to selected update source.
- Availability of failover clusters.
- Check for cluster update readiness and ensure that there are no major errors and warnings in the Cluster Readiness report for applying the CAU method. For more information about CAU, see Requirements and Best Practices for Cluster—aware Updating section at `Technet.microsoft.com`.
- Ensure that Windows Server 2012 or Windows Server 2012 R2 or Windows 2016 or Windows 2019 operating system is installed on all failover cluster nodes to support the CAU feature.
- Configuration of automatic updates is not enabled to automatically install updates on any failover cluster node.
- Enable firewall rule that enables remote shutdown on each node in the failover cluster.
- Ensure that the cluster group has minimum of two nodes.

NOTE:

- For information about applying the updates, see Upgrading and downgrading firmware versions using run update method .

- For information about Dell EMC Repository Manager to download firmware and driver updates, go to *Firmware and Driver update catalog for Dell EMC Solutions for Microsoft Azure Stack HCI* page in `dell.com\support` and download the catalog file.

20

Managing devices in OMIMSSC

Maintain servers and Modular Systems up-to-date by scheduling jobs for upgrading firmware for server and Modular Systems components. Manage servers by recovering servers to an earlier state by exporting its earlier configuration, applying the configurations of the old component on replaced component, and exporting LC logs for troubleshooting.

Topics:

Server recovery

Save a server's configurations in protection vault by exporting a server's configurations to a profile and importing the profile on same server to reinstate it to an earlier state.

Protection vault

Protection vault is a secure location where you can save server profiles. Export server profile from a server or a group of servers and import them to same server or group of servers. You can save this server profile on a shared location in the network by creating an external vault or on a vFlash Secure Digital (SD) card by creating an internal vault. You can associate a server or a group of servers with only one protection vault. However, you can associate one protection vault with many servers or group of servers. You can save a server profile on only one protection vault. However, you can save any number of server profiles on a single protection vault.

Creating protection vault

Ensure that vault location is accessible.

1. In **OMIMSSC**, click **Maintenance Center**, and then click **Maintenance Settings**.
2. In **Maintenance Center**, click **Protection Vault**, and then click **Create**.
3. Select a type of protection vault you want to use and provide the details.
   - If you are creating a protection vault of type **Network Share**, provide a location to save the profiles, credentials to access this location and a passphrase to secure the profile.

     NOTE: This type of protection vault provides support file sharing of type Common Internet File System (CIFS).
   - If you are creating a protection vault of type **vFlash**, provide the passphrase to secure the profile.

Modifying protection vault

You cannot modify the name, description, type of protection vault, and passphrase.

1. In **OMIMSSC**, click **Maintenance Center** > **Maintenance Settings** > **Protection Vault**.
2. To modify the vault, select the vault and click **Edit**.

   NOTE: If the protection vault is modified while the server profile export or import jobs are in progress, the edited information will be considered for the pending sub tasks in the job.

Deleting protection vault

You cannot delete a protection vault in the following circumstances:

- The protection vault is associated with a server or a group of servers.

  To delete such a protection vault, delete the server or group of servers, and then delete the protection vault.

- There is a scheduled job associated with the protection vault. However, to delete such a protection vault, delete the scheduled job, and then delete the protection vault.

1. In **OMIMSSC**, click **Maintenance Center** > **Maintenance Settings** > **Protection Vault**.
2. Select the vault to delete and click **Delete**.

Exporting server profiles

Export a server profile including the installed firmware images on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and the configuration of those components. OMIMSSC Appliance creates a file containing all the configurations, which you can save on a vFlash SD card or network share. Select a protection vault of your choice to save this file. You can export the configuration profiles of a server or a group of servers immediately or schedule it for later. Also, you can select a relevant recurrence option as to how frequently the server profiles have to be exported.

Disable the **F1/F2 Prompt on Error** option in **BIOS Settings**.

Consider the following before exporting server profiles:

- At an instance, you can schedule only one export configuration job for a group of servers.
- You cannot perform any other activity on that server or group of servers whose configuration profiles are being exported.
- Ensure that the **Automatic Backup** job in iDRAC is not scheduled at the same time.
- You cannot export server profiles if the filters are applied. To export server profiles, clear all the applied filters.
- To export server profiles, ensure that you have the iDRAC Enterprise license.
- Before exporting server profile, ensure that the IP address of the server is not changed. If the server IP has changed due to any other operation, then rediscover this server in OMIMSSC, and then schedule the export server profile job.

1. In OMIMSSC, click **Maintenance Center**. Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
   The **Export Server Profile** page is displayed.
2. In the **Export Server Profile** page, provide the job details, and then select a protection vault.

   For more information about protection vaults, see Creation of protection vault.

   In **Schedule Export Server Profile** select one of the following:

   - **Run Now**—export the server configuration immediately of the selected servers, or group of servers.
   - Schedule—provide a schedule to export the server configuration of the selected group of servers.
     - **Never**—select to export the server profile only once during the scheduled time.
     - **Once a week**—select to export the server profile on a weekly basis.
     - **Once every 2 weeks**—select to export the server profile once every two weeks.
     - **Once every 4 weeks**—select to export the server profile once every four weeks.

Importing server profile

You can import a server profile that was previously exported for that same server, or group of servers. Importing server profile is useful in restoring the configuration and firmware of a server to a state stored in the profile.

You can import server profiles in two ways:

- Quick import server profile—allows you to automatically import the latest exported server profile for that server. You need not select individual server profiles for each of the servers for this operation.
- Custom import server profile—allows you to import server profiles for each of the individually selected servers. For example, if exporting server profile is scheduled, and the server profile is exported every day, this feature allows you to select a specific server profile that is imported from the list of server profiles available in the protection vault of that server.

Import server profile notes:

- You can import a server profile from a list of exported server profiles for that server only. You cannot import the same server profiles for different servers or server groups. If you try to import server profile of another server or server group, the import server profile job fails.

- If a server profile image is not available for a particular server or group of servers, and an import server profile job is attempted for that particular server or group of servers, the import server profile job fails for those particular servers that do that have server profile. A log message is added in the Activity logs with the details of the failure.
- After exporting a server profile, if any component is removed from the server, and then an import profile job is started, all the components information are restored except the missing component information is skipped. This information is not available in the activity log of OMIMSSC. To know more about the missing components, see iDRAC's **LifeCycle Log**.
- You cannot import a server profile after applying the filters. To import server profiles, clear all the applied filters.
- To import server profiles, you must have the iDRAC Enterprise license.

1. In OMIMSSC, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.
   The **Import Server Profile** page is displayed.
2. Provide the details, select the **Import Server Profile Type** you want.

   ⓘ **NOTE:** A server profile is exported along with the existing RAID configuration. However, you can import the server profile including or excluding the RAID configuration on the server or group of servers. **Preserve Data** is selected by default and preserves the existing RAID configuration in the server. Clear the check box if you want to apply the RAID settings stored in the server profile.

3. To import the server profile, click **Finish**.

Applying firmware and configuration settings on replaced component

The part replacement feature automatically updates a replaced server component to the required firmware version or the configuration of the old component, or both. The update occurs automatically when you reboot the server after replacing the component.

To set the configurations for part replacement:

1. In OMIMSSC, click **Maintenance Center**, select the servers or group of servers, and then click **Part Replacement**.

   ⓘ **NOTE:** The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

   The **Part Replacement Configuration** window is displayed.
2. You can set **CSIOR**, **Part Firmware Update**, and **Part Configuration Update**, to any of the following options, and then click **Finish**:
   - Collect System Inventory On Restart (CSIOR)—collects all the component information on every system restart.
     - **Enabled**—the software and hardware inventory information of the server components are automatically updated during every system restart.
     - **Disabled**—the software and hardware inventory information of the server components are not updated.
     - **Do not change the value on the server**—the existing server configuration is retained.
   - Part firmware update—restores, or upgrades, or downgrades the component firmware version based on the selection made.
     - **Disabled**—the part firmware update is disabled and the same is applied on the replaced component.
     - **Allow version upgrade only**—the upgraded firmware versions are applied on the replaced component, if the firmware version of the new component is earlier than the existing version.
     - **Match firmware of replaced part**—the firmware version on the new component is matched to the firmware version of the original component.
     - **Do not change the value on the server**—the existing configuration of the component is retained.
   - Part configuration update—restores or upgrades the component configuration based on the selection made.
     - **Disabled**—the part configuration update is disabled and the saved configuration of the old component is not applied on the replaced component.
     - **Apply always**—the part configuration update is enabled and the saved configuration of the old component is applied on the replaced component.
     - **Apply only if firmware matches**—the saved configuration of the old component is applied on the replaced component, only if their firmware versions match.
     - **Do not change the value on the server**—the existing configuration is retained.

Collecting LC logs for servers

LC logs provide records of past activities in a managed server. These log files are useful for server administrators since they provide detailed information about recommended actions and some other technical information that is useful for troubleshooting purpose.

The various types of information available in LC logs are alerts-related, configuration changes on the system hardware components, firmware changes due to an upgrade or downgrade, replaced parts, temperature warnings, detailed timestamps of when the activity has started, severity of the activity, and so on.

The exported LC log file is saved in a folder and the folder is named after the server's service tag. LC logs are saved in the format: `<YYYYMMDDHHMMSSSSS>.<file format>`. For example, `201607201030010597.xml.gz` is the LC file name, which includes the date and time of the file when it was created.

There are two options to collect LC logs:

- Complete LC logs—exports active and archived LC log files. They are large in size, and hence compressed to `.gz` format and exported to the specified location on a CIFS network share.
- Active LC logs—exports recent LC log files immediately or schedule a job to export the log files at regular intervals. View, search, and export these log files to OMIMSSC Appliance. In addition, you can save a backup of log files in a network share.

To collect LC logs, perform the following steps:

1. In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and then click **Collect LC Logs**.
2. In **LC Log Collection**, select one of the following options, and click **Finish**:
   - **Export Complete LC Logs (.gz)**—select to export complete LC logs to a CIFS network share by providing Windows credentials.
   - **Export Active Logs (Run now)**—select to export the active logs immediately to OMIMSSC Appliance.
     - (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.
   - **Schedule LC Log Collection**—select select to export the active logs at regular intervals.

     In **Schedule LC Log Collection**, select a date and time to export the log files.

     Select a radio button depending on how frequently the files have to be exported. The available options for scheduling frequency to determine how often you want to collect the LC logs are:

     - **Never**—this option is selected by default. Select to export the LC logs only once at the scheduled time.
     - **Daily**—select to export the LC logs daily at the scheduled time.
     - **Once a week**—select to export the LC logs on a weekly basis at the scheduled time.
     - **Once every 4 weeks**—select to export the LC logs in every four weeks at the scheduled time.
     - (Optional) Select the **Back up LC logs on the network share** check box to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

   NOTE: Provide a share folder with sufficient storage space, since the exported files are large in size.

   To track this job, the **Go to the Job List** option is selected by default.

Viewing LC logs

View all the active LC logs, search for detailed description, and download the logs in CSV format.

Add OMIMSSC Appliance in **Local Intranet site** list as mentioned in *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User Guide*.

1. In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and click **View LC Logs**.
2. All the servers in the selected group and the servers for which LC logs are collected are listed with their LC log files. Click a file name to view all the log entries in the LC log file specific to that server. For more information, see File description.
3. (Optional) Use the search box to search description in all the log files, and export the file in CSV format.

   There are two ways to search message description in an LC file:

   - Click a file name to open the LC log file and search for a description in the search box.
   - Provide a description text in the search box, and then view all the LC files with these instances of text.

ⓘ **NOTE:** If the LC log message description is long, the message is truncated to 80 characters.

ⓘ **NOTE:** The time displayed against the LC log messages follows the iDRAC time zone.

File description

Use this page to view detailed information about recommended actions and some other technical information that are useful for tracking or alert purposes for a particular server.

To view the contents of a file, click a file name:

- You can search for particular message descriptions.
- You can either view the log files in the window or download the file to view additional log messages.
- You can view any comments provided by a user for an activity.

ⓘ **NOTE:** When using the search option, only the search results are exported to CSV file.

ⓘ **NOTE:** If the message is long, the message is truncated to 80 characters.

ⓘ **NOTE:** Click **Message ID** to view more information about the message.

Exporting inventory

Export the inventory of selected servers or a group of server to an XML or CSV format file. You can save this information in a Windows shared directory or on a management system. Use this inventory information to create a reference inventory file in an update source.

Ensure that you set the browser settings as mentioned in *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

ⓘ **NOTE:** You can import the XML file into DRM and create a repository based on the inventory file.

ⓘ **NOTE:** Though you select only the component information of a server and export it, the complete inventory information of the server is exported.

1. In **OMIMSSC**, click **Maintenance Center**.
2. Select the servers for which you want to export the inventory, and select the format from **Export Inventory** drop-down menu.

   The file is exported in CSV or XML format based on the selection. The file consists of details such as server groups, service tag of the server, host name or IP address, device model, component name, current firmware version on that component, firmware version from the update source, and update action on that component.

Cancelling scheduled jobs

Ensure that the job is in **Scheduled** state.

1. In OMIMSSC, do any of the following:
   - In the navigation pane, click **Maintenance Center**, and then click **Manage Jobs**.
   - In the navigation pane, click **Jobs and Log Center**, and then click **Scheduled** tab.
2. Select jobs that you want to cancel, click **Cancel**, and then to confirm, click **Yes**.

21

Provisioning devices from OMIMSSC

This chapter covers high-level details for discovering, deploying operating system, creating clusters, and maintaining Dell EMC devices using OMIMSSC.

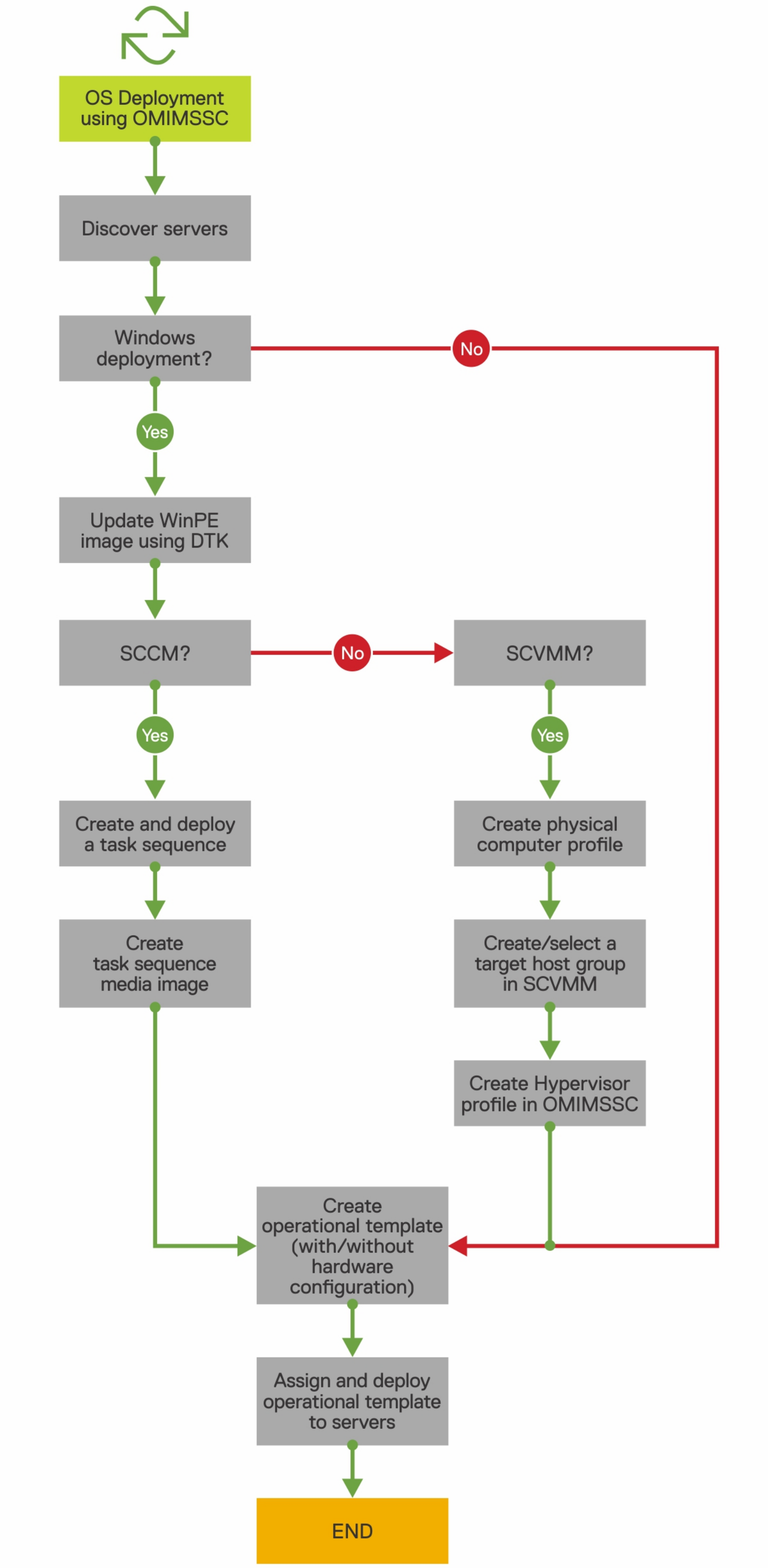
Topics:

Workflow for deployment scenarios

Use OMIMSSC to deploy Windows and non-Windows operating system in SCCM or SCVMM environments using Operational Templates.

NOTE: Ensure that you upgrade the device firmware versions to the latest versions available at `ftp.dell.com` or `downloads.dell.com` before deploying the operating system.

Here is a pictorial representation of the operating system deployment use cases in OMIMSSC.


OS Deployment using OMIMSSC
Discover servers
Windows deployment?
No
Yes
Update WinPE image using DTK
SCCM?
No
SCVMM?
Yes
Yes
Create and deploy a task sequence
Create physical computer profile
Create task sequence media image
Create/select a target host group in SCVMM
Create Hypervisor profile in OMIMSSC
Create operational template (with/without hardware configuration)
Assign and deploy operational template to servers
END

Deploying Windows OS using OMIMSSC console extension for SCCM

To deploy Windows OS through SCCM console using OMIMSSC, perform the following steps:

ⓘ **NOTE:** Before deploying OS on a host server, ensure that in SCCM, the **Client** status of the server is **No**.

1. Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot WIM image. For more information, see the WinPE update.
2. Import this .WIN image into the SCCM console, and create a boot image in SCCM. For more information, see the *Microsoft documentation*.
3. Create a task sequence in SCCM. For more information, see Creating task sequence.
4. Create a task sequence media image in SCCM. For more information, see the *Microsoft documentation*.

   ⓘ **NOTE:** To enable unattended OS deployment when creating task sequence media, in **Select the type of media**, select **Allow unattended operating system deployment** check-box.

5. Discover the reference server by using the **Discovery** page. For more information, see the Discovering servers using manual discovery.
6. Create an Operational Template, by capturing all the details of the discovered server. For more information, see Creating Operational Template from reference servers.
7. Assign an Operational Template on managed device, and check for the template compliance. For more information, see Assigning Operational Template and running Operational Template compliance.
8. Deploy an Operational Template to make the device template compliant. For more information, see Deploying Operational Template.
9. View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see Launching Jobs and Logs Center.

Deploying hypervisor using OMIMSSC console extension for SCVMM

The different scenarios for hypervisor deployment are as follows:

Table 10. Hypervisor deployment scenarios

Condition	Action
If you require the latest factory drivers.	While creating a hypervisor profile, enable Lifecycle Controller (LC) driver injection.
If you want to retain the existing hardware configuration.	While creating the Operational Template, clear the check box for all the components that do not require any changes.

To deploy hypervisor through SCVMM console using OMIMSSC, perform the following steps:

1. Download the latest Dell EMC Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot ISO image. For more information, see the WinPE update.
2. Create a physical computer profile, and a host group in SCVMM. For more information, see the SCVMM documentation.
3. Create a hypervisor profile in the OMIMSSC console extension for SCVMM. For more information, see Creating a hypervisor profile.
4. Discover the reference server by using the Discovery page. For more information, see the Discovering servers using manual discovery.
5. Create an Operational Template, by capturing all the details of the discovered server. For more information, see Creating Operational Template from reference servers.
6. Assign an Operational Template on managed device, and check for the template compliance. For more information, see Assigning Operational Template and running Operational Template compliance.
7. Deploy an Operational Template to make the device template compliant. For more information, see Deploying Operational Template.
8. View the job status for operating system deployment in the Jobs and Logs Center page. For more information, see Launching Jobs and Logs Center.

Redeploying Windows OS using OMIMSSC

To redeploy Windows OS on a server by using OMIMSSC console extension for SCCM or OMIMSSC console extension on SCVMM, perform the following steps:

1. Delete the server from the Microsoft console. For more information, see Microsoft documentation.
2. Rediscover the server or synchronize OMIMSSC with the registered Microsoft console. The server is added as an unassigned server in OMIMSSC. For more information about discovery, see Discovering servers using manual discovery. For more information about synchronization, see Synchronizing with enrolled Microsoft console.
3. Create an Operational Template, by capturing all the details of the discovered server. For more information, see Creating Operational Template from reference servers.
4. Assign an Operational Template on managed device, and check for the template compliance. For more information, see Assigning Operational Template and running Operational Template compliance.
5. Deploy an Operational Template to make the device template compliant. For more information, see Deploying Operational Template.
6. View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see Launching Jobs and Logs Center.

Deploying non-windows OS using OMIMSSC console extensions

To deploy non-windows OS using OMIMSSC, perform the following steps:

NOTE: Steps to deploy non-windows OS through OMIMSSC is common in both the Microsoft consoles.

1. Discover the reference server by using the **Discovery** page. For more information, see the Discovering servers using manual discovery.
2. Create an Operational Template, by capturing all the details of the discovered server. For more information, see Creating Operational Template from reference servers.
3. Assign an Operational Template on managed device, and check for the template compliance. For more information, see Assigning Operational Template and running Operational Template compliance.
4. Deploy an Operational Template to make the device template compliant. For more information, see Deploying Operational Template.

   NOTE: If the DHCP lookup fails while deployment, then the server times out and the server is not moved into **Managed Lifecycle Controller Lifecycle Controller (ESXi)** collection in SCCM.

Creating Storage Spaces Direct clusters by using predefined Operational Templates

To create clusters by using OMIMSSC, perform the following steps:

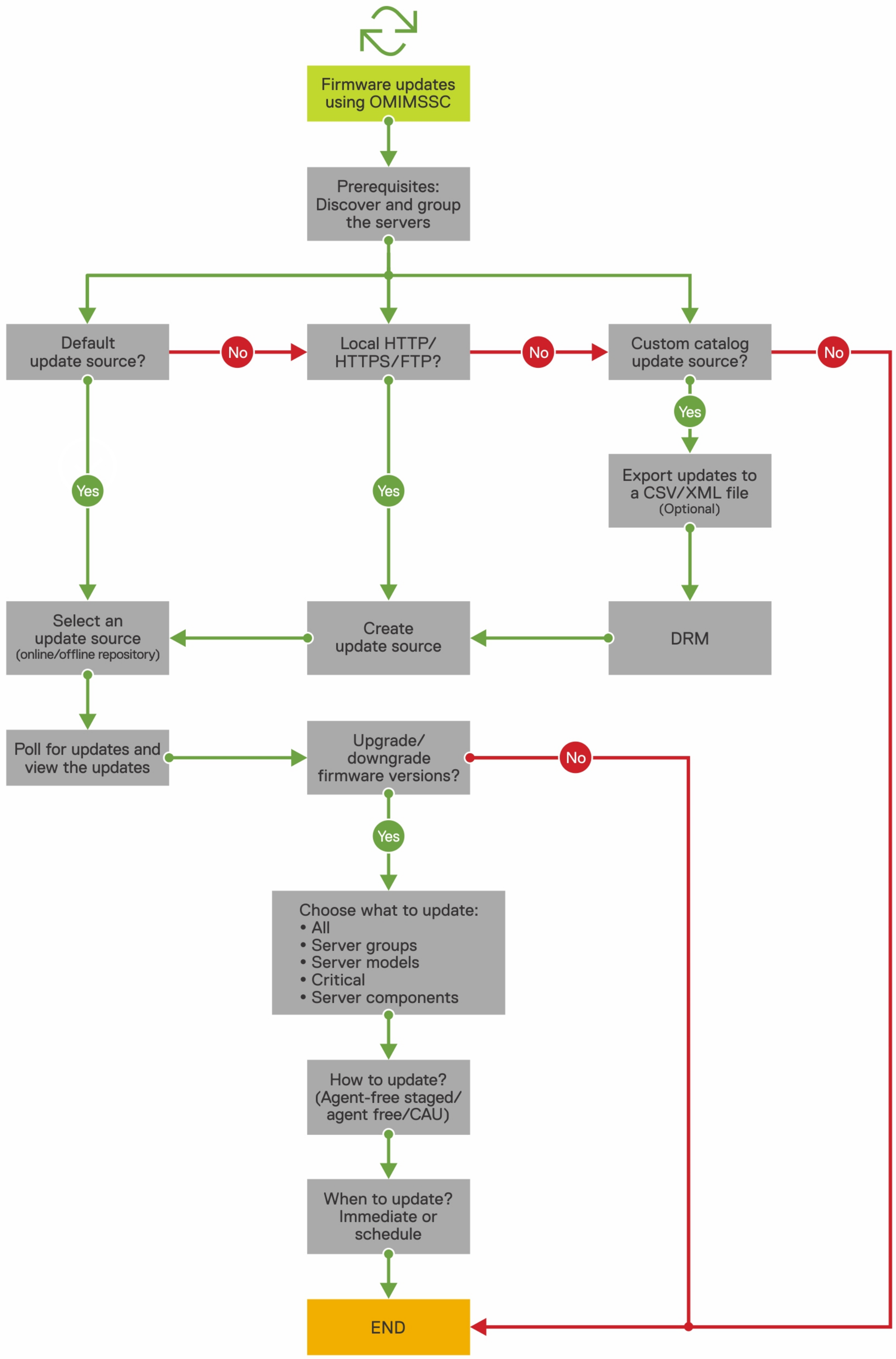
1. Discover the reference server by using the **Discovery** page. For more information, see the Discovering servers using manual discovery.
2. Edit the predefined Operational Template. For more information, see Modifying Operational Template.
3. Create a logical switch. For more information, see Creating logical switch.
4. Create Storage Spaces Direct cluster. For more information, see Creating Storage Spaces Direct clusters.

Workflow for maintaining devices

Maintain the discovered devices in OMIMSSC.

Updating the firmware of servers and MX7000 devices

Here is a pictorial representation of the firmware update workflow.


Firmware updates using OMIMSSC
Prerequisites: Discover and group the servers
Default update source?
No
Local HTTP/ HTTPS/FTP?
No
Custom catalog update source?
No
Yes
Yes
Yes
Export updates to a CSV/XML file (Optional)
Select an update source (online/offline repository)
Create update source
DRM
Poll for updates and view the updates
Upgrade/ downgrade firmware versions?
No
Yes
Choose what to update:
• All
• Server groups
• Server models
• Critical
• Server components
How to update? (Agent-free staged/ agent free/CAU)
When to update? Immediate or schedule
END

You can update the selected devices by using the following update sources:

- Online FTP or local FTP source
- Online HTTP or local HTTP source
- Online HTTPS or local HTTPS source
- Local Dell Repository Manager (DRM) source

1. Create or select a default update source. For more information about update source, see Update source.

> **NOTE:** Ensure that you update the update source with the latest catalog by using the polling and notification feature. For more information about polling and notification, see Polling and notification.

If you are updating Storage Spaces Direct clusters, select a predefined update source specific for Storage Spaces Direct clusters. These update sources are displayed only in the **Maintenance Center** page.

If you are updating MX7000 devices, select a predefined update source specific for Modular Systems. These update sources are displayed only in **Maintenance Center** page.

2. Create or select the default update groups. For more information about update groups, see Update groups.
3. Discover or synchronize the devices with a registered Microsoft console, and ensure that the device inventory is up-to-date. For more information about discovery and synchronization, see Device discovery and synchronization . For more information about server inventory, see Launching server view.
4. Update the device by using one of the following options:
   - Select the required devices, and click **Run Update**. For more information, see Upgrading or downgrading firmware versions using run update method.

     > **NOTE:** To downgrade the firmware of device components, select the **Allow Downgrade** check-box. If this option is not selected, there is no action on the component that requires a firmware downgrade.
   - Select the firmware update component in Operational Template and deploy this template. For more information about Operational Template, see Operational Template.

Configuring replaced components

To match the firmware version, or the configuration settings of the replaced component to that of the old component, see Applying firmware and configuration settings.

Exporting and importing server profiles

Export the server profile at a particular instance, and then import the profile to reinstate the server:

1. Create a protection vault. For more information about creating protection vault, see Creating protection vault.
2. Export a server profile. For more information about exporting server profile, see Exporting server profile.
3. Import server profile to the same server from which it was exported. For more information about importing server profile, see Importing server profile.

   > **NOTE:** You can import the server profile including the RAID configuration only if the RAID configuration is exported to the profile.

22

Configuration and deployment

Discover

1. In OMIMSSC console, perform any one of the following steps:
   - In the dashboard, click **Discover Servers**.
   - In the navigation pane, click **Configuration and Deployment**, click **Server View**, and then click **Discover**.
2. Click **Discover**.

To view the changes made, refresh the **Credential Profile** page.

Topics:

Use cases

1. Discover the reference server by using the **Discovery** page. For more information, see the Discovering servers using manual discovery.
2. Create an Operational Template, by capturing all the details of the discovered server. For more information, see Creating Operational Template from reference servers.
3. Assign an Operational Template on managed device, and check for the template compliance. For more information, see Assigning Operational Template and running Operational Template compliance.
4. Deploy an Operational Template to make the device template compliant. For more information, see Deploying Operational Template.
5. View the job status for operating system deployment in the **Jobs and Logs Center** page. For more information, see Launching Jobs and Logs Center.

Creating Operational Templates

Before creating Operational Template, ensure that you complete the following tasks:

- Discover a reference server by using the **Discovery** feature. For information about discovering servers, see Discovering servers using manual discovery.
- Discover a Modular System by using the **Discovery** feature. For information about discovering Modular Systems, see Discovering Modular System using manual discovery.
- If you are not using the default update source, and then create an update source. For more information, see Creating update source.
- For SCCM users:
    - Create a task sequence. For more information, see Creating task sequence.
    - For non-Windows operating system deployment, have a device type credential profile. For more information, see Creating credential profile.
- For SCVMM users:
    - Create a hypervisor profile. For information about creating hypervisor profile, see Creating hypervisor profile.
    - For Windows deployment, have a device type credential profile. For more information, see Creating credential profile.

1. In OMIMSSC, do any of the following to open an Operational Template:
    - In the OMIMSSC dashboard, click **Create Operational Template**.
    - In the navigation pane, click **Profiles** > **Operational Template**, and then click **Create**.

    The **Operational Template** wizard is displayed.
2. Click **Create**.
    The **Operational Template** wizard is displayed.
3. Enter a name and description for the template.
4. Select the type of device, and enter the IP address of reference device, and then click **Next**.

    NOTE: You can capture the configuration of reference server with iDRAC 2.0 and later.
5. In **Device Components**, click a component to view the available attributes and their values.

    The components are as follows:
    - Firmware update
    - Hardware components, which are RAID, NIC, and BIOS.

        NOTE: In **iDRAC Embedded 1** component, following are the privileges and their values for **User Admin Privilege** attribute.

        Table 11. Privilege value table

Value	Privilege
1	Login
2	Configure
4	Configure Users
8	Logs
16	System Control
32	Access Virtual Console
64	Access Virtual Media
128	System Operations
256	Debug
499	Operator Privileges

    - Operating system—select either Windows, or ESXi, or RHEL.
6. Use the horizontal scroll bar to locate a component. Select the component, expand a group, and then edit its attribute values. Use the vertical scroll bar to edit a groups and attributes of a component.
7. Select the check box against each component, because, the configurations of selected components are applied on the managed device, when the Operational Template is applied. However, all the configurations from the reference device are captured and saved in the template.

NOTE: Irrespective of the selection made in the check box against each component, all the configurations are captured in the template.

In **Operating System** component, perform the steps in either of the following options, as per your requirement:

- For Windows operating system deployment on SCCM, see Windows component for the OMIMSSC console extension for SCCM.
- For Windows operating system deployment on SCVMM, see Windows component for the OMIMSSC console extension for SCVMM.
- OMIMSSC
- For non-Windows operating system deployment, see Non-Windows component for the OMIMSSC console extensions.

8. To save the profile, click **Finish**.

Installer folders

The following folders are created after installing the console extension:

- Log—this folder consists of console-related log information.

NOTE: If the credentials for domain administrator account and local administrator account are different, do not use domain administrator account to log in to SCCM or SCVMM. Instead use a different domain user account to log in to SCCM or SCVMM.

Assign Operational Templates

1. In OMIMSSC click **Configuration and Deployment**, and then click **Server View**. Select the required servers and click **Assign Operational Template and Run Compliance**.

   The **Assign Operational Template and Run Compliance** page is displayed.
2. Select the required servers and click **Assign Operational Template and Run Compliance**.
3. In OMIMSSC click **Configuration and Deployment**, and click **Modular Systems View**. Select the required Modular System and click **Assign Operational Template** .

   The **Assign Operational Template** page is displayed.
4. Select the required Modular Systems, and click **Assign Operational Template and Run Compliance**.

   The **Assign Operational Template** page is displayed.
5. Select the template from **Operational Template** drop-down menu, enter a job name, and then click **Assign**.

   The Operational Template drop-down lists templates, of the same type as that of the devices selected in the previous step.

   If the device is compliant to the template, and then a **green** color box with a check mark is displayed.

   If the Operational Template is not applied successfully on the device or the hardware component in Operational Template is not selected, and then an **information** symbol box is displayed.

   If the device is noncompliant to the template, and then a **warning** symbol box is displayed. Only if the device is noncompliant to assigned Operational Template, you can view a summary report by clicking the template name link. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and device.

   To view a detailed report, perform the following steps:

   a. Click **View Detailed Compliance**. Here, the components with attribute values different from those of the assigned template are displayed. The colors indicate the different states of Operational Template compliance.

      - Yellow color warning symbol—non-compliance. represents that the configuration of the device does not match with the template values.
      - Red color box—represents that the component is not present on the device.

Deploy Operational Templates

ⓘ **NOTE:** Ensure that you do not enable attributes that change the credentials to log in to the device after deploying the Operational Template.

1. In OMIMSSC, click **Configuration and Deployment**, and click **Server View**. Select the servers on which you have applied the template, and then click **Deploy Operational Template**.
   The **Deploy Operational Template** page is displayed.
2. In OMIMSSC, click **Configuration and Deployment**, and click **Modular Systems View**. Select the Modular System on which you have assigned the template, and then click **Deploy Operational Template**.
   The **Deploy Operational Template** page is displayed.
3. (Optional) To export all the attributes that are marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 4.

   ⓘ **NOTE:** Before exporting the pool values, add the IP address of the OMIMSSC Appliance where the OMIMSSC console extension is installed, to the local intranet site. For more information about adding the IP address in IE browser, see *Browser settings* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User Guide*.

4. If you have exported the pool values, enter values for all the attributes that are marked as pool values in the .CSV file and save the file. In **Attribute Value Pool**, select this file to import it.

   The format of a .CSV file is `attribute-value-pool.csv`

   ⓘ **NOTE:** Ensure that you select a .CSV file which has all proper attributes and the iDRAC IP or iDRAC credentials do not change due to the template, since the job is not tracked by OMIMSSC after the iDRAC IP or iDRAC credentials changes and is marked as failed though the job may be successful in iDRAC.

5. Enter a unique job name, description for the job, and click **Deploy**.

   To track this job, the **Go to the Job List** option is selected by default.

Windows OS component for the OMIMSSC console extension for SCCM

1. Select a task sequence and deployment method.

   ⓘ **NOTE:** Only the task sequences deployed on collections are listed in the drop-down menu.

   For information about task sequence, see Task sequence.

2. Select one of the following options for the **Deployment method**:
   - **Boot to network ISO**—reboots specified ISO.
   - **Stage ISO to vFlash and Reboot**—downloads the ISO to vFlash and reboots.
   - **Reboot to vFlash**—reboots to vFlash. Ensure that the ISO is present in the vFlash.

     ⓘ **NOTE:** To use the **Reboot to vFlash** option, the label name of the partition that is created on vFlash must be **ISOIMG**.
3. (Optional) To use the image present in the network share, select the **Use Network ISO as Fallback** option.
4. enter an LC boot media image file.
5. Select the drivers required for the operating system.

Windows component for the OMIMSSC console extension for SCVMM

Select **Hypervisor Profile**, **Credential Profile**, and **Server IP from**.

ⓘ **NOTE: Host Name**, and **Server Management NIC** are always pool values. For server management NIC, provide the MAC address of the network port through which you want the operating system to communicate to SCVMM.

If you select **Server IP from** as **Static**, and then ensure that you have configured the logical network in SCVMM, and the following fields are pool values:

- **Console Logical Network**
- **IP Subnet**
- **Static IP Address**

Non-Windows component for the OMIMSSC console extension for SCCM/SCVMM

Select a non-windows operating system, operating system version, type of share folder, ISO file name, location of the ISO file and the password for the root account of the operating system.

(Optional) Select a Windows type credential profile for accessing the CIFS share.

Host name is a pool value and if you disable DHCP option, and then the following fields are pool values:

- **IP Address**
- **Subnet Mask**
- **Default Gateway**
- **Primary DNS**
- **Secondary DNS**

ⓘ **NOTE:** Network File System (NFS) and Common Internet File System (CIFS) share types are supported for non-Windows operating system deployment.

Discovery in enrolled MSSC

After discovery, the server is added to the **Hosts** tab or the **Unassigned** tab. Also, the discovered server is marked as compliant or noncompliant when it contains minimum versions of LC firmware, iDRAC, and BIOS that are required to work with OMIMSSC.

- When discover a PowerEdge server with an operating system on it and already be present in SCCM or SCVMM console, and then the server is listed as a host server under the **Hosts** tab in the OMIMSSC console where the discovery job is initiated.
  - If the host is a modular server, and then the service tag of the Modular System containing the server is also displayed.
  - If the host is part of a cluster, and then the Fully Qualified Domain Name (FQDN) of the cluster is displayed.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, and then the server is listed as an unassigned server under the **Unassigned** tab in all the enrolled OMIMSSC consoles.
- A license is consumed after discovering a server. The **Licensed Nodes** count decreases as the number of licenses are discovered.

Importing server profile

1. In OMIMSSC, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.
   The **Import Server Profile** page is displayed.
2. Select the servers' whose profiles you want to import, and click **Import** from **Device Profile** drop-down menu.
   The **Import Server Profile** page is displayed.

Export server profile

1. In OMIMSSC, click **Maintenance Center**. Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
   The **Export Server Profile** page is displayed.

2. Select the servers' whose profiles you want to export, and click **Export** from **Device Profile** from drop-down menu.
   The **Export Server Profile** page is displayed.

Viewing LC logs

1. In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and click **View LC Logs**.
2. Select the servers' whose logs you want to view, click **LC Logs** drop-down menu, and then click **View LC Logs**.

Collect LC logs

1. In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, click **LC Logs** drop-down menu and then click **Collect LC Logs**.
2. Select the servers' whose logs you want to export, and then click **LC Logs** drop-down menu and then click **Collect LC Logs**.

Part replacement

1. In OMIMSSC, click **Maintenance Center**, select the servers or group of servers, and then click **Part Replacement**.

   NOTE: The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

   The **Part Replacement Configuration** window is displayed.
2. Select the servers' whose component you want to configure, and then click **Part Replacement**.

   NOTE: The option name expands to **Configure Part Replacement** when you hover over to **Part Replacement**.

   The **Part Replacement Configuration** window is displayed.

Polling and notification

1. In OMIMSSC, click **Maintenance Center**, and then click **Polling and Notification**.
2. Click **Polling and Notification**.

Launch iDRAC

1. In OMIMSSC, expand **Configuration and Deployment**, and select one of the following:
   - Click **Server View**. Based on the server (if it is a host or an unassigned server), click **Unassigned Servers** or **Hosts** tab, and click the **iDRAC IP** address of the server.

     The **Unassigned Servers** tab is displayed by default.

     To view the hosts tab, click **Hosts**.
   - Click **Cluster View**. Expand the cluster type and expand cluster group to server level.

     The **Server** tab is displayed.
2. To launch iDRAC console, click **IP address**.
3. To launch iDRAC console, click **IP address**.

Launch Input Output Module

To launch Input Output Module console, perform the following steps:

1. In OMIMSSC, expand **Configuration and Deployment**, click **Modular Systems View**. Expand the model to individual devices level.

   All devices under that model are displayed.
2. Click **I/O Modules** tab.
3. Click **IP address** of the device.

Resolving synchronization errors

1. In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Resolve Sync Errors**.
2. Click **Resolve Sync Errors**.

Synchronizing OMIMSSC with enrolled Microsoft console

1. In OMIMSSC, click **Configuration and Deployment**, click **Server View**, and then click **Synchronize with OMIMSSC** to synchronize all the hosts that are listed in enrolled MSSC with the OMIMSSC Appliance.
2. To synchronize all the hosts that are listed in the enrolled MSSC with Appliance, click **Synchronize with OMIMSSC**.

   Synchronization is a long running task. View the job status in **Jobs and Logs** page.

Assign and deploy

In OMIMSSC, click **Configuration and Deployment**, and then click **Server View**. Select the servers on which you want to deploy a template on, and then click **Deploy Operational Template**.
The **Deploy Operational Template** page is displayed.

Run update

1. In OMIMSSC, click **Maintenance Center**, select the servers or Modular System groups, and an update source, and then click **Run Update**.
2. Select the servers or Modular System groups, and an update source, and then click **Run Update**.
3. enter a unique job name, description for the job, and click **Create**.

   To track this job, the **Go to the Job List** option is selected by default.

Deploy Azure Stack HCI cluster

1. Create the required Windows and device credential profiles.
2. Create WinPE image
   a. Install the WDS feature on SCVMM, and then configure it.
   b. Add PXE server in SCVMM server using add resources and specify the same server name (SCVVM hostname) PXE server.
   c. Create the shared folder within SCVMM server and then copy Boot.wim from *C:\RemoteInstall\DCMgr\Boot\Windows\Images* to a share folder.
   d. Download Dell EMC OpenManage deployment toolkit and extract the file in a shared folder created. For example, *\\Servername\sharefolder\DTK\DTK501*.
   e. Create a WinPE image.
   f. Ensure that the WinPE image is placed in a shared folder in SCVMM.
3. Add Windows Server 2016 and 2019 VM template to the in SCVMM library. For more information see, Microsoft documentation.
   a. Change the following properties:

- Operating system : Windows Server 2016 and 2019 datacenter
- Virtualization platform: Microsoft Hyper-V

  ⓘ **NOTE:** To create a windows server 2019 virtual disk(.vhdx) using .iso file for the OS deployment, see https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f

4. Create physical computer profile (PCP) in SCVMM. In the hardware configuration > disk and partitions, select partition scheme as **GUID Partition Table**. For more information, see Create a physical computer profile section in pre-requisites section of Microsoft documentation on provisioning a Hyper-V host or cluster from bare-metal computers.
5. Create a host group in SCVMM to host Azure Stack HCI cluster. For information about creating host groups in SCVMM, see Microsoft documentation.
6. Create Hypervisor profile.
7. Discover the servers in Dell EMC OpenManage extension.
8. Configure using predefined Operational Template.
9. (Optional) Check the compliance (configuration and deployment > server view > select the server and assign operational template).
10. Create Logical switch
11. Deploy Azure Stack HCI cluster.
    To verify the successful cluster deployment, go to **Cluster View** to check if the cluster is listed with the respective category.

23

Trouble shooting scenarios

Topics:

Resources required for managing OMIMSSC

Use this guide to check for required privileges and solve any problems encountered in OMIMSSC.

To troubleshoot any issues faced in OMIMSSC, ensure that you have the following resources:

- Read-only user's account details to login to OMIMSSC Appliance and perform various operations.

  For logging in as a read-only user from OMIMSSC Appliance VM, enter user name as `readonly` with the same password used to login to OMIMSSC Appliance VM.

- Log files having high level and complete details of the errors:
  - Activity logs—contains user specific, and high-level information about the jobs initiated in OMIMSSC, and status of jobs run in OMIMSSC. To view activity logs, go to **Jobs and Logs** page in OMIMSSC console extension.
  - Complete logs —contains Administrator-related logs, and multiple detailed logs specific to scenarios in OMIMSSC. To view the complete logs, go to **Jobs and Logs** page in **OMIMSSC Admin portal**, **Settings**, and then **Logs**.
  - LC Logs—contain server level information, detailed error messages on operations performed in OMIMSSC. To download and view the LC Logs, see *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

    NOTE: For troubleshooting individual devices from iDRAC or OpenManage Enterprise Module (OME-Modular) page, launch OMIMSSC, click **Configuration and Deployment** page, launch the respective view, and then click the device IP URL.

NOTE: SCVMM server Administrator user should not be an SCVMM service account.

NOTE: If you are upgrading from SC2012 VMM SP1 to SC2012 VMM R2, then upgrade to Windows PowerShell 4.0.

Verifying permissions for using OMIMSSC console extension for SCCM

After installing OMIMSSC, verify that the enrolled user has the following permissions:

1. On the system where OMIMSSC is installed, provide the **Write** permissions for the *<Configuration Manager Admin Console Install Dir>\XmlStorage\Extensions\DLCPlugin* folder using PowerShell commands.

   Complete the following prerequisites on the site server, and SMS provider server before installing OMIMSSC component:

   a. In PowerShell, run the command: `PSRemoting`.

If the `PSRemoting` command is disabled, run enable the `PSRemoting` command using the following commands.

   i. Run the command: `Enable-PSRemoting`
   ii. In the confirmation message, type `Y`.

b. In PowerShell, run the command: `Get-ExecutionPolicy`.

   If the policy is not set to `RemoteSigned`, then set it to `RemoteSigned`using the following commands.

   i. Run the command: `Set-ExecutionPolicy RemoteSigned`.
   ii. In the confirmation message, type `Y`.

2. Configure user access to Windows Management Instrumentation (WMI). For more information, see the Configuring user access to WMI.
3. Provide share and folder permissions to write files to the inboxes folder.

   To grant share and folder permissions to write files to the DDR inbox:

   a. From the Configuration Manager console, under **Administration**, grant the user permission to write to the **SMS_<sitecode>** share.
   b. Using **File Explorer**, go to the share location **SMS_<sitecode>** share, and then to the `ddm.box` folder. Grant full control to the domain user for the following folders:
      - **SMS_<sitecode>**
      - Inboxes
      - `ddm.box`

Configuring user access to WMI

To configure user access to WMI remotely:

NOTE: Make sure that firewall of the system does not block the WMI connection.

1. To access the Distributed Component Object Model (DCOM) remotely, provide permissions to the enrolled SCCM user.

   To grant user permissions for DCOM:

   a. Launch `dcomcnfg.exe`.
   b. From the left pane, in the **Component Services** console, expand **Computers**, right-click **My Computer**, and select **Properties**.
   c. On **COM Security**:
      - From **Access Permissions**, click **Edit Limits** and select **Remote Access**.
      - From **Launch and Activation Permission**, click **Edit Limits** and select **Local Launch**, **Remote Launch**, and **Remote Activation**.
2. To access the DCOM Config Windows Management and Instrumentation (WMI) components, provide user permissions to the enrolled user.

   To grant user permissions for DCOM Config WMI:

   a. Launch `dcomcnfg.exe`.
   b. Expand **My Computer** > **DCOM Config**.
   c. Right-click **Windows Management and Instrumentation**, and select **Properties**.
   d. On **Security**, from **Launch and Activation Permission**, click **Edit** and select the **Remote Launch** and **Remote Activation** permissions.
3. Set the namespace security and grant permissions.

   To set namespace security and grant permissions:

   a. Launch `wmimgmt.msc`
   b. In **WMI Control** pane, right-click **WMI Control**, select **Properties**, and then select **Security**.
   c. Navigate to `ROOT\SMS Namespace`.
   d. Select the **Execute Methods**, **Provider Write**, **Enable Account**, and the **Remote Enable permissions**.
   e. Navigate to `Root\cimv2\OMIMSSC`.
   f. Select the **Execute Methods**, **Provide Write**, **Enable Account**, and the **Remote Enable permissions** .
      Alternatively, the Configuration Manager user becomes a member of the **SMS_Admin** group, and you can grant **Remote Enable** to the existing permissions of the group.

Verifying PowerShell permissions for using OMIMSSC console extension for SCVMM

Check if the **`PSRemoting`** status is enabled and **`ExecutionPolicy`** is set to **`RemoteSigned`**. If the status is different then perform the following steps in PowerShell:

a. In PowerShell, run the command: `PSRemoting`.

   If the `PSRemoting` command is disabled, run enable the `PSRemoting` command using the following commands.

   i. Run the command: `Enable-PSRemoting`

   ii. In the confirmation message, type `Y`.

b. In PowerShell, run the command: `Get-ExecutionPolicy`.

   If the policy is not set to `RemoteSigned`, then set it to `RemoteSigned`using the following commands.

   i. Run the command: `Set-ExecutionPolicy RemoteSigned`.

   ii. In the confirmation message, type `Y`.

Install and upgrade scenarios in OMIMSSC

This section has all the troubleshooting information related to installing and upgrading OMIMSSC.

Verifying OMIMSSC Appliance VM configuration

To verify that the OMIMSSC Appliance VM is configured appropriately, select and then right-click the OMIMSSC Appliance VM, click **Settings**, and then perform the following tasks:

1. Check if the allocation of memory for the OMIMSSC Appliance is as per the requirement mentioned in the *Common requirements* section of *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User Guide*. Else provide the memory in **Startup RAM**, and click **Apply**.
2. Check if the processor count is as per the requirement mentioned in the *Common requirements* section of *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User Guide*. Else provide the number of processor counts in **Number of Virtual processors** count under **Processors**.
3. Check if the **Virtual hard disk** field under IDE Controller: **IDE Controller 0** > **Hard Drive** the **Virtual hard disk** referring to the **OMIMSSC—v7** file else, click **Browse** and navigate to the location where the VHD file is unzipped and select the **OMIMSSC—v7** file and click **Apply**.
4. Check if **Network Adapter** > **Virtual Switch** is connected to a physical NIC card, else configure the NIC card, and select the appropriate NIC card from the **Virtual Switch** drop-down menu and click **Apply**.

If the newly created virtual machine with the selected virtual hard disk of OMIMSSC Appliance fails to boot with any kernel panic exception, edit the virtual machine settings, and enable the dynamic memory option for this virtual machine.To enable the dynamic memory option for a virtual machine, perform the following tasks:

1. Right-click the OMIMSSC Appliance VM, click **Settings**, and then click **Memory**.
2. Under **Dynamic Memory**, select the **Enable Dynamic Memory** check box, and provide the details.

Enrollment failure

If the test connection or enrollment fails, then you get an error message.

As a workaround, perform the following steps:

- Ping from OMIMSSC Appliance to enrolled SCCM or SCVMM server FQDN by logging in to OMIMSSC Appliance VM as a read-only user. If there is a response, then wait for some time and then continue with the enrollment.

  To launch the OMIMSSC Appliance VM as a read-only user, enter user name as `readonly` with the same password used to log into the OMIMSSC Appliance VM.

- Ensure that the SCCM or SCVMM server is running.

- The Microsoft account used to enroll the console should be a delegated admin or an administrator in System Center, and a local administrator for the System Center server.
- Specific for SCVMM users:
  - Ensure that the SCVMM server is not registered with any other OMIMSSC Appliance. If you want to register the same SCVMM server with the OMIMSSC Appliance, then delete the **OMIMSSC Registration Profile** application profile from the SCVMM server.
  - If you have applied SCVMM roll up update, then check the Indigo TCP port number of SCVMM console in registry `(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings)`. Use the same port number that was used to register SCVMM console. By default it is 8100.

Failure of test connection

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2` . When you try to enroll with the above domain user account, the test connection fails.

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

Failure to connect to OMIMSSC console extension for SCVMM

After enrolling and installing OMIMSSC console extension in SCVMM environment, when you try to launch OMIMSSC, the following error is displayed: `Connection to server failed`.

As a workaround, perform the following steps:

1. Add the OMIMSSC Appliance IP and FQDN into local intranet in SCVMM console, when you are launching OMIMSSC.
2. Add the OMIMSSC Appliance IP and FQDN in **Forward Lookup Zones** and **Reverse Lookup Zones** in DNS.
3. For further details, check if there are any error messages in `C:\ProgramData\VMMLogs\AdminConsole` file.

Error accessing console extension after updating SCVMM R2

After applying Update Rollup for SC2012 R2 VMM, if you try to open the already installed OMIMSSC console, SCVMM displays an error message for security reasons, and you cannot access the OMIMSSC console.

As a workaround, do the following:

1. Delete the folder at default path: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Restart SCVMM.
3. Remove the console extension, and then import the console extension as mentioned in *Importing OMIMSSC console extension for SCVMM* section of *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

IP address not assigned to OMIMSSC Appliance

After creating and starting the OMIMSSC Appliance VM, the OMIMSSC Appliance IP address is not assigned or displayed.

As a workaround, check if the virtual switch is mapped to a physical switch, if the switch is configured correctly, and then connect to OMIMSSC Appliance.

SCVMM crashes while importing OMIMSSC console extension

SC2016 VMM RTM build 4.0.1662.0 Administrator console may crash when importing OMIMSSC console extension.

As a workaround, upgrade SCVMM using the 4094925 KB article available at `support.microsoft.com/kb/4094925`, and then import the OMIMSSC console extension.

Failed to login to OMIMSSC console extensions

After logging in to OMIMSSC console extensions with different credentials used to login to Microsoft console, the login activity fails with following error message: `Username or Password is incorrect`

As a workaround, login and launch Microsoft console with the credentials used to login to OMIMSSC console extension. This is a one-time activity.

SC2012 VMM SP1 crashing during update

After upgrading to SC2012 VMM SP1, when importing OMIMSSC console extension to SC2012 VMM UR5 or later, the SCVMM console may crash.

For information about this issue and resolving the issue, see issue 5 in the knowledge base URL: `support.microsoft.com/kb/2785682`.

As a workaround, update SCVMM irrespective of the version of the update rollup that is installed.

OMIMSSC admin portal scenarios

This section has all the troubleshooting information related to OMIMSSC's admin portal

Error message while accessing OMIMSSC admin portal through Mozilla Firefox browser

When accessing the OMIMSSC admin portal by using Mozilla Firefox browser, you get the following warning message: "`Secure Connection Failed`".

As a workaround, delete the certificate created from a previous entry of the admin portal in the browser. For information about deleting certificate from Mozilla Firefox browser, see `support.mozilla.org`

Failure to display Dell EMC logo in OMIMSSC admin portal

When the OMIMSSC admin portal is launched on a Windows 2016 default IE browser, the admin portal is not displayed with the Dell EMC logo.

As a workaround, do one of the following:

- Upgrade IE browser to the latest version.
- Delete the browsing history, and then add the OMIMSSC admin portal URL to browser's favorite list.

Discovery, synchronization and inventory scenarios in OMIMSSC

This section has all the troubleshooting information related to credentials issues, discovering servers, grouping servers, synchronizing enrolled Microsoft console with OMIMSSC when using OMIMSSC.

Failure to discover servers

When multiple Microsoft consoles are enrolled to an OMIMSSC Appliance, and you try to discover a server, if even one of the SCCM consoles are not reachable, then the server discovery job will fail.

As a workaround, de-enroll the SCCM console that is not reachable, or fix the errors and ensure that the SCCM console is reachable from OMIMSSC Appliance.

Discovered servers not added to All Dell Lifecycle Controller Servers collection

After discovering the servers in OMIMSSC for SCCM console extension, the server may not get added into **All Dell Lifecycle Controller Servers** collection.

As a workaround, delete the **All Dell Lifecycle Controller Servers** collection and then discover the server. The collection is automatically created in SCCM and the server is added to this group.

Failure to discover servers due to incorrect credentials

If you provide incorrect credential details during discovery, then based on the iDRAC version, the following resolutions are available:

- - While discovering a 12th generation PowerEdge server with iDRAC version 2.10.10.10 and later, if incorrect details are provided in the credential profile, the server discovery fails, with the following behavior:
    - For first attempt, server IP address is not blocked.
    - For second attempt, server IP address is blocked for 30 seconds.
    - For third and subsequent attempts, server IP address is blocked for 60 seconds.

    You can reattempt server discovery with correct credential profile details after the IP address is unblocked.
  - If the default iDRAC credential profile is changed after a server is discovered and added in the Appliance, then no activity can be performed on the server. To work with the server, rediscover the server with the new credential profile.

Creation of incorrect VRTX chassis group after server discovery

When modular servers that were previously in another chassis are added to a VRTX chassis and discovered in OMIMSSC, the modular servers carry previous chassis service tag information. Hence, a VRTX chassis group with old chassis information is created in the Appliance instead of the latest chassis information.

As a workaround, do the following:

1. Enable CSIOR, and reset iDRAC on the newly added modular server.
2. Manually delete all the servers in the VRTX chassis group, and then rediscover the servers.

Unable to synchronize host servers with enrolled SCCM

During synchronization of OMIMSSC console extension with enrolled SCCM, the servers are not listed as sub tasks in synchronization job and hence does not get synchronized.

As a workaround, launch SCCM console with "Run as Administrator Privilege" and update out of band configuration for a server. Then synchronize OMIMSSC console extension with enrolled SCCM.

For more information, see Synchronizing with enrolled Microsoft console topic in *OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide.*

Empty cluster update group not deleted during autodiscovery or synchronization

When a cluster is discovered in OMIMSSC, a cluster update group gets created in the **Maintenance Center** with all the servers listed in the cluster update group. Later, if all the servers are removed from this cluster through SCVMM, and an autodiscovery or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Maintenance Center**.

As a workaround, to delete the empty server group, rediscover the servers.

Failure to perform maintenance-related tasks on rediscovered servers

When you delete a server or all the servers in an update group from OMIMSSC, and rediscover them you cannot perform any other operations on these servers like updating firmware, exporting and importing LC logs, exporting and importing server profiles.

As a workaround, after rediscovering the deleted server or servers, perform firmware updates using the **Deploy Operational Template** feature in **Server View** and for other maintenance scenarios use iDRAC.

Generic scenarios in OMIMSSC

This section contains troubleshooting information which are independent of any workflow in OMIMSSC.

Failure to access CIFS share using hostname

The modular servers are not able to access the CIFS share using the host name for performing any job in OMIMSSC.

As a workaround, specify the IP address of the server having the CIFS share instead of the host name.

Failure to display Jobs and Logs page in console extension

The **Jobs and Logs Center** page is not displayed in OMIMSSC console extensions.

As a workaround, re-enroll the console and then launch the **Jobs and Logs** page.

Failure of operations on managed systems

All the features of OMIMSSC does not perform as expected on the managed systems due to a Transport Layer Security (TLS) version.

If you are using iDRAC firmware version 2.40.40.40 or later, Transport Layer Security (TLS) versions 1.1 or later is enabled by default. Before installing the console extension, install the update to enable TLS 1.1 and later as mentioned in the following KB article: `Support.microsoft.com/en-us/kb/3140245`. It is recommended that you enable support for TLS 1.1 or later on your SCVMM server and SCVMM console to ensure that OMIMSSC operates as expected. And for more information about iDRAC, see Dell.com/idracmanuals.

Failure to launch online help for OMIMSSC

When using Windows 2012 R2 operating system, the context sensitive online help content is launched displaying an error message.

As a solution, update the operating system using the latest KB articles, and then view the online help content.

Firmware update scenarios in OMIMSSC

This section has all the troubleshooting information related to update sources, update groups, repositories, and inventory after updates.

Failure of creation of update source

When the Domain Name System (DNS) network configuration of the Appliance is changed, creation of HTTP or FTP type of update source fails.

As a workaround, restart the Appliance, and then create the update source of type HTTP or FTP.

Failure to connect to FTP using system default update source

After setting up and configuring, upgrading, or migrating OMIMSSC when you try to access the FTP site using the default update source **Dell Online Catalog** it may fail if proxy credentials are required.

As a workaround, to access the FTP site using **Dell Online Catalog** as an update source, edit the update source to add the proxy credentials.

Failure of test connection for local update source

After proving the details of a local update source, the test connection may fail as the required files may be not accessible.

As a workaround, ensure that `catalog.gz` file is present in the following folder structure.

- For local HTTP update source: `http:\\IP address\catalog\catalog.gz`
- For local FTP update source: `ftp:\\IP address\catalog\catalog.gz`
- For local DRM update source: `\\IP address\\catalog\<catalogfile>.gz`

Failure to create DRM update source

Creating DRM update source on management server running on Windows 10 Operating System (OS) may fail, displaying the following error message: `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Refer the **omimsscappliance_main** log in OMIMSSC Admin portal, if the error message displayed is: *`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

As a workaround, see to the following KB article: *support.microsoft.com/en-us/help/4034314*

Failure to create repository during firmware update

Creation of a repository may fail during a firmware update because of incorrect credentials provided while creating an update source, or update source is not reachable by OMIMSSC Appliance.

As a workaround, ensure that the update source is reachable from where the OMIMSSC Appliance is hosted, and provide the correct credentials while creating an update source.

Failure to display comparison report after upgrading or migrating OMIMSSC

After upgrading to the latest version of OMIMSSC, if the connection to `ftp.dell.com` or `downloads.dell.com` fails, the default Dell online FTP, or Dell HTTP update source cannot download the catalog file. Hence, the comparison report is not available.

As a workaround, to view a comparison report for the default update source, edit the default Dell online FTP, or Dell HTTP update source, create proxy credentials, and then select the update source from **Select Update Source** drop-down menu. For more information about editing an update source, see *Modifying update source* section from *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

Failure to update firmware of clusters

After a job is submitted in OMIMSSC to update firmware of clusters, the clusters are not updated due to certain reasons displaying the following error messages in **Activity Logs**.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

NOTE: The Cluster Aware Update actions are logged in the following locations : \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports folder where the Cluster Aware Update report will be stored. The \\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log folder will further contain the Dell EMC System Update (DSU) plugin logs for each node. Extended script logs are available in C:\Window\Temp location which consists precau.log and postcau.log files in each cluster nodes for S2D cluster.

Reasons of failure of firmware update on clusters with the following workaround:

- If the required DUPs and catalog files are not present in the selected local update source.

  As a workaround is to ensure that all the required DUPs and catalog files are available in the repository, and then update the firmware of clusters.

- Cluster group becomes unresponsive or firmware update job was canceled in CAU due to an in-progress job, then the DUPs are downloaded and placed in each server cluster node belonging to the cluster group.

  As a workaround, delete all the files in Dell folder, and then update the firmware of clusters.

- If Lifecycle Controller (LC) is busy with other operations, then firmware update task on a cluster node fails. To check if the update failed because of LC being busy, check for the following error message in each node of the cluster at the following path: `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then
  reboot the system.
  ```

  As a workaround, shut down the server, remove the power cables, and then restart the server. After reboot, update the firmware on clusters.

Failure of firmware update because of job queue being full

Firmware update job submitted from OMIMSSC to iDRAC fails, and the OMIMSSC main log displays the following error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

As a workaround, manually delete the completed jobs in iDRAC, and retry the firmware update job. For more information about deleting jobs in iDRAC, see iDRAC documentation at **dell.com/support/home**.

Failure of firmware update when using DRM update source

Firmware update job may fail if you are using DRM update source with insufficient access to the share folders. If the Windows credential profile provided while creating DRM update source is not a part of domain administrator group or the local administrator group, the following error message is displayed: `Local cache creation failure.`

As a workaround, perform the following:

1. After creating the repository from DRM, right-click on the folder, click **Security** tab, and then click **Advanced**.
2. Click **Enable inheritance** and select the **Replace all child object permission entries with inheritable permission entries from this object** option, and then share the folder with **Everyone** with read-write permission.

Firmware update on components irrespective of selection

The same components on identical servers get updated during a firmware update irrespective of the selection of components made on these individual servers. This behavior is observed for 12th and 13th generation of PowerEdge servers with Enterprise license of iDRAC.

As a workaround, do one of the following:

- First apply updates for common components on identical servers, and then apply updates for specific components on individual servers.
- Perform staged updates with planned outage time to accommodate the firmware update.

Failure to display latest inventory information after firmware update

After successfully updating the firmware versions on 11th generation PowerEdge servers, the latest inventory information is not displayed.

In OMIMSSC, refreshing the inventory is an activity performed immediately after a firmware update job is complete. Firmware update is completed even before the PowerEdge server's CSIOR activity is complete, due to which the earlier firmware inventory information is displayed.

As a workaround, check if the CSIOR activity is complete in the PowerEdge server, and then refresh the firmware inventory in OMIMSSC. Also, ensure to restart the server after applying agent-free staged update. For more information about refreshing the inventory, see *Viewing and refreshing firmware inventory* section in *OpenManage Integration for Microsoft System Center Configuration Manager and Virtual Machine Manager User's Guide*.

For more information about CSIOR, see the Troubleshooting section in the latest version of *Dell Lifecycle Controller GUI User's Guide* available at **dell.com/support/home**.

Failure to delete a custom update group

After scheduling any job on a server belonging to a custom update group, if the server is deleted from Microsoft console and you synchronize registered Microsoft console with OMIMSSC, the server is removed from the custom update group and the server is moved to a predefined update group. You cannot delete such custom update group, because it is associated with a scheduled job.

As a workaround, delete the scheduled job from **Jobs and Logs** page, and then delete the custom update group.

Failure to update WinPE image

When you try to update the WinPE image, update job may fail with the following error message: `Remote connection to console failed.`

As a workaround, run the **DISM** command to clean up all previously mounted images in Microsoft console, and then retry to update the WinPE image.

Changing of polling and notification bell color after updating the frequency

If a managed server is not discovered in OMIMSSC, and you change the frequency of polling and notification option, the bell color changes to yellow after sometime, even if there are no changes in the catalog.

As a workaround, discover managed servers and then change the frequency of polling and notification option.

Operating system deployment scenarios in OMIMSSC

This section has all the troubleshooting information related to operating system, or hypervisor (for SCVMM) deployment using Operational Template in OMIMSSC.

Operating system deployment generic scenarios

This section has all the generic troubleshooting information related to operating system deployment.

Failure to deploy Operational Template

After deploying the Operational Template on the selected servers, the attributes or attribute values are not appropriate for the selected .CSV file, or the iDRAC IP or iDRAC credentials are changed due to the configurations in the template. The job in iDRAC is successful, however the status of this job in OMIMSSC is shown as unsuccessful or failure due to invalid .CSV file, or the job cannot be tracked due to the iDRAC changes on the target server.

As a workaround, ensure the selected .CSV file has all the proper attributes and attribute values, and the iDRAC IP or credentials do not change due to the configurations in the template.

Failure to save an Operational Template

When you are creating an Operational Template, if you select and clear a dependent attribute's check box having pool value, you are not able to save the Operational Template with the following error message:

```
Select atleast one attribte, under the selected components, before creating the
Operational Template.
```

As a workaround, perform any one of the following:

- Select any other dependent attribute having pool value or the same dependent attribute and save the Operational Template.
- Create a new Operational Template.

Operating system deployment scenarios for SCCM users

This section has all the troubleshooting information related to operating system deployment using OMIMSSC in SCCM console.

Deploy option not visible in task sequence

The **Deploy** option is not displayed in an existing task sequence after uninstalling and reinstalling OMIMSSC console extension for SCCM.

As a workaround, open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option is displayed again.

To re-enable the **Apply** option:

1. Right-click the task sequence, and select **Edit**.
2. Select **Restart in Windows PE**. In the **Description** section, type any character and delete it so the change is not saved.
3. Click **OK**.

   This re-enables the **Apply** option.

Failed to add servers into Managed Lifecycle Controller Lifecycle Controller ESXi collection in SCCM

If the DHCP lookup fails while operating system deployment, then the server times out and the server is not moved into Managed Lifecycle Controller Lifecycle Controller (ESXi) collection in SCCM.

As a workaround, install the SCCM client server, and then perform a synchronization to add the servers in Managed Lifecycle Controller Lifecycle Controller (ESXi) collection.

Operating system deployment scenarios for SCVMM users

This section has all the troubleshooting information related to hypervisor deployment using OMIMSSC in SCVMM console.

Hypervisor deployment failure due to LC or firewall protection

Hypervisor deployment fails displaying the following error message in activity log: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

This error may occur due to one of these reasons:

- Dell Lifecycle Controller's state is bad.

  As resolution, log in to iDRAC user interface and reset Lifecycle Controller.

  After resetting Lifecycle Controller, if you still face the problem try the following alternative:

- The antivirus or firewall may restrict the successful run of the `WINRM` command.

  See the following KB article for workaround: `support.microsoft.com/kb/961804`

Hypervisor deployment failure due to driver files retained in library share

Hypervisor deployment fails displaying the following error message in activity log:

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

These errors may occur due to exception output by the VMM command-let `GET-SCJOB status` and driver files are retained in the library share. Before you retry or do another hypervisor deployment you must remove these files from the library share.

To remove files from library share:

1. From SCVMM console, select **Library** > **Library Servers** and then select the IG server that was added as the library server.
2. In the library server, select and delete the library share.
3. After the library share is deleted, connect to the IG share using `\\<Integration Gateway server>\LCDriver\`.
4. Delete the folder that contains the driver files.

After this, you can deploy the hypervisors.

SCVMM error 21119 while adding servers to Active Directory

While adding servers to Active Directory, SCVMM error 21119 is displayed. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

As a workaround, do the following:

1. Wait for some time to see if the server is added to the Active Directory.
2. If the server is not added to the Active Directory, then manually add the servers to the Active Directory.
3. Add the server in to SCVMM.
4. After the server is added in to SCVMM, rediscover the server in OMIMSSC.

   The server will now be listed under the **Host** tab.

LC driver injection failure

When deploying OS and injecting LC drivers using SC2012 VMM, the OS is deployed successfully but, the LC drivers are not injected.

To resolve the issue, apply the latest rollup for SCVMM.

S2D cluster creation scenarios for SCVMM users

This section has all the troubleshooting information related to creating Storage Spaces Direct using OMIMSSC in SCVMM console.

Health status of S2D cluster is unknown

When you create a Storage Spaces Direct cluster on nodes that were part of an existing cluster, then the storage pool and the disk configurations have the configurations of the existing cluster. Hence, the cluster storage pool might not be created and if the cluster storage pool is created the health status may be displayed as unknown.

As a workaround, clear the storage pool and disk configuration having existing cluster details and then create the Storage Spaces Direct cluster. For more information on clearing the storage pool, see *Troubleshoot Storage Spaces Direct health and operational states* section from Microsoft documentation.

Server profile scenarios in OMIMSSC

This section has all the troubleshooting information related to exporting, and importing the server profiles in OMIMSSC.

Failure to export server profiles

After scheduling an export server profile job, the server profile is not exported, and the following error message is displayed: `The selectors for the resource are not valid.`

As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see iDRAC documentation available at `dell.com/support`.

Importing server profile job gets timed out after two hours

After submitting the import server profile job in OMIMSSC , the job gets timed out after two hours.

As a workaround, perform the following steps:

1. Start the server, press F2, and then enter **BIOS Settings**.
2. Click **System Setup**, and select **Miscellaneous Settings**.
3. Disable **F1/F2 Prompt on Error**.

After performing the following steps, export the server profile again, and use the same server profile to import on that server.

LC Logs scenarios in OMIMSSC

This section has all the troubleshooting information related to exporting, and viewing LC logs.

Failure to export LC logs in .CSV format

When you try to download the LC log files to .CSV format, the download operation fails.

As a workaround, add the OMIMSSC Appliance FQDN in the browser under local intranet site. For information about adding the OMIMSSC Appliance in local intranet, see *Viewing LC logs* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.2.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

Failure to open LC log files

After collecting the LC logs, when you try to view the LC log file for a server, the following error message is displayed: `“Failed to perform the requested action. For more information see the activity log”.`

As a workaround, reset iDRAC, and then collect and view the LC logs. For information about resetting iDRAC, see iDRAC documentation available at `dell.com/support`.

Failure of test connection

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2` . When you try to enroll with the above domain user account, the test connection fails.

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

24

Appendix

Provide the time zone attribute values manually in MX7000 devices by referring to the bellow table:

Table 12. Time zone details

Time zone ID	Time zone difference
TZ_ID_1	(GMT-12:00) International Date Line West
TZ_ID_2	(GMT+14:00) Samoa
TZ_ID_3	(GMT-10:00) Hawaii
TZ_ID_4	(GMT-09:00) Alaska
TZ_ID_5	(GMT-08:00) Pacific Time (US and Canada)
TZ_ID_6	(GMT-08:00) Baja California
TZ_ID_7	(GMT-07:00) Arizona
TZ_ID_8	(GMT-07:00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07:00) Mountain Time (US and Canada)
TZ_ID_10	(GMT-06:00) Central America
TZ_ID_11	(GMT-06:00) Central Time (US and Canada)
TZ_ID_12	(GMT-06:00) Guadalajara, Mexico City, Monterrey
TZ_ID_13	(GMT-06:00) Saskatchewan
TZ_ID_14	(GMT-05:00) Bogota, Lima, Quito
TZ_ID_15	(GMT-05:00) Eastern Time (US and Canada)
TZ_ID_16	(GMT-05:00) Indiana (East)
TZ_ID_17	(GMT-04:30) Caracas
TZ_ID_18	(GMT-04:00) Asuncion
TZ_ID_19	(GMT-04:00) Atlantic Time (Canada)
TZ_ID_20	(GMT-04:00) Cuiaba
TZ_ID_21	(GMT-04:00) Georgetown, La Paz, Manaus, San Juan
TZ_ID_22	(GMT-04:00) Santiago
TZ_ID_23	(GMT-03:30) Newfoundland
TZ_ID_24	(GMT-03:00) Brasilia
TZ_ID_25	(GMT-03:00) Buenos Aires
TZ_ID_26	(GMT-03:00) Cayenne, Fortaleza
TZ_ID_27	(GMT-03:00) Greenland
TZ_ID_28	(GMT-03:00) Montevideo
TZ_ID_29	(GMT-02:00) Mid-Atlantic
TZ_ID_30	(GMT-01:00) Azores
TZ_ID_31	(GMT-01:00) Cape Verde Is

Table 12. Time zone details (continued)

Time zone ID	Time zone difference
TZ_ID_32	(GMT+00:00) Casablanca
TZ_ID_33	(GMT+00:00) Coordinated Universal Time
TZ_ID_34	(GMT+00:00) Dublin, Edinburgh, Lisbon, London
TZ_ID_35	(GMT+00:00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
TZ_ID_37	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
TZ_ID_38	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
TZ_ID_39	(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
TZ_ID_40	(GMT+01:00) West Central Africa
TZ_ID_41	(GMT+02:00) Windhoek
TZ_ID_42	(GMT+02:00) Amman
TZ_ID_43	(GMT+03:00) Istanbul
TZ_ID_44	(GMT+02:00) Beirut
TZ_ID_45	(GMT+02:00) Cairo
TZ_ID_46	(GMT+02:00) Damascus
TZ_ID_47	(GMT+02:00) Harare, Pretoria
TZ_ID_48	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
TZ_ID_49	(GMT+02:00) Jerusalem
TZ_ID_50	(GMT+02:00) Minsk
TZ_ID_51	(GMT+03:00) Baghdad
TZ_ID_52	(GMT+03:00) Kuwait, Riyadh
TZ_ID_53	(GMT+03:00) Moscow, St. Petersburg, Volgograd
TZ_ID_54	(GMT+03:00) Nairobi
TZ_ID_55	(GMT+03:30) Tehran
TZ_ID_56	(GMT+04:00) Abu Dhabi, Muscat
TZ_ID_57	(GMT+04:00) Baku
TZ_ID_58	(GMT+04:00) Port Louis
TZ_ID_59	(GMT+04:00) Tbilisi
TZ_ID_60	(GMT+04:00) Yerevan
TZ_ID_61	(GMT+04:30) Kabul
TZ_ID_62	(GMT+05:00) Ekaterinburg
TZ_ID_63	(GMT+05:00) Islamabad, Karachi
TZ_ID_64	(GMT+05:00) Tashkent
TZ_ID_65	(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi
TZ_ID_66	(GMT+05:30) Sri Jayawardenepura
TZ_ID_67	(GMT+05:45) Kathmandu

Table 12. Time zone details (continued)

Time zone ID	Time zone difference
TZ_ID_68	(GMT+06:00) Astana
TZ_ID_69	(GMT+06:00) Dhaka
TZ_ID_70	(GMT+06:00) Novosibirsk
TZ_ID_71	(GMT+06:30) Yangon (Rangoon)
TZ_ID_72	(GMT+07:00) Bangkok, Hanoi, Jakarta
TZ_ID_73	(GMT+07:00) Krasnoyarsk
TZ_ID_74	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
TZ_ID_75	(GMT+08:00) Irkutsk
TZ_ID_76	(GMT+08:00) Kuala Lumpur, Singapore
TZ_ID_77	(GMT+08:00) Perth
TZ_ID_78	(GMT+08:00) Taipei
TZ_ID_79	(GMT+08:00) Ulaanbaatar
TZ_ID_80	(GMT+08:30) Pyongyang
TZ_ID_81	(GMT+09:00) Osaka, Sapporo, Tokyo
TZ_ID_82	(GMT+09:00) Seoul
TZ_ID_83	(GMT+09:00) Yakutsk
TZ_ID_84	(GMT+09:30) Adelaide
TZ_ID_85	(GMT+09:30) Darwin
TZ_ID_86	(GMT+10:00) Brisbane
TZ_ID_87	(GMT+10:00) Canberra, Melbourne, Sydney
TZ_ID_88	(GMT+10:00) Guam, Port Moresby
TZ_ID_89	(GMT+10:00) Hobart
TZ_ID_90	(GMT+10:00) Vladivostok
TZ_ID_91	(GMT+11:00) Magadan, Solomon Is New Caledonia
TZ_ID_92	(GMT+12:00) Auckland, Wellington
TZ_ID_93	(GMT+12:00) Fiji
TZ_ID_94	(GMT+13:00) Nuku'alofa
TZ_ID_95	(GMT+14:00) Kiritimati
TZ_ID_96	(GMT+02:00) Athens, Bucharest

25

Appendix 2

Populating Pool value CSV file

Table 13. Pool value file

serviceTag(auto populated)	FQDD(auto populated)	poolAttributeName	poolAtrributeValue
Service Tag of the device(s) from which the system specific attributes are exported	Identifies the component associated to the system specific attribute	Identifies the system specific attribute to be configured	Set the value for the specified system specific attribute

Table 14. Examples

serviceTag(auto populated)	FQDD(auto populated)	poolAttributeName	poolAtrributeValue	Details on what is the attribute and how to populate
xxxxxxx	WINDOWS	HOSTNAME	WIN19SRVDTA	What : this is the hostname to be set on deployed / provisioned server.
xxxxxxx	WINDOWS	ServerMngNIC	<MAC Adresses>	What : This is the MAC Address of the network port which can communicate to System Center and OMMISSC Appliance. How : Retrieve the MAC Address from iDRAC by navigating to specific port.
xxxxxxx	WINDOWS	LOGICALNETWORK	OSD USING STATIC IP	What : This is the Network Profile created in SCVMM that carries static IP pool, subnet and other network details to be applied on MN How : Create the Logical Network Profile in SCVMM and provide the created template name. For more information, see Plan the VMM networking fabric section of Microsoft Documentation.
xxxxxxx	WINDOWS	IPSUBNET	100.100.28.0/22	What : This is the subnet mask for the static IP pool input in above logical network profile.
xxxxxxx	WINDOWS	IPADDRESS	100.100.31.145	What : This is the static IP to be applied on deployed /provisioned managed node.

26

Accessing documents from the Dell EMC support site

You can access the required documents in one of the following ways:

- Using the following links:
    - For Dell EMC Enterprise Systems Management, Dell EMC Remote Enterprise Systems Management, and Dell EMC Virtualization Solutions documents — www.dell.com/esmmanuals
    - For Dell EMC OpenManage documents — www.dell.com/openmanagemanuals
    - For iDRAC documents — www.dell.com/idracmanuals
    - For Dell EMC OpenManage Connections Enterprise Systems Management documents — www.dell.com/OMConnectionsEnterpriseSystemsManagement
    - For Dell EMC Serviceability Tools documents — https://www.dell.com/serviceabilitytools
- From the Dell EMC Support site:
    1. Go to https://www.dell.com/support.
    2. Click **Browse all products**.
    3. From **All products** page, click **Software**, and then click the required link from the following:
        - **Analytics**
        - **Client Systems Management**
        - **Enterprise Applications**
        - **Enterprise Systems Management**
        - **Mainframe**
        - **Operating Systems**
        - **Public Sector Solutions**
        - **Serviceability Tools**
        - **Support**
        - **Utilities**
        - **Virtualization Solutions**
    4. To view a document, click the required product and then click the required version.
- Using search engines:
    - Type the name and version of the document in the search box.