OpenManage Integration Version 7.0 for Microsoft System Center

User’s Guide

Notes, cautions, and warnings

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

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

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

2017 - 08

Rev. A00

Contents

1 Introduction......7

OMIMSSC features......7

2 About OMIMSSC components......9

3 About Admin Portal......10

Modifying IG and SCCM or SCVMM accounts......10

Modifying credentials in OMIMSSC Admin Portal......10

Repairing OMIMSSC console extension for SCCM......11

Repairing OMIMSSC console extension for SCVMM......11

Repairing OMIMSSC IG......11

4 Launching OMIMSSC from enrolled MSSC console......12

Browser settings......12

Launching OMIMSSC console extension for SCCM......12

Launching OMIMSSC console extension for SCVMM......12

5 Use cases......13

OS deployment using OMIMSSC console extension for SCCM......13

OS deployment using OMIMSSC console extension for SCVMM......14

Non-windows OS deployment using OMIMSSC console extensions......14

Apply updates on servers......14

Configuring replaced components......15

Export and import server profiles......15

6 Profiles......16

About credential profile......16

Predefined credential profiles......16

Creating credential profile......16

Modifying credential profile......17

Deleting credential profile......18

About hypervisor profile......18

Creating hypervisor profile......18

Modifying hypervisor profile......19

Deleting hypervisor profile......19

7 Launching Configuration and Deployment......20

8 Discovering servers and synchronizing with MSSC console......22

About reference server configuration......22

Discovering servers in OMIMSSC......22

Server discovery in OMIMSSC console extension for SCCM......23

Server discovery in OMIMSSC console extension for SCVMM.... 23
System requirements for managed systems 23
Discovering servers using auto discovery.... 24
Discovering servers using manual discovery.... 24
Synchronizing OMIMSSC console extensions with enrolled SCCM.... 24
Synchronizing OMIMSSC console extension with enrolled SCVMM....25
Synchronizing with enrolled MSSC.... 25
Resolving synchronization errors.... 25
Deleting servers from OMIMSSC.... 26
Launching iDRAC console....26

9 OMIMSSC licensing....27
Options after uploading licenses.... 27
License file for new purchases.... 27
Stacking licenses.... 27
Replacement of licenses 28
Reimporting licenses....28
Importing multiple licenses....28
Enforcement.... 28
Upgrading licenses.... 28
Evaluation License....28
License consumption in OMIMSSC after server discovery.... 28
Importing license in to OMIMSSC.... 29
Viewing license details....29

10 Operational Template.... 30
Preparing for deployment.... 30
Creating WinPE ISO image 30
Task sequence....31
Editing a task sequence.... 33
Creating Lifecycle Controller boot media....33
Setting a default share location for the Lifecycle Controller boot media....33
Creating a task sequence media bootable ISO....34
For working with deploying non-Windows operating systems 34
Managing Operational Template....34
Creating Operational Template.... 34
Viewing Operational Template.... 37
Editing Operational Template.... 37
Deleting Operational Template....38
Assigning Operational Template and running Operational Template compliance.... 38
Deploying Operational Template....38

11 Integration with Dell Repository Manager(DRM).... 40

12 Maintenance.... 41
About firmware updates 41

Applying updates on servers....42
Recovery....49
Protection vault....49
Exporting server profiles....50
Importing server profile....51
Applying firmware and configuration settings....52
Collecting LC logs....52
Viewing LC logs....53
File description....54
Exporting inventory....54

13 Viewing information in OMIMSSC....55
Viewing jobs....55
Managing jobs....56

14 Troubleshooting....57
Deploy option not visible in task sequence....57
Duplicate VRTX chassis group gets created 58
Empty cluster update group does not get deleted during autodiscovery or synchronization....58
Failure of creation of update source....58
Failure of firmware update because of job queue being full....58
Failure of firmware update on cluster update group....58
Failure of firmware update on 11th generation of servers....59
Failure of firmware update while using DRM update source 59
Failure of scheduled job on an update group....59
Failure to apply Operational Template 59
Failure to access CIFS share using hostname....59
Failure to connect to FTP using system default update source....59
Failure to create a repository during a firmware update....60
Failure to delete a custom update group....60
Failure to display Jobs and Logs....60
Failure to export LC logs in CSV format....60
Failure to export server profiles 60
Failure to display Dell EMC logo in OMIMSSC Admin Portal....60
Failure to view LC logs 60
Firmware update on a few components irrespective of the selection....61
Hypervisor deployment failure....61
Hypervisor deployment failure due to driver files retained in library share....61
Hypervisor deployment failure for 11th generation PowerEdge blade servers when using Active Directory....62
Incorrect credentials during discovery....62
IG installation issue while running multiple instances of the installer on the same server 62
Importing server profile job gets timed out after two hours....62
Latest inventory information is not displayed even after firmware update....63
SCVMM error 21119 while adding servers to active directory....63

15 Appendix....64

16 Accessing documents from the Dell EMC support site....... 65

Contacting Dell....... 65

1

Introduction

OpenManage Integration for Microsoft System Center (OMIMSSC) provides integrations into the System Center suite of products that enable full lifecycle management of the Dell EMC servers by using the integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC).

OMIMSSC offers operating system deployment, hardware patching, firmware update, and server maintenance. With OMIMSSC, you can either integrate with Microsoft System Center Configuration Manager (SCCM) for managing the Dell EMC servers in traditional data center, or use the integration with Microsoft System Center Virtual Machine Manager (SCVMM) for managing the Dell EMC servers in virtualized and cloud environments.

This guide provides information about using the product and all the use cases of the product.

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

OMIMSSC features

Table 1. Features for this release

Feature	Description
Non-windows Operating System (OS) deployment	Support for non-Windows(ESXi and RHEL) operating system deployments.
14th generation PowerEdge servers	Support for discovering and managing 14th generation of the Dell EMC PowerEdge servers.
iDRAC Lock Down Mode	Support for iDRAC Lockdown Mode for 14th generation PowerEdge servers.
Multiconsole	Support for integration with multiple SCCM and SCVMM consoles with a single OMIMSSC Appliance.
Discovery	Discover 11th generation PowerEdge servers and later, and deploy them in the Microsoft System Center (MSSC) environment.
Synchronization with MSSC	Synchronize all Dell EMC host systems listed in the enrolled SCCM or SCVMM environment with OMIMSSC.
License center	Manage OMIMSSC licenses from the Admin Portal.
Inventory	View key inventory details about the Dell EMC servers.
Configure hardware	Support for configuring network adapter, fiber channel, and the PCIe, SSD components of the PowerEdge servers.
Boot media creation	Support a zero-touch deployment boot media from your task sequence media.
Operational template	Usage of a uniform template for firmware update, hardware configuration, and operating system deployment.
Operational template compliance	Verify hardware configuration compliance against operational template.

Microsoft Cluster-Aware Updating (CAU)	Automate the firmware update process through the CAU feature of Microsoft.
Export inventory	After comparing the servers inventories against the update source, you can export the comparison report to .CSV or .XML file.
Export server profile	Export a server profile including firmware images on components such as Basic Input Output System (BIOS), Redundant Array of Independent Disks (RAID), Network Interface Controller (NIC), iDRAC, LC, and so on, to an internal or external location.
Import server profile	Import a server profile by either retaining or excluding the current RAID settings.
Collect and View LifeCycle Controller (LC) log messages	Export, view, download to .CSV file, and search the LC log messages.
Polling and notifications	Configure notifications to receive alerts when new catalogs are available in update source.

About OMIMSSC components

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

- OpenManage Integration for Microsoft System Center Appliance virtual machine, also known as Appliance is hosted 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.
  - Enables you to administer the OMIMSSC Appliance through the Admin Portal.
- OMIMSSC Integration Gateway also known as Integration Gateway (IG) is a set of web services installed on the Windows server and performs the following tasks:
  - Runs SCCM or SCVMM Powershell commands, and acts as an intermediate gateway between SCCM or SCVMM and Appliance.
  - Customizes WinPE for Appliance.
- OpenManage Integration for Microsoft System Center console, also known as the OMIMSSC console
  - OMIMSSC console plug-in for SCCM, also known as the OMIMSSC console extension for SCCM
  - OMIMSSC console Add-in for SCVMM, also known as the OMIMSSC console extension for SCVMM

3

About Admin Portal

The Admin Portal allows you to log in to OMIMSSC as an administrator to view all jobs started in OMIMSSC by various users, view license details, console details, download the required components, and to upgrade OMIMSSC. Following are the use cases in admin portal along with licensing.

Topics:

- Modifying IG and SCCM or SCVMM accounts
- Repairing OMIMSSC console extension for SCCM
- Repairing OMIMSSC console extension for SCVMM
- Repairing OMIMSSC IG

Modifying IG and SCCM or SCVMM accounts

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

About this task

You can modify the SCCM, the SCVMM administrator credentials, and IG credentials from the Admin Portal. This process is a sequential activity.

- For the IG account, perform the following prerequisites before modifying the account in OMIMSSC:
  a. Modify the credentials in active directory.
  b. Modify the credentials in IG installer.
- For SCCM or SCVMM account, modify the credentials in active directory, before modifying the account in OMIMSSC.

To modify the OMIMSSC IG account from installer:

Steps

1. Run the IG installer.
2. In **Program Maintenance**, select **Modify** and then click **Next**.
3. Change password and then click **Next**.
4. In **Modify the program**, click **Install**.
5. Click **Finish** after the modify task is complete.

Modifying credentials in OMIMSSC Admin Portal

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 details and, click **Finish** to save the changes.

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**.

Repairing OMIMSSC IG

About this task

By using this option, you can reinstall the deleted or corrupt files, or recreate the folders required for OMIMSSC IG.

Steps

1. Run the OMIMSSC IG installer.
2. In **Program Maintenance**, select **Repair**, and then click **Next**.
3. In **Ready to Repair**, provide the IG user account password, and then click **Install**.
4. Click **Finish** after the repair task is complete.

4

Launching OMIMSSC from enrolled MSSC console

Launch OMIMSSC from enrolled SCCM or SCVMM console.

Topics:

- Browser settings
- Launching OMIMSSC console extension for SCCM
- Launching OMIMSSC console extension for SCVMM

Browser settings

About this task

Before launching OMIMSSC, add the IP address of OMIMSSC as a prerequisite into the **Local Intranet** site list to perform the following operations:

- export and view firmware inventory
- view LC logs
- export pool values in Operational Template

Before downloading .CSV files, perform the following steps:

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

Prerequisites

Log in to Windows OS with the same credentials that is used to log in to the OMIMSSC console extension for SCCM.

Steps

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), 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

1. In the 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 the **Home** ribbon, select **OMIMSSC**.

5

Use cases

You can deploy OS only on servers whose hardware configuration is compatible with OMIMSSC. Before deploying OS, make sure you upgrade the firmware versions to the latest versions available at ftp.dell.com or downloads.dell.com, and then continue with OS deployment. Following are some of the scenarios of using OMIMSSC console extensions:

Topics:

- OS deployment using OMIMSSC console extension for SCCM
- OS deployment using OMIMSSC console extension for SCVMM
- Non-windows OS deployment using OMIMSSC console extensions
- Apply updates on servers
- Configuring replaced components
- Export and import server profiles

OS deployment using OMIMSSC console extension for SCCM

About this task

To deploy OS on selected servers, perform the following steps:

Steps

1. Download the latest Dell Deployment ToolKit (DTK) and create a Windows Preinstallation Environment (WinPE) boot ISO image. For more information, see the WinPE update.
2. Import this .wim 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*.
5. Generate an unattended ISO image. For more information, see LC Boot media creation.
6. Discover a reference server by using the **Discovery** page. For more information, see Discovering servers using manual discovery.
7. Create an Operational Template. For more information, see Creating Operational Template.
8. Assign an Operational Template. For more information, see Assigning Operational Template.
9. Deploy an Operational Template. For more information, see Deploying Operational Template.

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

   ⓘ **NOTE: After deploying Windows OS successfully in the SCCM environment, the server is not listed as a host in OMIMSSC. To view the server in the host tab, verify that the Client status of the server is YES in SCCM, and then synchronize OMIMSSC with SCCM.**
10. View the job status on firmware update and OSD in the **Jobs and Logs Center** page. For more information, see Viewing information in OMIMSSC.

OS deployment using OMIMSSC console extension for SCVMM

About this task

To deploy OS on the selected servers, perform the following steps:

Steps

1 Download the latest Dell 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 in SCVMM. For more information, see the SCVMM documentation.

3 Create a target host group in SCVMM. For more information, see the SCVMM documentation.

4 Create a hypervisor profile in the OMIMSSC console extension for SCVMM. For more information, see Creating a hypervisor profile.

5 Discover a reference server by using the **Discovery** page. For more information, see the Discovering servers using manual discovery.

6 Create an Operational Template. For more information, see Creating Operational Template.

7 Assign an Operational Template. For more information, see Assigning Operational Template.

8 Deploy an Operational Template. For more information, see Deploying Operational Template.

Table 3. Different scenarios for hypervisor deployment

If you require the latest factory drivers and out-of-band drivers	While creating a hypervisor profile, enable LC (Lifecycle Controller) driver injection.
If you want to retain the existing hardware configuration	While creating the Operational Template, clear the checkbox for all the physical components .

9 View the job status on firmware update and OSD in the **Jobs and Logs Center** page. For more information, see Viewing information in OMIMSSC.

Non-windows OS deployment using OMIMSSC console extensions

About this task

To deploy any flavor of non-windows OS:

Steps

1 Create an Operational Template. For more information, see Creating Operational Template.

2 Assign an Operational Template. For more information, see Assigning Operational Template.

3 Deploy an Operational Template. For more information, see Deploying Operational Template.

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

Apply updates on servers

About this task

You can update the selected servers or server groups by using the following update sources:

- Online FTP and local FTP source
- Online HTTP and local HTTP
- Local Dell Repository Manager (DRM) repository

Steps

1. Before you begin updates, view information about update sources and update groups. For more information about update source, see Update source. Ensure that there is an update source created. For more information, see Creating an update source.
2. Discover or synchronize servers with registered MSSC. For more information, see Device discovery and synchronization .Ensure that the servers inventory is up-to-date. For more information, see Launching configuration and deployment.
3. Update the servers by using one of the following options:
   - Select the required server groups to apply the updates. For more information, see Applying updates on servers.

     ⓘ **NOTE: Select Allow Downgrade to downgrade the firmware version of the components.**
   - Use the firmware update component in Operational Template. For more information, see Creating Operational Template.
4. Modify the update source with the latest catalog by using polling and notification. For more information, see Polling and notification.

Configuring replaced components

For updating a replaced server component to the required firmware version or the configuration of the old component, or both, see Applying firmware and configuration settings.

Export and import server profiles

To export and import a server profile:

1. Create a protection vault. For more information, see Creating protection vault.
2. Export a server profile. For more information, see Creating export job.
3. Export a server profile including the RAID configuration, and import a server profile including the RAID configuration. For more information, see Recovery.

6

Profiles

Profiles allow you to manage your credentials and customize WinPE images for deployment. The various types of profiles supported in OMIMSSC are:

Topics:

- About credential profile
- About hypervisor profile

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. A credential profile authenticates a user's role-based capabilities. The Appliance 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 when working with different features of iDRAC.

You can create four types of credential profiles:

- Device Credential Profile — this profile is used to log in to iDRAC or Chassis Management Controller (CMC).

  > ⓘ **NOTE: When no default profile is created or selected, the default iDRAC factory setting is used. The default user name as `root` and password as `calvin` is used.**
  >
  > The default iDRAC profile is used to access the server when you discover a server or perform synchronization.

  > ⓘ **NOTE: The default CMC profile has user name as `root` and password as `calvin`, and is used to access the modular server to get information about the chassis.**

  > ⓘ **NOTE: Use the device type credential profile to discover a server, log in to CMC, resolve synchronization issues, and deploy operating system.**
- Windows Credential Profile — this profile is used for accessing Windows Shares while creating a DRM update source.
- FTP Credential Profile — this profile is used for accessing an FTP site.
- Proxy Server Credentials — this profile is used for providing proxy credentials for accessing any FTP sites for updates.

Predefined credential profiles

SYSTEM DEFAULT FTP account is a predefined credential profile of the type FTP credentials having **Username** and **Password** as **anonymous**. It is not editable. This profile is used to access `ftp.dell.com`

Creating credential profile

About this task

When creating a credential profile, consider the following:

- When a device type credential profile is created, an associated **RunAsAccount** is created in **SCVMM** to manage the server and the name of the **RunAsAccount** is `Dell_CredentialProfileName`.

- During auto discovery, if there is no credential profile available for iDRAC, then the default iDRAC factory settings is used. The default user name is **root**, and password is **calvin**.

Steps

1. In OMIMSSC, do any of the following to open Credential Profile:
   - In the OMIMSSC dashboard, click **Create Credential Profile**.
   - In the navigation pane, click **Profiles** > **Credential Profile**, and then click **Create**.
2. In **Credential Profile**, select the credential profile type that you want to use.

   OMIMSSC supports four types of credential profiles and there is one predefined credential profile. You can create the following four types of credential profile:

   - **Device Credential Profile**—use this profile to log in to iDRAC or Chassis Management Controller (CMC).

     > ⓘ NOTE: **When creating Device Credential Profile, select iDRAC, to make it as default profile for iDRAC, or CMC to make it default profile for Chassis Management Controller (CMC). Select None if you choose not to set this profile as a default profile.**

     - When a device type credential profile is created, an associated **RunAsAccount** is created in **SCVMM** to manage the server, and the name of the account is **Dell_CredentialProfileName**.
       - Recommended to not edit or delete the **RunAsAccount**.
     - If you delete the device type credential profile, the associated **RunAsAccount** from SCVMM is also deleted. Hence, the corresponding credential profile is not visible in OMIMSSC.
   - **Windows Credential Profile**—use this profile for accessing shared folders in Windows.
   - **FTP Credential Profile**—use this profile for accessing the FTP site.

     > ⓘ NOTE: **The default FTP credential profile that is available in Appliance is, System Default FTP.**

   - **SYSTEM DEFAULT FTP**—predefined credential profile of type FTP credentials, and the password field is not mandatory for this type.
   - **Proxy Server Credentials**—use this profile for providing proxy credentials for FTP sites for firmware updates.
3. In **Domain**, provide the domain details for the Windows credentials, in **Proxy Server URL**, provide the proxy server URL `http://hostname:port` or `http://IPaddress:port` format, in **Default Profile for**, select to make this profile as the default profile to log in to iDRAC or CMC. Select **None**, if you choose not to set the profile as a default profile.

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

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

Modifying credential profile

About this task

Consider the following when you are modifying a credential profile:

- After creating, you cannot modify the type of a credential profile. However, you can modify other fields. To view the modifications, refresh the screen.
- You cannot modify a device type credential profile if it is being used.
- You cannot modify a credential profile, if it is in use.

Steps

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

Deleting credential profile

About this task

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 Appliance.
- To delete a credential profile that is used in server discovery, delete the discovered server information and then delete the credential profile.
- To delete a device type credential profile that is used for deployment, first delete the servers 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.

Steps

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

About hypervisor profile

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.

NOTE: Hypervisor profiles are applicable only for OMIMSSC console extension for SCVMM.

Creating hypervisor profile

You can create a hypervisor profile and use the profile to deploy the operating system on servers.

Prerequisites

- During hypervisor profile creation, the required WinPE ISO is created and the same is available in the share folder of OMIMSSC IG. To update the WinPE image, see WinPE update.
- Create a host group, a host profile, or physical computer profile, in SCVMM.

Steps

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** > **Hypervisor Profiles** > **Create**.
2 In the **Hypervisor Profile Wizard** > **Welcome** > **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.
5 In **WinPE Boot Image Source**,
   a Select the method that you want to use to access the operating system and the associated settings and in **Network WinPE ISO Name**
   b Select the operating system ISO you want to use and then click **Next**.
6 (Optional) To enable LC driver injection
   a Select the operating system that you want to deploy so that the relevant drivers are picked up
   b Select **Enable LC Drivers Injection**

c Select the hypervisor version **Hypervisor Version**.

7 In **Summary**, click **Finish**.

Modifying hypervisor profile

About this task

Consider the following when you are modifying a hypervisor profile:

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

Steps

1 Select the profile that you want to modify and click **Edit**.

2 Provide the details, and click **Finish**.

Deleting hypervisor profile

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

7

Launching Configuration and Deployment

The **Configuration and Deployment** page lists all unassigned and host servers. By using the host name or IP address of a server, you can view the server details such as the iDRAC IP address or host name, server identifier, cluster FQDN, chassis service tag, server model, server generation, CPU, memory, and compliance status. On hovering with your mouse over the **Hardware Compatibility** column, you can view the versions of BIOS, iDRAC, LC, and driver packs.

About this task

Before launching the OMIMSSC console extensions, verify the iDRAC System Lockdown Mode setting. The System Lockdown Mode setting is available in iDRAC for 14th generation of PowerEdge servers. 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. 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.

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

ⓘ **NOTE: For 14th generation PowerEdge servers, ensure that you manually disable the Sytem Lockdown Mode setting of the managed hosts from the iDRAC console.**

By using the **Configuration and Deployment** page, perform the following tasks:

- Discover servers
- Refresh the page to view updated information
- Delete servers from OMIMSSC
- Synchronize with enrolled MSSC.
- Resolve synchronization errors
- Assign Operational Template and run Operational Template compliance.
- Deploy Operational Template
- Correlate host servers to cluster group and the chassis to which the server belongs to.
- Launch iDRAC Console.

ⓘ **NOTE: If the server is not part of a chassis, then the Chassis Service Tag is displayed blank.**

ⓘ **NOTE: If the host server is a part of a cluster, to correlate a server to its cluster group and to know the chassis information, see the Cluster FQDN and Chassis Service Tag columns.**

ⓘ **NOTE: To work with the servers discovered in the prior versions of OMIMSSCAppliance, 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 this user. Hence, make sure that you have the required privileges before performing any operations on the servers.**

ⓘ **NOTE: If the server is Operational Template compliant, then there is a green color box with a tick against the assigned Operational Template.**

ⓘ **NOTE: If the server is Operational Template noncompliant, then there is a red color warning message against the assigned Operational Template.**

To view servers:

Steps

In the OMIMSSC console extension, click **Configuration and Deployment**.

> ⓘ **NOTE: All the server groups that exist in registered MSSC are listed in OMIMSSC because this page is not user-specific. Make sure you have access to perform any operations on those servers.**

All the servers discovered or synchronized with the registered MSSC are listed under the **Unassigned Servers** or **Hosts** tab.

8

Discovering servers and synchronizing with MSSC console

Discovery is the process of adding supported PowerEdge bare-metal server or host servers in OMIMSSC, and synchronization with MSSC console allows you to add host servers from SCCM or SCVMM console into OMIMSSC.

Topics:

- About reference server configuration
- Discovering servers in OMIMSSC
- Server discovery in OMIMSSC console extension for SCCM
- Server discovery in OMIMSSC console extension for SCVMM
- System requirements for managed systems
- Discovering servers using auto discovery
- Discovering servers using manual discovery
- Synchronizing OMIMSSC console extensions with enrolled SCCM
- Synchronizing OMIMSSC console extension with enrolled SCVMM
- Synchronizing with enrolled MSSC
- Resolving synchronization errors
- Deleting servers from OMIMSSC
- Launching iDRAC console

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 by capturing these settings in an Operational Template, and replicate it across different servers with same hardware configuration.

Discovering servers in OMIMSSC

You can discover hosts and unassigned servers in OMIMSSC. The discovered servers information is saved in the OMIMSSC database.

Consider the following points after discovering a server:

- The discovered server is added to the **Hosts** or **Unassigned** tab in the **Configuration and Deployment** page of OMIMSSC.
- The discovered server is marked as hardware compatible when it contains supported versions of LC firmware, iDRAC, and BIOS to work with OMIMSSC. For information about the supported versions, see *OpenManage Integration for Microsoft System Center Release Notes*.
- A license is consumed for the discovered server.

  The **Licensed Nodes** count in **License Center** page decreases as the number of servers are discovered.
- When you discover a PowerEdge server with an operating system deployed on it, and the server is already present in SCCM or SCVMM console, then the server is listed as a host server under the **Hosts** tab in OMIMSSC console extensions where the discovery job is initiated.

  - If the host is a modular server, then the service tag of the chassis containing the server is also displayed on the **Configuration and Deployment** page.
- When you discover a PowerEdge server that is not listed in SCCM or SCVMM, then the server is listed as an unassigned server under the **Unassigned** tab in all the enrolled OMIMSSC console extensions.

You can discover Dell EMC servers using their iDRAC IP address using:

- Auto discovery
- Manual discovery

Server discovery in OMIMSSC console extension for SCCM

After discovering a server, the server is added to one of the following SCCM predefined groups or collections—**All Lifecycle Controller 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 is no predefined groups or collections in SCCM, the predefined collections are created and the discovered servers are added to the respective group.

ⓘ NOTE: **The discovered server 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.***

Server discovery in OMIMSSC console extension for SCVMM

You can discover hyper-V hosts, modular hyper-V hosts, and unassigned servers in OMIMSSC console extension for SCVMM.

ⓘ NOTE: **If the host is part of a cluster, then the Fully Qualified Domain Name (FQDN) of the cluster is displayed.**

System requirements for managed systems

Managed systems are the systems that are managed using OMIMSSC. For discovering servers using OMIMSSC console extension for SCCM or OMIMSSC console extension for SCVMM following are the system requirements:

- OMIMSSC console extension for SCVMM supports modular and monolithic server models on 11th and later generations of PowerEdge servers.
- OMIMSSC console extension for SCCM supports modular, monolithic, and tower server models on 11th and later generations of PowerEdge 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 the servers, connect the PowerEdge servers to the network and power on the servers for OMIMSSC. OMIMSSC auto discovers the unassigned Dell EMC servers by using the remote enablement feature of iDRAC. OMIMSSC works as the provisioning server and uses the iDRAC reference to auto discover Dell EMC servers.

1 In OMIMSSC, create a device type credential profile (by specifying the iDRAC credentials and marking it as default) for Dell EMC servers. For more information, see Creating a credential profile.
2 To auto discover Dell EMC servers, perform the following tasks:
   a Disable the existing Administrator account in iDRAC.

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

   b To enable auto-discovery of the target server, in **iDRAC Settings**, under in **Remote Enablement**, select **Enabled** option for **Enable Auto-Discovery** feature.
   c After enabling auto discovery, provide the provisioning server's IP address (IP address of server where OMIMSSC is installed) and restart the server.

Discovering servers using manual discovery

You can manually discover the 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.

1 In the OMIMSSC console, do any of the following:
   - In the dashboard, click **Discover Unassigned Servers**.
   - In the navigation pane, click **Configuration and Deployment**, 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 **Dell 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 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, and click **Finish**.
7 (Optional) to track this job select **Go to the Job List** option.

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

Synchronizing OMIMSSC console extensions with enrolled SCCM

You can synchronize all PowerEdge servers (hosts and unassigned) from SCCM to OMIMSSC.

Prerequisites

Before synchronizing PowerEdge servers with OMIMSSC console extension and the enrolled SCCM or SCVMM console, ensure that the following requirements are met:

- The servers' default iDRAC credential profile details are required.

- 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.

About this task

After synchronizing OMIMSSC with SCCM, if the server is not present in SCCM, 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.

Synchronizing OMIMSSC console extension with enrolled SCVMM

You can synchronize all Dell EMC 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 of the servers after synchronization.

Consider the following points before synchronizing OMIMSSC with SCVMM:

- Synchronization uses the servers' default iDRAC credential profile details.
- If the host server's Baseboard Management Controller (BMC) is not configured with the iDRAC IP address, 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 R2 supports numerous hosts in the environment, due to which synchronization is a long running task. Synchronization occurs as follows:
  - Hosts listed in the SCVMM environment are added to the **Hosts** tab in OMIMSSC Appliance.
  - If a server is listed as an unassigned server and manually added to SCVMM, then after synchronization, the server is added in to the **Hosts** tab of the OMIMSSC Appliance.
  - If a host server belongs to a Hyper-V cluster, then the cluster details are available in the **Hosts** tab. The host server is added or moved to the cluster update group and you can view this information in **Maintenance Center** page.
  - If a host is a modular server, then the service tag of the chassis containing the modular server is added to the **Hosts** tab. If the modular server does not belong to a Hyper-V cluster, the host server is added or moved in to the chassis update group and you can view this information in the **Maintenance Center** page.
  - Any changes to the host inventory details such as hostname, iDRAC IP address, memory, cluster membership, and so on are updated in the **Hosts** tab.
  - If a default update source is provided, then the firmware inventory is compared against the update source, and the latest information is added to the update group.

Synchronizing with enrolled MSSC

In OMIMSSC, click **Configuration and Deployment**, and then click **Synchronize with OMIMSSC** to synchronize all the hosts 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.

About this task

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

To resynchronize servers with credential profile issues:

Steps

1. In OMIMSSC, click **Configuration and Deployment** and then click **Resolve Sync Errors**.
2. Select the servers for resyncronization, 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.

Deleting servers from OMIMSSC

About this task

After you delete a server, the consumed license is relinquished.

You can delete a server 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.

Steps

1. In the OMIMSSC console, click **Configuration and deployment**:
   - 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**.

Launching iDRAC console

In **Configuration and Deployment**, under the **Unassigned Servers** or **Hosts** tab, click the **iDRAC IP** address of the server.

ⓘ NOTE: **If you use Windows 2012 OS and iDRAC 2.40.40.40 or later firmware version, enable support for TLS 1.1 and later based on the web browser to launch the iDRAC console.**

9

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 store. If you are unable to download your license key(s), contact Dell Support by going to www.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
- Enforcement
- Importing license in to OMIMSSC
- Viewing license details

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 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 store. 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

About this task

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

Steps

1. In 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.

Operational Template

Operational Template deploys operating systems and updates firmware versions on PowerEdge servers within MSSC environment .

You can capture the complete server configuration from a reference server, and then configure the hardware configurations, set firmware update attributes and OS parameters in an Operational Template and deploy this template across servers. Also, you can check the server compliance status against an assigned operational template and view the differences in a summary page. For information about reference server, see About reference server configuration.

The following table lists all the features that operational template supports:

Table 4. Functionality of OMIMSSC

Component	Configuration and deployment	Firmware update	View inventory	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	—

Consider the following points before deploying an Operational Template:

- If you select any of the hardware component for configuration (BIOS, RAID NIC/CNA, FC or iDRAC), ensure that you select servers of the same model.
- If you select firmware component, you can update the firmware across any servers.

Topics:

- Preparing for deployment
- Managing Operational Template

Preparing for deployment

Before deploying an Operational Template create a WinPE image, task sequence and an Operational Template.

Creating WinPE ISO image

A unique job name is assigned to each Windows Preinstallation Environment (WinPE) update. A PreExecution Environment (PXE) server is required for creating a WinPE ISO image. A WinPE ISO is created from the WinPE image and Dell OpenManage Deployment Toolkit (DTK). Once a WinPE ISO image is created, stop the PXE server. Ensure that relevant operating system-related driver packs are installed in

Lifecycle Controller. While using the latest version of DTK for creating a WinPE ISO image, use the WinPE version of the DTK files. DTK file contains the necessary firmware versions required for servers on which you are deploying the operating systems.

Prerequisites

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

Steps

1 Add the PXE server to the OMIMSSC Appliance.

2 After adding the PXE server, copy the boot.wim file from the PXE server to OMIMSSC IG for the SCVMM share WIM folder. The boot.wim is present in the following path: C:\RemoteInstall\DCMgr\Boot\Windows\Images

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

Extracting DTK drivers

About this task

DTK is a self-extracting executable file.

To work with DTK:

Steps

1 Double click the DTK executable file.

2 To extract the DTK drivers, select the folder, for example C:\DTK501.

3 Copy the extracted DTK folder to the IG's DTK share folder. For example \\OMIMSSC IG Share\DTK\DTK501

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

Updating WinPE image

1 In OMIMSSC, select **WinPE Update**, under **Image Source**, for **Custom WinPE Image Path**, provide the WinPE image path.

   For example, \\OMIMSSC IG Share\WIM\boot.wim.

2 Under **DTK Path**, for **DTK Drivers Path**, provide the location for the Dell Deployment Toolkit drivers.

   For example, \\OMIMSSC IG Share\DTK\DTK501

3 Provide either of the files for:

   - Provide WIM file name for SCCM.
   - Provide ISO file name for SCVMM.

4 To view the job list, select **Go to the Job List**.

   A unique job name is assigned to each Windows Preinstallation Environment (WinPE) update.

5 Click **Update**.

   WinPE ISO with the name provided in the preceding step is created under \\OMIMSSC IG Share\ISO.

Task sequence

Task sequence is used to capture the operating system image, or deploy an operating system on SCCM console.

Before creating Operational Template, it is recommended 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 Server discovery.

- 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.**

Creating a task sequence

You can create a task sequence in two ways which will be used for server configurations:

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

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

Creating Dell specific task sequence

About this task

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

Steps

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 **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**, 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

About this task

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

Steps

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.**

Creating Lifecycle Controller boot media

About this task

Create a zero-touch deployment boot media from your task sequence media, using this feature.

ⓘ NOTE: **This feature is applicable only for the OMIMSSC console extension for SCCM.**

Steps

1. Launch OMIMSSC, and then click **Boot Media Creation**.
2. In **Image Source** provide the ISO file that contains the operating system image.

   For more information, see Creating a task sequence media bootable ISO.
3. In **Output File**, provide the name of the ISO file, which is an unattended ISO file.
4. (Optional) to navigate to the **Jobs and logs** page after the job has started, select the **Go to the Job List** check box.
5. Click **Update** to save the output file in ISO share.

Setting a default share location for the Lifecycle Controller boot media

About this task

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

Steps

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.
> - OMIMSSC: OMIMSSC does not support the Standalone Media method to create Task Sequence Media.

2 From the **Task Sequence Media Wizard**, select **Bootable Media** 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 appears with the task sequence media information.

9 Click **Next**.

The progress bar is displayed.

10 On completion, close the wizard.

For working with deploying non-Windows operating systems

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

- Non-Windows 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 disk is available on the target system.
- After deploying ESXi OS the server is moved to **Managed Lifecycle Controller (ESXi)**collection in SCCM.
- After deploying any flavor of non-windows OS, 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.

Managing Operational Template

You can create, edit, and delete an Operational Template in OMIMSSC.

Creating Operational Template

Prerequisites

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

- Discover a reference server by using the **Discovery** page. For more information, see Discovering servers using manual discovery.
- (Optional) Create an update source. For more information, see Creating update source.

- (Optional) In OMIMSSC for SCCM:
  - Create a task sequence.

    For more information, see Creating task sequence.
  - For non-Windows OS deployment, have a device type credential profile. For more information, see Creating credential profile.
  - Create an unattended boot media. For more information, see Creating LC boot media.
- (Optional) In OMIMSSC for SCVMM:
  - 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.

About this task

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 for other PowerEdge homogenous servers.

Steps

1 In OMIMSSC, do any of the following to open 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 Provide a name and description for the template. Also, provide the IP address of the reference server, and then click **Next**.

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

3 In **Server 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
- Operating system—select either Windows, or ESXi, or RHEL

4 (Optional) edit the values for the available attributes, if necessary.

5 Select the check box against each component as only the selected components configuration of selected components is applied when the Operational Template is applied on all the configurations that are captured.

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

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

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

Windows OS component for OMIMSSC console extension for SCCM

About this task

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

Steps

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 created on vFlash must be ISOIMG.**

3 (Optional) to use the image present in the network share if the image present in vFlash is corrupt select the **Use Network ISO as Fallback** option.

4 Provide an LC boot media image file, and (optional) use **Enable LC Drivers Injection**. For more information about creating LC boot media image, see the Create LC boot media.

5 Select the drivers required for the OS.

Windows component for OMIMSSC console extension for SCVMM

About this task

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

Steps

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

> ⓘ NOTE: **Host Name, and Server Management NIC are always pool values.**

If you select **Server IP from** as **Static**, 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

About this task

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

Steps

Select a nonwindows OS, OS version, type of share folder, ISO file name, location of the ISO file and the password for the root account of the OS.

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

Host name is a pool value and if you disable DHCP option, 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 OS deployment.**

Viewing Operational Template

To view Operational Template templates:

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

Editing Operational Template

About this task

You can edit an Operational Template to modify the update source, hardware configurations, and operating system components of the reference server.

ⓘ **NOTE: Some attributes may depend on other attributes values. If these attributes are not updated, then applying hardware configuration may fail. Hence, it is recommended to not edit the reference configuration.**

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

Steps

1 Select the template you want to modify and click **Edit**.

The Operational Template page is displayed.

2 Edit the name and description of the template (if required), and then click **Next**.

3 To view the available attributes and their values in **Server Components**, click a component.

4 Modify the values of the available attributes if necessary.

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

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

5 For the OS component, perform either of the following tasks depending on your requirement:

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

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

Windows component for OMIMSSC console extension for SCCM

While editing Operational Template, perform the following steps mentioned in Windows OS component for OMIMSSC console extension for SCCM.

Windows component for OMIMSSC console extension for SCVMM

While editing Operational Template, perform the following steps mentioned in Windows OS component for OMIMSSC console extension for SCVMM.

Non-Windows component for OMIMSSC console extensions

While editing Operational Template, perform the following steps mentioned in Non-Windows OS component for OMIMSSC console extensions.

Deleting Operational Template

To delete an Operational Template, perform the following steps:

About this task

Before deleting an Operational Template, ensure that:

- The selected Operational Template is not associated with any server. If it is associated with a server, then, unassign the template and then delete the template.
- No jobs associated with Operational Template are running.

Steps

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

Assigning Operational Template and running Operational Template compliance

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.

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

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

   If the server is compliant to the template, then a **green** color tick mark is displayed.

   If the server is noncompliant to the template, only then you can view a summary report by clicking the template name link only if the servers are not complaint. The **Operational Template Compliance-Summary Report** page displays a summary report of the differences between the template and server configurations.

   To view a detailed report, perform the following steps:

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

Deploying Operational Template

About this task

You can deploy Windows and non-Windows OS—ESXi and RHEL.

> **NOTE: Download and install appropriate drivers from Dell.com/support if a yellow bang appears under Device Manager after you deploy Windows 2016 OS on 12th generation of the PowerEdge servers.**

Steps

1 In OMIMSSC, click **Configuration and Deployment**. 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.

2 (Optional) To export all the attributes marked as pool values in the selected template to a .CSV file, click **Export Pool Attributes**, else, go to step 3.

> ⓘ NOTE: **Before exporting the pool values, add the IP address of the server where the OMIMSSC console extensions is installed, to the local intranet site. For more information about adding the IP address in IE browser, see Browser settings.**

> ⓘ NOTE: **If you have exported the pool values, provide all values for all the attributes marked as pool values in the .CSV file and save the file. In Attribute Value Pool, select this file to import it.**

> ⓘ 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.**

> ⓘ NOTE: **Download and install appropriate drivers from Dell.com/support if a yellow bang appears under Device Manager after you deploy Windows 2016 OS on 12th generation of the PowerEdge servers.**

3 Provide a unique job name, description for the job, and click **Deploy**. To view the jobs, **Go to the Job List**.

Unassigning Operational Template

1 In OMIMSSC , click **Configuration and deployment**.

2 Select the servers to unassign the template from, and then click **Assign Operational Template and Run Compliance**.

The **Assign Operational Template and Run Compliance** page is displayed.

3 Select **Unassign** from Operational Template drop-down menu, and click **Assign**.

Integration with Dell Repository Manager(DRM)

OMIMSSC is integrated with DRM version 2.2 onwards providing the server inventory information of the existing servers from the OMIMSSC Appliance to DRM. By using the inventory information, you can create a custom repository in DRM and set it as an update source in OMIMSSC Appliance for performing firmware update jobs on the servers, or group of servers. For more information about creating a repository in DRM, see *Dell Repository Manager* documents.

About this task

ⓘ NOTE: **After upgrading OMIMSSC, reintegrate DRM with OMIMSSC Appliance to view the latest information about servers.**

To create a repository for the OMIMSSC Appliance by using DRM:

Steps

1 Open the **Dell Repository Manager Data Center** version.

2 Click **My Repositories**, click **New** and then click **Dell Console Integration**.

3 Enter the **URL (Rest API)** in the following format: `https:// IP address of appliance/genericconsolerepository/` and then click **Next**.

4 Provide the **UserName** and **Password** that was used in OMIMSSC Appliance, click **Ok**, and then click **Ok**.

12

Maintenance

Using **Maintenance Center** page you can export server inventory, and schedule jobs for upgrading the servers, recovering servers to an earlier state by exporting its earlier configuration, applying the same configurations as that of the old component on replaced components, and exporting LC logs for troubleshooting.

Topics:

- About firmware updates
- Recovery
- Applying firmware and configuration settings
- Collecting LC logs
- Exporting inventory

About firmware updates

You can maintain up-to-date firmware versions of Dell EMC server components as per the recommendations. Create update sources, and custom update groups, or use the predefined update groups to do the firmware update. You can create, and schedule jobs for firmware updates, and schedule notifications to receive alerts when new catalogs are available at update source. A comparison report for the existing firmware version and the baseline version is provided. Based on this information, you can create an inventory file. Also, you can filter the information based on the type of updates, server components, and server models. You can perform updates only on servers whose hardware is compatible because the iDRAC updates are available only for the minimum supported version and later.

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

OMIMSSC provides the following update actions in the **Maintenance center** page:

- Downgrade—there is an earlier version available at update source and you can downgrade the firmware to this version.
- No Action Required—the firmware version is at the same level as the one in the repository.
- No Update Available—no firmware updates are available for the component.
- Upgrade - Optional—updates consist of new features or any specific configuration upgrades that are optional.
- Upgrade - Urgent—critical updates used for resolving security, performance, or break-fix situations in components such as BIOS, and so on, are available.
- Upgrade - Recommended—updates carry bug fixes or any feature enhancements in the OMIMSSC. Also, compatibility fixes with other firmware updates are included.

OMIMSSC provides the following methods to perform firmware updates:

- **Update using DRM repository**—export the inventory information of the discovered servers from Appliance to prepare a repository in DRM. For information about exporting the inventory information, see the Exporting inventory.
  - After creating a repository in DRM, select the relevant servers and initiate an update on the servers. Consider other factors such as testing on test environment, security updates, application recommendations, Dell advisories, and so on, to prepare the required updates. For more information about creating a repository, see the *Dell Repository Manager* documents available at **Dell.com/support/home**.
- **Update using FTP or HTTP**—update any specific component to the latest update provided on the FTP or HTTP site. Dell IT prepares a repository at a quarterly cadence.

- Integration with Dell Online Catalog—connect to Dell FTP and download the catalog file in the cache directory if it is an FTP update source, or connect to `downloads.dell.com` if it is an HTTP update source, and then make it as a reference inventory.
- View the comparison report against the update source, select the relevant servers or server components, and then initiate an update on the servers.

- **Referencing firmware inventory and comparison**—create a reference inventory file that contains the firmware inventory of the selected servers or groups of servers. Later, you can compare the inventory information of servers present in the Appliance against the saved reference inventory file. The reference server inventory file contains inventory information from a single server of same type or model, or can have multiple servers of different types or models.

Applying updates on servers

Prerequisites

Before you apply updates on servers, ensure that perform the following conditions are met:

- To perform updates on servers, an update source is available on the Dell online FTP or HTTP site, local FTP or HTTP site, or Dell Repository Manager (DRM).
- iDRAC job queue is cleared before applying the updates, on the servers where the updates are applied.
- IG user has local administrator privileges on all the cluster nodes.
- For firmware repository creation, ensure that the FTP server is reachable from where the OMIMSSC is hosted, there are no network issues, and provide the right credentials while creating a firmware update job.

About this task

NOTE: You can apply firmware updates on a single component of a server, or to the entire environment.

NOTE: If there are no applicable upgrades or downgrades for a server or a group of servers, performing a firmware update on the servers cause no action on the servers.

NOTE: When you are updating component level information, if the existing firmware version is same as the firmware version at the update source, then there is no action on that component.

NOTE: You can apply immediate updates or schedule the updates on servers or on a group of servers by creating firmware update jobs. The jobs created for updates are listed under the Jobs and Logs Center page.

NOTE: You cannot update the CMC firmware directly from the OMIMSSC Appliance; however, you can update the firmware of the modular server present in CMC. For updating CMC firmware, see *Updating CMC firmware* section in *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide*. For updating CMC firmware in VRTX, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide*, and for updating CMC firmware in FX2, see *Updating firmware* section in *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide*.

NOTE: You can downgrade the firmware version to a suggested version by selecting Allow Downgrade. If this option is not selected, then there is no action on the component that requires a firmware downgrade.

Steps

1. In OMIMSSC, click **Maintenance Center**, select the server or server group and an update source, and then click **Run Update**.
2. In **Update Details**, provide the firmware update job name and description.
3. In **Schedule Update**, select one of the following:
   - **Run Now**—to apply the updates now.
   - Select a date and time to schedule a firmware update in future.
4. Select an update method that can be either **Agent-free Update**, or **Agent-free Staged Update**, and then click **Finish**.
   - **Agent-free staged updates**—the firmware that is directly applicable and do not require a system restart are applied immediately. The remaining updates are applied during system restart. The updates are performed through iDRAC. The OMIMSSC Appliance assumes that the update is successful when the iDRAC reports that the update is successful. The OMIMSSC Appliance does not interact with the server after applying updates. The entire update job fails if the operation fails on even one server.
   - **Agent-free updates**—the firmware update is out-of-band update with immediate restart if necessary.

ⓘ NOTE: **Updates for cluster update group happen through cluster update coordinator that is present on the same system where the IG is installed. 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, the OMIMSSC Appliance interacts with iDRAC for status of the job and provides status updates in the Jobs and Logs page of the Admin Portal. Sometimes iDRAC does not provide any status updates on the jobs tracked by the OMIMSSC Appliance. OMIMSSC Appliance waits for maximum 6 hours, and if there is no response from the iDRAC, then the firmware update job status is considered as failed.**

Updates using CAU

Updates on servers happen through cluster update coordinator which is present on the same system where IG is installed and not through iDRAC. The updates are not staged and are applied immediately. Using CAU, you can minimize any disruption or server downtime allowing 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 Cluster Readiness report of the following:

- Connectivity to update source.
- Availability of failover clusters.
- Ensure that Windows Server 2012 or Windows Server 2012 R2 or Windows 2016 OS 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.
- Enablement of a firewall rule that allows remote shutdown on each node in the failover cluster.
- Cluster group should have minimum of two nodes.
- Check for cluster update readiness. For more information about CAU, see Requirements and Best Practices for Cluster—aware Updating section at Technet.microsoft.com.
- For a component level update, expand the server groups to its component level, and click **Run Update**.
- When performing a firmware update for 11th generation of the PowerEdge servers, you cannot upgrade the Power Supply Unit (PSU) firmware versions.

ⓘ NOTE: **Ensure that there are no major errors and warnings in the report for applying the CAU method.**

For information about applying the updates, see Run update.

Polling and notification

You can configure polling notifications to receive alerts when there are new catalogs available at the predefined, and user selected default update source. The color of the notification bell is changed to orange color when there is a new catalog file available at the update source. To replace the locally cached catalog available at the update source, click the bell icon. After the old catalogs are replaced by the latest catalogs, the bell color changes to green.

About this task

To set the polling frequency:

Steps

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

2 Select how frequently the polling should happen:

   - **Never**—by default this option is selected. Select to receive updates about new catalogs available at update source only once for the scheduled time.
   - **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.

Update source overview

Update source enables you to select and apply updates from Dell's update sources. You can create, view, and manage the update sources. The types of update sources supported are DRM repository, FTP, and HTTP. You can create a DRM, HTTP, or FTP update source and set it as a default update source.

Update sources have the catalog files that contain Dell updates (BIOS, firmware, application, drivers, and driver packs) and carry the self-contained executable file called Dell Update Packages (DUPs).

You can compare the inventory information available at the update source against the inventory information of a selected server or group of servers inventory information and create a baseline version. You can also change the update source and compare the inventory information of the servers or group of servers against the version information available from the selected update source.

It is recommended that you upgrade to the latest firmware to use security, bug fixes, and new feature requests. Dell publishes the following updates through PDK catalogs posted on Dell FTP at a quarterly cadence:

- Server BIOS and firmware
- Dell certified operating system driver packs (for operating system deployment)

Predefined and default update source

DELL ONLINE CATALOG is a predefined update source of type FTP available in OMIMSSC Appliance after a fresh installation or upgrade. You cannot delete, or change the name of a predefined update source.

DELL ONLINE HTTP CATALOG is a default update source available in OMIMSSC Appliance after a fresh installation or upgrade. You cannot delete or change the name of this default update source. However, you can create another update source and mark it as a default update source.

ⓘ NOTE: **After installing OMIMSSC, add the proxy details for DELL ONLINE CATALOG and, DELL ONLINE HTTP CATALOG update source and save it.**

Test connection

Use **Test Connection** to verify if the location of the update source is reachable by using the credentials mentioned while creating the update source.

You can create an update source, only after confirming that the catalog location is accessible through the provided credentials.

Setting up local FTP

To set up your 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.xml.gz file from online FTP and extract 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

1 Create a folder structure in your local HTTP that is an exact replica of downloads.dell.com.
2 Download the catalog.xml.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**.

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 is displayed.

Creating update source

Prerequisites

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

Steps

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.**

- 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 only view a comparison report by using Inventory Output files as an update source, that compares inventory information of one server with all other servers.**

4 In **Location**, provide the URL of the update source of an FTP or HTTP 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 required 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

About this task

While modifying an update source, ensure that you note and remember the following points:

- 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 continue with 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 recreate the update source.

Steps

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

Deleting update source

About this task

You cannot delete an update source when:

- The update source is a predefined update source that is **Dell Online Catalog** and **DELL ONLINE HTTP CATALOG**.
- The update source is used by an in-progress, or a scheduled job.
- The update source is a default update source.

Steps

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

Update groups

Update groups are a group of servers that require similar update management. There are two types of update groups available:

- Predefined update groups—you can only view the servers in the group.

  You cannot create, modify, or delete the predefined update groups manually.
- Custom update groups—you can create, and maintain servers in the group.

ⓘ **NOTE: All server groups that exist in SCVMM are listed in OMIMSSC since it is not user-specific. Make sure you have access to perform any operations on those servers.**

Predefined update groups

The description and behavior of the predefined update groups are as follows:

Generic update groups—this group consists of hosts and unassigned servers that are updated in a single session.

All update groups—this group consists of all the server groups. Any group present in the OMIMSSC is a member of the all update groups. This group is of the type generic update group.

Default unassigned server update group—this group consists of all the unassigned servers that are not part of any other group. This group is of the type generic update group. The servers are added to the default unassigned server update group after:

- A fresh discovery or rediscovery of bare metal servers.
- A synchronization or resynchronization, after it is deleted from SCVMM but present in the OMIMSSC Appliance.

Cluster update group—this group consists of the Windows Server Failover clusters. If a modular server belongs to a cluster, then it is added to the cluster update group. If a 12th or 13th generation of Dell PowerEdge modular server is part of cluster, then the CMC information is also added in the inventory in the **Maintenance Center** page.

To know about the cluster update group to which a server belongs to, see the **Configutation and Deployment** page where the host name and cluster FQDN is displayed for all the servers listed in OMIMSSC.

Host update group—this group consists of host servers, and updates are applied in a single session, wherein, a single session is updating all servers within the group at once.

Default host update group—this group consists of all the discovered hosts that are not part of any other update group. This group is of the type host update group.

Chassis update group—modular servers belonging to a chassis and not part of any cluster group are classified as chassis update group. 12th or 13th generation of PowerEdge servers are discovered along with their CMC information. By default, a group is created with the naming format, Chassis-Service-tag-of-Chassis-Group. For example, `Chassis-GJDC4BS-Group`. If a modular server is deleted from a cluster update group, 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.

Default Non-Windows Host Update group—this group consists of servers having non-windows OS.

Custom update groups

This group allows you to create, modify, and delete update groups. However, you can add a server into a custom update group only from **Default unassigned update groups** and the **Default host update groups**. After you add a server into a custom update group, the server is removed from the predefined update group and this server is available only in the custom update group. To add the servers in custom update group, search for the required servers using their service tag.

ⓘ NOTE: **If a server is deleted from MSSC, and you synchronize OMIMSSC with enrolled MSSC, the server is removed from the custom update group and is moved to the appropriate predefined group.**

Updating methods

You can apply updates on selected server groups whose hardware is compatible with OMIMSSC.

- You can perform the following updates on server groups:
  - **Agent-free staged updates**—is staging of firmware updates. The firmware updates that are immediately applicable and that do not require a restart are applied immediately. The remaining updates that require a system restart are applied at the time of restarting the server. Updates are performed in batches at the scheduled time by using iDRAC. The batch size is determined when the update is happening. To check if all the updates are applied, refresh the inventory . The entire update job fails if the operation fails on even one server.
  - **Agent-free updates**—is out of band update with immediate server restart.
  - **Cluster-Aware Updating (CAU)**—automates the update process by using Windows CAU feature on cluster update groups to maintain server's availability. For more information about CAU, see Updates using CAU.

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 and 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**.

Modifying custom update groups

About this task

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:
  a Remove the server from an existing custom update group. It is then automatically added into the predefined update group.
  b Edit the custom group to add the server into, and then search for the server by using the service tag.

Steps

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

About this task

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 scheduled, in-progress, or waiting.
- 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.
- Delete the scheduled jobs associated with a custom update group before deleting the server group.

Steps

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.

Applying filters

Apply filters to view selected information in the comparison report.

About this task

The OMIMSSC Appliance 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 filters:

Steps

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

Next steps

To remove filters:

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

Viewing and refreshing firmware inventory

You can view and refresh the firmware inventory of servers or a specific group of servers.

You can view comparison report of a server or chassis inventory against a selected update source. You can change the update source, and view the comparison report of inventory information of the selected servers, server groups, or chassis against the changed update source.

You can refresh the firmware inventory for a server, a group of servers, or chassis to view the latest information. When you refresh the component information of a server, the complete inventory information of the server is updated.

ⓘ **NOTE: At the time of creation, a local copy of the catalog file is cached in OMIMSSC. Hence, update the catalog file to display the latest comparison report. To update the catalog file, edit the update source and save it, or delete and recreate the update source.**

ⓘ **NOTE: Server details such as Driver Pack Version and Drivers Available For OS are not updated in Dell Out of Band Controllers (OOB) properties of the server in SCCM console on refreshing the inventory. To update the OOB page, synchronize OMIMSSC with SCCM.**

ⓘ **NOTE: When you upgrade to this version of OMIMSSC, the latest information is not shown for servers discovered in prior versions. For the latest server information and correct comparison report, rediscover the servers.**

To view or refresh firmware inventory for a server or a group of servers:

1. In **OMIMSSC**, under **Maintenance Center** select an update group from **Select Update Group**.
2. (Optional) To change the update source, select an update source from **Select Update Source**.
3. To view firmware information of the current version, baseline version, and update action recommended by OMIMSSC Appliance, expand the server group from **Device Group/Servers** to the server level, and then to the component level.

    ⓘ **NOTE:**

    When viewing component level information, the NIC-related information for the 11th generation of the PowerEdge server is displayed as follows:

    - After applying filters based on **Nature of Update** as **Urgent**, a report with the components only with urgent updates are displayed. If this report is exported, then components with downgrade action which in turn have critical update is also exported.
    - When there are multiple network interfaces available in a single NIC card, there is only one entry for all the interfaces in the **Component Information** list. Once the firmware update is applied, all the NIC cards are upgraded.
    - When a NIC card is added along with the existing cards, the newly added NIC card is listed as another instance in the **Component Information** list. Once the firmware update is applied, all the NIC cards are upgraded.
4. Select the server or group of servers that you want to refresh, and then click **Refresh Inventory**.

Recovery

You can save the server profile in protection vault by exporting the profile and importing the profile to the same server to reinstate it to an earlier state.

Protection vault

Protection vault is a secure location where you can export and import server profiles for a server or a 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 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.

Creating protection vault

Prerequisites

Ensure that vault location is accessible.

Steps

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

About this task

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

Steps

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

Deleting protection vault

About this task

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.

Steps

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

Exporting server profiles

You can 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. The 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 a later date. Also, you can select a relevant recurrence option as to how frequently the server profiles are exported. 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.

Prerequisites

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

About this task

ⓘ **NOTE: Ensure that the Automatic Backup job in iDRAC is not scheduled at the same time.**

ⓘ **NOTE: You cannot export server profiles after applying the filters. To export server profiles, clear all the applied filters.**

ⓘ **NOTE: To export server profiles, you must have the iDRAC Enterprise license.**

ⓘ **NOTE: Before exporting the server profile, make sure 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.**

Steps

1. In OMIMSSC, click **Maintenance Center**. Select the servers' whose profiles you want to export and then click **Export Server Profile**.
2. In the **Export Server Profile**, window, 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. In such cases, you can replace the server profile on that server, or group of servers by importing a previously exported server profile of that server or group of servers.

About this task

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.

Steps

1. In OMIMSSC, under **Maintenance Center**, select the servers' whose profiles you want to import, and click **Import Server Profile**.
2. Provide the details, select the **Import Server Profile Type** you want.

   ⓘ **NOTE: 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

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 your system after replacing the component.

About this task

To set the parameters for part replacement:

Steps

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

About this task

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

There are two options to collect LC logs:

- Active LC logs—these are the recent LC log files. You can view, search, and export these log files to the Appliance. You can schedule a job to collect the LC logs to Appliance or a network share. Also, you can save a backup of the log file in the network share.

- Complete LC logs—these logs contain active and archived LC log files. They are large and hence compressed to `.gz` format and exported to the specified location on a CIFS network share.

Steps

1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, 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)**—exports the active and archived LC logs to a CIFS network share by providing the Windows credentials.

    For example, 201607201030010597.xml.gz is the LC file name, which includes the date and time of the file when it was created.

    ⓘ NOTE: **Ensure that the shared folder has enough space to save the complete LC logs since these are large files.**

    ⓘ NOTE: **Exporting complete LC logs is not supported for 11th generation of the PowerEdge servers.**

    ⓘ NOTE: **LC logs are saved in the following format: `<YYYYMMDDHHMMSSSSS>.<file format>`**

  - **Export Active Logs (Run now)**—select to export the active logs immediately to Appliance.

    - (Optional) Enable the **Back up LC logs on the network share** option to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

      ⓘ NOTE: **Ensure to update to the latest versions of iDRAC and LC before exporting active LC logs for 11th generation of the PowerEdge servers.**

  - **Schedule LC Log Collection**—select a date, time, and frequency to export the active LC logs.

    - (Optional) Enable the **Back up LC logs on the network share** option to save a backup of the LC logs on CIFS network share by providing the Windows credentials.

    The available options for scheduling frequency to determine how often you want to collect the LC logs are:

    - **Never**—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 once a week at the scheduled time.
    - **Once every 4 weeks**—select to export the LC logs after every four weeks at a scheduled time.

    ⓘ NOTE: **The exported LC log file is saved within a folder name of that particular server's service tag.**

Viewing LC logs

You can view all the active LC logs, search for detailed description, and download the logs in CSV format using View LC logs feature.

Prerequisites

Set the browser settings as mentioned in the Browser settings.

Steps

1 In OMIMSSC, click **Maintenance Center**. Select a server or a group of servers, and then 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.**

ⓘ **NOTE: Before downloading the LC logs, add Appliance in the Local intranet site.**

To add Appliance in the **Local intranet** site in **Internet Explorer**:

a Launch a browser, click **Tools**, and then click **Internet Options**.

b Click **Security** > **Local intranet** > **Sites**.

The **Local intranet** page is displayed.

c Click **Advanced**, type `Appliance URL`, and then click **Add**.

File description

Use this window 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

In OMIMSSC, you can 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.

Prerequisites

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

Set the browser settings as mentioned in Browser settings.

About this task

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

Steps

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 exported 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.

Next steps

After exporting the XML file, to create a repository in DRM, perform the following steps:

1 Click **My Repositories** > **New** > **Dell Modular Chassis inventory**.

2 Provide a name and description in the **Base Repository** section, and click **Next**.

3 To select the inventory file exported from Appliance click **Browse** in the **Modular Chassis Inventory** section, and then click **Next**.

For more information on creating a repository, see the *Dell Repository Manager* documents available at **Dell.com/support/home**.

13

Viewing information in OMIMSSC

You can view all information about the activities initiated in OMIMSSC along with a job's progress status, and its subtask through the **Jobs and logs center** page. Also, you can filter and view jobs for a particular category. You can view the jobs from the OMIMSSC Admin Portal and OMIMSSC console extension.

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

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

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

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

The various states of jobs defined in OMIMSSC Appliance are:

- Canceled—job has been manually canceled by you, or when OMIMSSC Appliance restarts.
- Successful—job has been successfully completed.
- Failed—job is not successful.
- In Progress—job is running.
- Scheduled—job has been scheduled for a future time.

  ⓘ **NOTE: If multiple jobs are submitted at the same time to the same server, the jobs fail. Hence, ensure that you schedule the jobs at different times.**
- Waiting—job is in a queue to start running.
- Recurring Schedule—job recurring after a fixed interval of time.

Topics:

- Viewing jobs
- Managing jobs

Viewing jobs

About this task

You can view all jobs created in OMIMSSC along with their status information.

Steps

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 the job to view all the servers included in the 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 category of jobs and you can view it is status in **Status** column.

Managing jobs

Prerequisites

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

Steps

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**.

14

Troubleshooting

Topics:

- Deploy option not visible in task sequence
- Duplicate VRTX chassis group gets created
- Empty cluster update group does not get deleted during autodiscovery or synchronization
- Failure of creation of update source
- Failure of firmware update because of job queue being full
- Failure of firmware update on cluster update group
- Failure of firmware update on 11th generation of servers
- Failure of firmware update while using DRM update source
- Failure of scheduled job on an update group
- Failure to apply Operational Template
- Failure to access CIFS share using hostname
- Failure to connect to FTP using system default update source
- Failure to create a repository during a firmware update
- Failure to delete a custom update group
- Failure to display Jobs and Logs
- Failure to export LC logs in CSV format
- Failure to export server profiles
- Failure to display Dell EMC logo in OMIMSSC Admin Portal
- Failure to view LC logs
- Firmware update on a few components irrespective of the selection
- Hypervisor deployment failure
- Hypervisor deployment failure due to driver files retained in library share
- Hypervisor deployment failure for 11th generation PowerEdge blade servers when using Active Directory
- Incorrect credentials during discovery
- IG installation issue while running multiple instances of the installer on the same server
- Importing server profile job gets timed out after two hours
- Latest inventory information is not displayed even after firmware update
- SCVMM error 21119 while adding servers to active directory

Deploy option not visible in task sequence

The **Deploy** option does not appear in an existing task sequence after uninstalling and reinstalling OMIMSSC console extension for SCCM.

As a work around, open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option appears 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.

Duplicate VRTX chassis group gets created

When modular servers that were previously in another chassis are added to a VRTX chassis and discovered, the modular servers carry previous chassis service tag information and create a duplicate VRTX chassis group in the Appliance.

To resolve, do the following:

1 Remove a modular server from one chassis, and add it in another chassis. For more information, see Server modules section in *Dell PowerEdge VRTX Enclosure Owner's Manual*.

2 Configure CMC. For more information, see Installing and Setting Up CMC in *Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX User's Guide*, available at dell.com/support /home.

After you do the preceding tasks, if there are duplicate chassis group entries, then 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.

Empty cluster update group does not get deleted during autodiscovery or synchronization

When a cluster group is discovered in the Appliance, 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 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 of firmware update because of job queue being full

Firmware update jobs submitted from the Appliance to iDRAC fail, and the Appliance 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 on deleting jobs in iDRAC, see iDRAC documentation at **dell.com/support/home**.

Failure of firmware update on cluster update group

After scheduling a firmware update job on a cluster update group, if the firmware update job fails for various reasons such as IG is unreachable, the cluster group becomes unresponsive, or the firmware update job was canceled in CAU for an in-progress job, the DUPs are downloaded and placed in each server cluster node belonging to the cluster group. All the DUP files are placed under the folder called Dell consuming memory.

As a workaround, delete all the files in Dell folder, and then schedule a firmware update job.

Failure of firmware update on 11th generation of servers

A firmware update job started on 11th generation of PowerEdge servers may fail due to incompatible versions of iDRAC and LC with the following error: `WSMan command failed to execute on server with iDRAC IP <IP address>`.

As a workaround, upgrade the iDRAC and LC to the latest versions and then start the firmware update job.

Failure of firmware update while using DRM update source

The 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, do 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.

Failure of scheduled job on an update group

After scheduling a job on an update group, if all the servers are moved out of the update group and there are no servers present in the update group then, the scheduled job fails.

As a workaround, cancel the scheduled job, add the servers to another update group, and then schedule a job on the update group.

Failure to apply Operational Template

After submitting the **Deploy** the Operational Template job 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 Template, then the job in iDRAC is successful. However, the status of this job in OMIMSSC is shown as unsuccessful/fail 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 template.

Failure to access CIFS share using hostname

The modular servers may not be 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.

Failure to connect to FTP using system default update source

After setting up and configuring, or upgrading the Appliance, trying to access the FTP site using system created update source **Dell Online Catalog** might fail if proxy credentials are required.

To access the FTP site using **Dell Online Catalog** as an update source edit, and add the proxy credentials.

Failure to create a repository during a firmware update

Creation of a repository may fail during a firmware update because of network issues, improper credentials, or server not reachable, and so on.

As a workaround, ensure that the FTP server is reachable from where the Appliance is hosted, there are no network issues, and provide the right credentials during a firmware update.

Failure to delete a custom update group

After scheduling a job on a server belonging to a custom update group, if the server is deleted from SCVMM and synchronization is done, the server is removed from the custom update group and is moved to the appropriate predefined group. You cannot delete such custom update groups, because it is associated with a scheduled job.

As a workaround, to delete this custom update group, delete the scheduled job from jobs page, and then delete the custom update group.

Failure to display Jobs and Logs

The **Jobs and Logs Center** is not displayed in OMIMSSC console extensions.

As a workaround, reenroll the console.

Failure to export LC logs in CSV format

When viewing LC logs, if you try to download the log files to CSV format the download operation fails.

As a workaround, add the Appliance FQDN in the browser under local intranet site. For information about adding the Appliance in local intranet, see Viewing LC logs section.

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.

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 Admin Portal URL to browser's favorite list.

Failure to view LC logs

After collecting the LC Logs, when you 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 more information, see iDRAC documentation available at dell.com/support.

Firmware update on a few components irrespective of the selection

Same components on identical servers get updated during a firmware update irrespective of the selection of components made on individual servers. This behavior is seen for 12th and 13th generation of PowerEdge servers with Enterprise license of iDRAC.

As a workaround, do one of the following:

- To prevent irrelevant updates on identical servers, apply common components on identical servers and then apply specific components separately on individual servers.
- Perform staged updates with planned outage times to accommodate the required firmware update.

Hypervisor deployment failure

Hypervisor deployment is failing and the activity log displays the following error: `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 either 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 anti-virus 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 is failing and the activity log displays the following error:

About this task

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information**: `Successfully deleted drivers from library share sttig.tejasqa.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:

Steps

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.

Now, you can deploy operating systems.

Hypervisor deployment failure for 11th generation PowerEdge blade servers when using Active Directory

Hypervisor deployment fails on the 11th generation PowerEdge blade servers when using the Active Directory user credentials. The 11th generation PowerEdge blade servers use the Intelligent Platform Management Interface (IPMI) protocol for communication. However, the IPMI standard is not supported for using credentials from the Active Directory setup.

About this task

As a workaround to deploy operating systems on these servers, use supported credential profiles.

Steps

Incorrect credentials during discovery

- 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 once the IP address is unblocked.
  - While discovering an 11th or 12th generation PowerEdge server with iDRAC versions prior to 2.10.10.10, if server discovery attempts fail due to incorrect credential profile details, then rediscover the server with the correct credential profile details.
  - For iDRAC versions prior to 2.10.10.10, blocking of IP addresses is configurable. For more information, see iDRAC documentation at **Dell.com/idracmanuals**. Based on your requirement, you can also disable blocking of IP addresses. And you can also check if the iDRAC.IPBlocking.BlockEnable feature is enabled in iDRAC.
  - 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.

IG installation issue while running multiple instances of the installer on the same server

After you start installing the IG, if you try running another instance of the IG, then an error message is displayed. After you click OK, you are prompted to save another IG MSI file.

As a workaround, do not save this file and continue with the first installation.

Importing server profile job gets timed out after two hours

After submitting the import server profile job in the Appliance, it may get timed out after two hours.

As a workaround, perform the following steps:

1. Press F2 and enter **BIOS Settings**.
2. Click **System Setup** and select **Miscellaneous Settings**.
3. Disable **F1/F2 Prompt on Error**.

After performing the following steps, schedule the export server profile job and use the same to complete the import server profile job successfully.

Latest inventory information is not displayed even after firmware update

Even though the firmware update job is complete on an 11th generation of PowerEdge server, in the Appliance, the inventory does not display the latest firmware versions.

In the Appliance, 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 in the Appliance, refresh the firmware inventory. Also, ensure to restart the server after applying agent-free staged update. For more information on refreshing the inventory, see Viewing and refreshing firmware inventory.

For more information on CSIOR, refer to the Troubleshooting section in the latest version of the *Dell Lifecycle Controller GUI User's Guide* available at **dell.com/support/home**.

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>.`

About this task

As a workaround, do the following:

Steps

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 Once the server is added in to SCVMM, rediscover the server in OMIMSSC console extension for SCVMM.

The server will be listed under the **Host** tab.

15

Appendix

16

Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — Dell.com/SoftwareSecurityManuals
- For Dell EMC OpenManage documents — Dell.com/OpenManageManuals
- For Dell EMC Remote Enterprise Systems Management documents — Dell.com/esmmanuals
- For iDRAC and Dell EMC Lifecycle Controller documents — Dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — Dell.com/OMConnectionsEnterpriseSystemsManagement
- For Dell EMC Serviceability Tools documents — Dell.com/ServiceabilityTools
- For Client Command Suite Systems Management documents — Dell.com/DellClientCommandSuiteManuals
-
  a Go to Dell.com/Support/Home.

  b Click **Choose from all products**.

  c From **All products** section, click **Software & Security**, and then click the required link from the following:

    - **Enterprise Systems Management**
    - **Remote Enterprise Systems Management**
    - **Serviceability Tools**
    - **Dell Client Command Suite**
    - **Connections Client Systems Management**

  d To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

Contacting Dell

Prerequisites

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

About this task

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

Steps

1 Go to **Dell.com/support.**

2 Select your support category.

3 Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.

4 Select the appropriate service or support link based on your need.