Dell EMC OpenManage Integration for Microsoft System Center Version 7.2 for System Center Configuration Manager and System Center Virtual Machine Manager

Best Practices 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.**

2019 - 09

Rev. A00

Contents

Resources required for managing OMIMSSC

Use this guide to check for required privileges and solve any problems encountered in OMIMSSC.

To troubleshoot any issues faced in OMIMSSC, ensure that you have the following resources:

- Read-only user's account details to login to OMIMSSC Appliance and perform various operations.

  For logging in as a read-only user from OMIMSSC Appliance VM, enter user name as `readonly` with the same password used to login to OMIMSSC Appliance VM.
- Log files having high level and complete details of the errors:
  - Activity logs—contains user specific, and high-level information about the jobs initiated in OMIMSSC, and status of jobs run in OMIMSSC. To view activity logs, go to **Jobs and Logs** page in OMIMSSC console extension.
  - Complete logs —contains Administrator-related logs, and multiple detailed logs specific to scenarios in OMIMSSC. To view the complete logs, go to **Jobs and Logs** page in **OMIMSSC Admin portal**, **Settings**, and then **Logs**.
  - LC Logs—contain server level information, detailed error messages on operations performed in OMIMSSC. To download and view the LC Logs, see *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

    NOTE: For troubleshooting individual devices from iDRAC or OpenManage Enterprise Module (OME-Modular) page, launch OMIMSSC, click Configuration and Deployment page, launch the respective view, and then click the device IP URL.

NOTE: SCVMM server Administrator user should not be an SCVMM service account.

NOTE: If you are upgrading from SC2012 VMM SP1 to SC2012 VMM R2, then upgrade to Windows PowerShell 4.0.

Verifying permissions for using OMIMSSC console extension for SCCM

After installing OMIMSSC, verify that the enrolled user has the following permissions:

1. On the system where OMIMSSC is installed, provide the **Write** permissions for the *<Configuration Manager Admin Console Install Dir>\XmlStorage\Extensions\DLCPlugin* folder using PowerShell commands.

   Complete the following prerequisites on the site server, and SMS provider server before installing OMIMSSC component:

   a) In PowerShell, run the command: `PSRemoting`.

      If the `PSRemoting` command is disabled, run enable the `PSRemoting` command using the following commands.

      1. Run the command: `Enable-PSRemoting`
      2. In the confirmation message, type `Y`.

   b) In PowerShell, run the command: `Get-ExecutionPolicy`.

      If the policy is not set to `RemoteSigned`, then set it to `RemoteSigned`using the following commands.

      1. Run the command: `Set-ExecutionPolicy RemoteSigned`.
      2. In the confirmation message, type `Y`.
2. Configure user access to Windows Management Instrumentation (WMI). For more information, see the Configuring user access to WMI.
3. Provide share and folder permissions to write files to the inboxes folder.

   To grant share and folder permissions to write files to the DDR inbox:

   a) From the Configuration Manager console, under **Administration**, grant the user permission to write to the **SMS_<sitecode>** share.

   b) Using **File Explorer**, go to the share location **SMS_<sitecode>** share, and then to the `ddm.box` folder. Grant full control to the domain user for the following folders:

      - **SMS_<sitecode>**
      - Inboxes
      - `ddm.box`

Topics:

- Configuring user access to WMI

Configuring user access to WMI

To configure user access to WMI remotely:

ⓘ **NOTE: Make sure that firewall of the system does not block the WMI connection.**

1. To access the Distributed Component Object Model (DCOM) remotely, provide permissions to the enrolled SCCM user.

   To grant user permissions for DCOM:

   a) Launch `dcomcnfg.exe`.

   b) From the left pane, in the **Component Services** console, expand **Computers**, right-click **My Computer**, and select **Properties**.

   c) On **COM Security**:

      - From **Access Permissions**, click **Edit Limits** and select **Remote Access**.
      - From **Launch and Activation Permission**, click **Edit Limits** and select **Local Launch**, **Remote Launch**, and **Remote Activation**.
2. To access the DCOM Config Windows Management and Instrumentation (WMI) components, provide user permissions to the enrolled user.

   To grant user permissions for DCOM Config WMI:

a) Launch `dcomcnfg.exe`.

b) Expand **My Computer** > **DCOM Config**.

c) Right-click **Windows Management and Instrumentation**, and select **Properties**.

d) On **Security**, from **Launch and Activation Permission**, click **Edit** and select the **Remote Launch** and **Remote Activation** permissions.

3. Set the namespace security and grant permissions.

   To set namespace security and grant permissions:

   a) Launch `wmimgmt.msc`

   b) In **WMI Control** pane, right-click **WMI Control**, select **Properties**, and then select **Security**.

   c) Navigate to `ROOT\SMS Namespace`.

   d) Select the **Execute Methods**, **Provider Write**, **Enable Account**, and the **Remote Enable permissions**.

   e) Navigate to `Root\cimv2\DLCI`.

   f) Select the **Execute Methods**, **Provide Write**, **Enable Account**, and the **Remote Enable permissions** .
   Alternatively, the Configuration Manager user becomes a member of the **SMS_Admin** group, and you can grant **Remote Enable** to the existing permissions of the group.

3

Verifying PowerShell permissions for using OMIMSSC console extension for SCVMM

Check if the `PSRemoting` status is enabled and `ExecutionPolicy` is set to `RemoteSigned`. If the status is different then perform the following steps in PowerShell:

a) In PowerShell, run the command: `PSRemoting`.

   If the `PSRemoting` command is disabled, run enable the `PSRemoting` command using the following commands.

   1. Run the command: `Enable-PSRemoting`
   2. In the confirmation message, type `Y`.

b) In PowerShell, run the command: `Get-ExecutionPolicy`.

   If the policy is not set to `RemoteSigned`, then set it to `RemoteSigned`using the following commands.

   1. Run the command: `Set-ExecutionPolicy RemoteSigned`.
   2. In the confirmation message, type `Y`.

Install and upgrade scenarios in OMIMSSC

This section has all the troubleshooting information related to installing and upgrading OMIMSSC.

Verifying OMIMSSC Appliance VM configuration

To verify that the OMIMSSC Appliance VM is configured appropriately, select and then right-click the OMIMSSC Appliance VM, click **Settings**, and then perform the following tasks:

1. Check if the allocation of memory for the OMIMSSC Appliance is as per the requirement mentioned in the *Common requirements* section of *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*. Else provide the memory in **Startup RAM**, and click **Apply**.
2. Check if the processor count is as per the requirement mentioned in the *Common requirements* section of *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*. Else provide the number of processor counts in **Number of Virtual processors** count under **Processors**.
3. Check if the **Virtual hard disk** field under IDE Controller: **IDE Controller 0** > **Hard Drive** the **Virtual hard disk** referring to the **OMIMSSC—v7** file else, click **Browse** and navigate to the location where the VHD file is unzipped and select the **OMIMSSC—v7** file and click **Apply**.
4. Check if **Network Adapter** > **Virtual Switch** is connected to a physical NIC card, else configure the NIC card, and select the appropriate NIC card from the **Virtual Switch** drop-down menu and click **Apply**.

If the newly created virtual machine with the selected virtual hard disk of OMIMSSC Appliance fails to boot with any kernel panic exception, edit the virtual machine settings, and enable the dynamic memory option for this virtual machine.To enable the dynamic memory option for a virtual machine, perform the following tasks:

1. Right-click the OMIMSSC Appliance VM, click **Settings**, and then click **Memory**.
2. Under **Dynamic Memory**, select the **Enable Dynamic Memory** check box, and provide the details.

Topics:

Enrollment failure

If the test connection or enrollment fails, then you get an error message.

As a workaround, perform the following steps:

- Ping from OMIMSSC Appliance to enrolled SCCM or SCVMM server FQDN by logging in to OMIMSSC Appliance VM as a read-only user. If there is a response, then wait for some time and then continue with the enrollment.

  To launch the OMIMSSC Appliance VM as a read-only user, enter user name as `readonly` with the same password used to log into the OMIMSSC Appliance VM.
- Ensure that the SCCM or SCVMM server is running.
- The Microsoft account used to enroll the console should be a delegated admin or an administrator in System Center, and a local administrator for the System Center server.
- Specific for SCVMM users:

- Ensure that the SCVMM server is not registered with any other OMIMSSC Appliance. If you want to register the same SCVMM server with the OMIMSSC Appliance, then delete the **OMIMSSC Registration Profile** application profile from the SCVMM server.
- If you have applied SCVMM roll up update, then check the Indigo TCP port number of SCVMM console in registry `(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings)`. Use the same port number that was used to register SCVMM console. By default it is 8100.

Failure of test connection

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2` . When you try to enroll with the above domain user account, the test connection fails.

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

Failure to connect to OMIMSSC console extension for SCVMM

After enrolling and installing OMIMSSC console extension in SCVMM environment, when you try to launch OMIMSSC, the following error is displayed: `Connection to server failed`.

As a workaround, perform the following steps:

1. Add the OMIMSSC Appliance IP and FQDN into local intranet in SCVMM console, when you are launching OMIMSSC.
2. Add the OMIMSSC Appliance IP and FQDN in **Forward Lookup Zones** and **Reverse Lookup Zones** in DNS.
3. For further details, check if there are any error messages in `C:\ProgramData\VMMLogs\AdminConsole` file.

Error accessing console extension after updating SCVMM R2

After applying Update Rollup for SC2012 R2 VMM, if you try to open the already installed OMIMSSC console, SCVMM displays an error message for security reasons, and you cannot access the OMIMSSC console.

As a workaround, do the following:

1. Delete the folder at default path: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Restart SCVMM.
3. Remove the console extension, and then import the console extension as mentioned in *Importing OMIMSSC console extension for SCVMM* section of *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager Installation Guide*.

IP address not assigned to OMIMSSC Appliance

After creating and starting the OMIMSSC Appliance VM, the OMIMSSC Appliance IP address is not assigned or displayed.

As a workaround, check if the virtual switch is mapped to a physical switch, if the switch is configured correctly, and then connect to OMIMSSC Appliance.

SCVMM crashes while importing OMIMSSC console extension

SC2016 VMM RTM build 4.0.1662.0 Administrator console may crash when importing OMIMSSC console extension.

As a workaround, upgrade SCVMM using the 4094925 KB article available at `support.microsoft.com/kb/4094925`, and then import the OMIMSSC console extension.

Failed to login to OMIMSSC console extensions

After logging in to OMIMSSC console extensions with different credentials used to login to Microsoft console, the login activity fails with following error message: `Username or Password is incorrect`

As a workaround, login and launch Microsoft console with the credentials used to login to OMIMSSC console extension. This is a one-time activity.

SC2012 VMM SP1 crashing during update

After upgrading to SC2012 VMM SP1, when importing OMIMSSC console extension to SC2012 VMM UR5 or later, the SCVMM console may crash.

For information about this issue and resolving the issue, see issue 5 in the knowledge base URL: `support.microsoft.com/kb/2785682`.

As a workaround, update SCVMM irrespective of the version of the update rollup that is installed.

OMIMSSC admin portal scenarios

Error message while accessing OMIMSSC admin portal through Mozilla Firefox browser

When accessing the OMIMSSC admin portal by using Mozilla Firefox browser, you get the following warning message: "`Secure Connection Failed`".

As a workaround, delete the certificate created from a previous entry of the admin portal in the browser. For information about deleting certificate from Mozilla Firefox browser, see `support.mozilla.org`

Failure to display Dell EMC logo in OMIMSSC admin portal

When the OMIMSSC admin portal is launched on a Windows 2016 default IE browser, the admin portal is not displayed with the Dell EMC logo.

As a workaround, do one of the following:

- Upgrade IE browser to the latest version.
- Delete the browsing history, and then add the OMIMSSC admin portal URL to browser's favorite list.

6

Discovery, synchronization and inventory scenarios in OMIMSSC

Failure to discover servers

When multiple Microsoft consoles are enrolled to an OMIMSSC Appliance, and you try to discover a server, if even one of the SCCM consoles are not reachable, then the server discovery job will fail.

As a workaround, de-enroll the SCCM console that is not reachable, or fix the errors and ensure that the SCCM console is reachable from OMIMSSC Appliance.

Discovered servers not added to All Dell Lifecycle Controller Servers collection

After discovering the servers in OMIMSSC for SCCM console extension, the server may not get added into **All Dell Lifecycle Controller Servers** collection.

As a workaround, delete the **All Dell Lifecycle Controller Servers** collection and then discover the server. The collection is automatically created in SCCM and the server is added to this group.

Failure to discover servers due to incorrect credentials

If you provide incorrect credential details during discovery, then based on the iDRAC version, the following resolutions are available:

- While discovering a 12th generation PowerEdge server with iDRAC version 2.10.10.10 and later, if incorrect details are provided in the credential profile, the server discovery fails, with the following behavior:
  - For first attempt, server IP address is not blocked.
  - For second attempt, server IP address is blocked for 30 seconds.
  - For third and subsequent attempts, server IP address is blocked for 60 seconds.

  You can reattempt server discovery with correct credential profile details after the IP address is unblocked.
- 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.

Creation of incorrect VRTX chassis group after server discovery

When modular servers that were previously in another chassis are added to a VRTX chassis and discovered in OMIMSSC, the modular servers carry previous chassis service tag information. Hence, a VRTX chassis group with old chassis information is created in the Appliance instead of the latest chassis information.

As a workaround, do the following:

1. Enable CSIOR, and reset iDRAC on the newly added modular server.

2. Manually delete all the servers in the VRTX chassis group, and then rediscover the servers.

Unable to synchronize host servers with enrolled SCCM

During synchronization of OMIMSSC console extension with enrolled SCCM, the servers are not listed as sub tasks in synchronization job and hence does not get synchronized.

As a workaround, launch SCCM console with "Run as Administrator Privilege" and update out of band configuration for a server. Then synchronize OMIMSSC console extension with enrolled SCCM.

For more information, see Synchronizing with enrolled Microsoft console topic in *OpenManage Integration for Microsoft System Center Version 7.2 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide.*

Empty cluster update group not deleted during autodiscovery or synchronization

When a cluster is discovered in OMIMSSC, a cluster update group gets created in the **Maintenance Center** with all the servers listed in the cluster update group. Later, if all the servers are removed from this cluster through SCVMM, and an autodiscovery or synchronization with SCVMM operation is performed, the empty cluster update group is not deleted in **Maintenance Center**.

As a workaround, to delete the empty server group, rediscover the servers.

Failure to perform maintenance-related tasks on rediscovered servers

When you delete a server or all the servers in an update group from OMIMSSC, and rediscover them you cannot perform any other operations on these servers like updating firmware, exporting and importing LC logs, exporting and importing server profiles.

As a workaround, after rediscovering the deleted server or servers, perform firmware updates using the **Deploy Operational Template** feature in **Server View** and for other maintenance scenarios use iDRAC.

7

Generic scenarios in OMIMSSC

Failure to access CIFS share using hostname

The modular servers are not able to access the CIFS share using the host name for performing any job in OMIMSSC.

As a workaround, specify the IP address of the server having the CIFS share instead of the host name.

Failure to display Jobs and Logs page in console extension

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

As a workaround, re-enroll the console and then launch the **Jobs and Logs** page.

Failure of operations on managed systems

All the features of OMIMSSC does not perform as expected on the managed systems due to a Transport Layer Security (TLS) version.

If you are using iDRAC firmware version 2.40.40.40 or later, Transport Layer Security (TLS) versions 1.1 or later is enabled by default. Before installing the console extension, install the update to enable TLS 1.1 and later as mentioned in the following KB article: `Support.microsoft.com/en-us/kb/3140245`. It is recommended that you enable support for TLS 1.1 or later on your SCVMM server and SCVMM console to ensure that OMIMSSC operates as expected. And for more information about iDRAC, see Dell.com/idracmanuals.

Failure to launch online help for OMIMSSC

When using Windows 2012 R2 operating system, the context sensitive online help content is launched displaying an error message.

As a solution, update the operating system using the latest KB articles, and then view the online help content.

8

Firmware update scenarios in OMIMSSC

Failure of creation of update source

When the Domain Name System (DNS) network configuration of the Appliance is changed, creation of HTTP or FTP type of update source fails.

As a workaround, restart the Appliance, and then create the update source of type HTTP or FTP.

Failure to connect to FTP using system default update source

After setting up and configuring, upgrading, or migrating OMIMSSC when you try to access the FTP site using the default update source **Dell Online Catalog** it may fail if proxy credentials are required.

As a workaround, to access the FTP site using **Dell Online Catalog** as an update source, edit the update source to add the proxy credentials.

Failure of test connection for local update source

After proving the details of a local update source, the test connection may fail as the required files may be not accessible.

As a workaround, ensure that `catalog.gz` file is present in the following folder structure.

- For local HTTP update source: `http:\\IP address\catalog\catalog.gz`
- For local FTP update source: `ftp:\\IP address\catalog\catalog.gz`
- For local DRM update source: `\\IP address\\catalog\<catalogfile>.gz`

Failure to create DRM update source

Creating DRM update source on management server running on Windows 10 Operating System (OS) may fail, displaying the following error message: `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Refer the **dlciappliance_main** log in OMIMSSC Admin portal, if the error message displayed is: *`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

As a workaround, see to the following KB article: *support.microsoft.com/en-us/help/4034314*

Failure to create repository during firmware update

Creation of a repository may fail during a firmware update because of incorrect credentials provided while creating an update source, or update source is not reachable by OMIMSSC Appliance.

As a workaround, ensure that the update source is reachable from where the OMIMSSC Appliance is hosted, and provide the correct credentials while creating an update source.

Failure to display comparison report after upgrading or migrating OMIMSSC

After upgrading to the latest version of OMIMSSC, if the connection to `ftp.dell.com` or `downloads.dell.com` fails, the default Dell online FTP, or Dell HTTP update source cannot download the catalog file. Hence, the comparison report is not available.

As a workaround, to view a comparison report for the default update source, edit the default Dell online FTP, or Dell HTTP update source, create proxy credentials, and then select the update source from **Select Update Source** drop-down menu. For more information about editing an update source, see *Modifying update source* section from *Dell EMC OpenManage Integration for Microsoft System Center for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

Failure to update firmware of clusters

After a job is submitted in OMIMSSC to update firmware of clusters, the clusters are not updated due to certain reasons displaying the following error messages in **Activity Logs**.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

NOTE: The Cluster Aware Update actions are logged in the following locations : \\<SCVMM CIFS share>\OMIMSSC_UPDATE\reports folder where the Cluster Aware Update report will be stored. The \\SCVMM CIFS share\OMIMSSC_UPDATE\reports\log folder will further contain the Dell EMC System Update (DSU) plugin logs for each node. Extended script logs are available in C:\Window\Temp location which consists precau.log and postcau.log files in each cluster nodes for S2D cluster.

Reasons of failure of firmware update on clusters with the following workaround:

- If the required DUPs and catalog files are not present in the selected local update source.

  As a workaround is to ensure that all the required DUPs and catalog files are available in the repository, and then update the firmware of clusters.
- Cluster group becomes unresponsive or firmware update job was canceled in CAU due to an in-progress job, then the DUPs are downloaded and placed in each server cluster node belonging to the cluster group.

  As a workaround, delete all the files in Dell folder, and then update the firmware of clusters.
- If Lifecycle Controller (LC) is busy with other operations, then firmware update task on a cluster node fails. To check if the update failed because of LC being busy, check for the following error message in each node of the cluster at the following path: `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then
  reboot the system.
  ```

  As a workaround, shut down the server, remove the power cables, and then restart the server. After reboot, update the firmware on clusters.

Failure of firmware update because of job queue being full

Firmware update job submitted from OMIMSSC to iDRAC fails, and the OMIMSSC main log displays the following error: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

As a workaround, manually delete the completed jobs in iDRAC, and retry the firmware update job. For more information about deleting jobs in iDRAC, see iDRAC documentation at **dell.com/support/home**.

Failure of firmware update when using DRM update source

Firmware update job may fail if you are using DRM update source with insufficient access to the share folders. If the Windows credential profile provided while creating DRM update source is not a part of domain administrator group or the local administrator group, the following error message is displayed: `Local cache creation failure`.

As a workaround, perform the following:

1. After creating the repository from DRM, right-click on the folder, click **Security** tab, and then click **Advanced**.
2. Click **Enable inheritance** and select the **Replace all child object permission entries with inheritable permission entries from this object** option, and then share the folder with **Everyone** with read-write permission.

Firmware update on components irrespective of selection

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

As a workaround, do one of the following:

- First apply updates for common components on identical servers, and then apply updates for specific components on individual servers.
- Perform staged updates with planned outage time to accommodate the firmware update.

Failure to display latest inventory information after firmware update

After successfully updating the firmware versions on 11th generation PowerEdge servers, the latest inventory information is not displayed.

In OMIMSSC, refreshing the inventory is an activity performed immediately after a firmware update job is complete. Firmware update is completed even before the PowerEdge server's CSIOR activity is complete, due to which the earlier firmware inventory information is displayed.

As a workaround, check if the CSIOR activity is complete in the PowerEdge server, and then refresh the firmware inventory in OMIMSSC. Also, ensure to restart the server after applying agent-free staged update. For more information about refreshing the inventory, see *Viewing and refreshing firmware inventory* section in *OpenManage Integration for Microsoft System Center Configuration Manager and Virtual Machine Manager User's Guide*.

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

Failure to delete a custom update group

After scheduling any job on a server belonging to a custom update group, if the server is deleted from Microsoft console and you synchronize registered Microsoft console with OMIMSSC, the server is removed from the custom update group and the server is moved to a predefined update group. You cannot delete such custom update group, because it is associated with a scheduled job.

As a workaround, delete the scheduled job from Jobs and Logs page, and then delete the custom update group.

Failure to update WinPE image

When you try to update the WinPE image, update job may fail with the following error message: `Remote connection to console failed.`

As a workaround, run the **DISM** command to clean up all previously mounted images in Microsoft console, and then retry to update the WinPE image.

Failure of firmware update on 11th generation of servers

Firmware updates applied 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 apply the firmware updates. The table lists out the latest versions of LC and iDRAC.

Table 1. Versions of LC and iDRAC

Lifecycle Controller Version	Integration Dell Remote Access Controller Version
1.7.5.4 or higher	• For Modular servers: 2.90 or higher • For Monolithic servers: 3.85 or higher

Changing of polling and notification bell color after updating the frequency

If a managed server is not discovered in OMIMSSC, and you change the frequency of polling and notification option, the bell color changes to yellow after sometime, even if there are no changes in the catalog.

As a workaround, discover managed servers and then change the frequency of polling and notification option.

9

Operating system deployment scenarios in OMIMSSC

Operating system deployment generic scenarios

This section has all the generic troubleshooting information related to operating system deployment.

Failure to deploy Operational Template

After deploying the Operational Template on the selected servers, the attributes or attribute values are not appropriate for the selected .CSV file, or the iDRAC IP or iDRAC credentials are changed due to the configurations in the template. The job in iDRAC is successful, however the status of this job in OMIMSSC is shown as unsuccessful or failure due to invalid .CSV file, or the job cannot be tracked due to the iDRAC changes on the target server.

As a workaround, ensure the selected .CSV file has all the proper attributes and attribute values, and the iDRAC IP or credentials do not change due to the configurations in the template.

Failure to save an Operational Template

When you are creating an Operational Template, if you select and clear a dependent attribute's check box having pool value, you are not able to save the Operational Template with the following error message:

```
Select atleast one attribte, under the selected components, before creating the Operational
Template.
```

As a workaround, perform any one of the following:

- Select any other dependent attribute having pool value or the same dependent attribute and save the Operational Template.
- Create a new Operational Template.

Operating system deployment scenarios for SCCM users

This section has all the troubleshooting information related to operating system deployment using OMIMSSC in SCCM console.

Deploy option not visible in task sequence

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

As a workaround, open the task sequence for editing, re-enable the **Apply** option, and click **OK**. The **Deploy** option is displayed again.

To re-enable the **Apply** option:

1. Right-click the task sequence, and select **Edit**.
2. Select **Restart in Windows PE**. In the **Description** section, type any character and delete it so the change is not saved.
3. Click **OK**.

   This re-enables the **Apply** option.

Failed to add servers into Managed Lifecycle Controller Lifecycle Controller ESXi collection in SCCM

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

As a workaround, install the SCCM client server, and then perform a synchronization to add the servers in Managed Lifecycle Controller Lifecycle Controller (ESXi) collection.

Operating system deployment scenarios for SCVMM users

This section has all the troubleshooting information related to hypervisor deployment using OMIMSSC in SCVMM console.

Hypervisor deployment failure due to LC or firewall protection

Hypervisor deployment fails displaying the following error message in activity log: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

This error may occur due to one of these reasons:

- Dell Lifecycle Controller's state is bad.

  As resolution, log in to iDRAC user interface and reset Lifecycle Controller.

  After resetting Lifecycle Controller, if you still face the problem try the following alternative:
- The antivirus or firewall may restrict the successful run of the `WINRM` command.

  See the following KB article for workaround: `support.microsoft.com/kb/961804`

Hypervisor deployment failure due to driver files retained in library share

Hypervisor deployment fails displaying the following error message in activity log:

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

These errors may occur due to exception output by the VMM command-let `GET-SCJOB status` and driver files are retained in the library share. Before you retry or do another hypervisor deployment you must remove these files from the library share.

To remove files from library share:

1. From SCVMM console, select **Library** > **Library Servers** and then select the IG server that was added as the library server.
2. In the library server, select and delete the library share.
3. After the library share is deleted, connect to the IG share using `\\<Integration Gateway server>\LCDriver\`.
4. Delete the folder that contains the driver files.

After this, you can deploy the hypervisors.

SCVMM error 21119 while adding servers to Active Directory

While adding servers to Active Directory, SCVMM error 21119 is displayed. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

As a workaround, do the following:

1. Wait for some time to see if the server is added to the Active Directory.
2. If the server is not added to the Active Directory, then manually add the servers to the Active Directory.
3. Add the server in to SCVMM.
4. After the server is added in to SCVMM, rediscover the server in OMIMSSC.

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

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.

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

LC driver injection failure

When deploying OS and injecting LC drivers using SC2012 VMM, the OS is deployed successfully but, the LC drivers are not injected.

To resolve the issue, apply the latest rollup for SCVMM.

S2D cluster creation scenarios for SCVMM users

This section has all the troubleshooting information related to creating Storage Spaces Direct using OMIMSSC in SCVMM console.

Health status of S2D cluster is unknown

When you create a Storage Spaces Direct cluster on nodes that were part of an existing cluster, then the storage pool and the disk configurations have the configurations of the existing cluster. Hence, the cluster storage pool might not be created and if the cluster storage pool is created the health status may be displayed as unknown.

As a workaround, clear the storage pool and disk configuration having existing cluster details and then create the Storage Spaces Direct cluster. For more information on clearing the storage pool, see *Troubleshoot Storage Spaces Direct health and operational states* section from Microsoft documentation.

10

Server profile scenarios in OMIMSSC

Failure to export server profiles

After scheduling an export server profile job, the server profile is not exported, and the following error message is displayed: `The selectors for the resource are not valid.`

As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see iDRAC documentation available at `dell.com/support`.

Importing server profile job gets timed out after two hours

After submitting the import server profile job in OMIMSSC , the job gets timed out after two hours.

As a workaround, perform the following steps:

1. Start the server, press F2, and then enter **BIOS Settings**.
2. Click **System Setup**, and select **Miscellaneous Settings**.
3. Disable **F1/F2 Prompt on Error**.

After performing the following steps, export the server profile again, and use the same server profile to import on that server.

11

LC Logs scenarios in OMIMSSC

Failure to export LC logs in .CSV format

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

As a workaround, add the OMIMSSC Appliance FQDN in the browser under local intranet site. For information about adding the OMIMSSC Appliance in local intranet, see *Viewing LC logs* section in *Dell EMC OpenManage Integration for Microsoft System Center Version 7.1 for System Center Configuration Manager and System Center Virtual Machine Manager User's Guide*.

Failure to open LC log files

After collecting the LC logs, when you try to view the LC log file for a server, the following error message is displayed: "`Failed to perform the requested action. For more information see the activity log`".

As a workaround, reset iDRAC, and then collect and view the LC logs. For information about resetting iDRAC, see iDRAC documentation available at `dell.com/support`.

Failure of test connection

If user names are same and the passwords are different for the domain user account and local user account, then the test connection between Microsoft console and OMIMSSC Appliance fails.

For example, domain user account is: `domain\user1` and password is `pwd1`. And local user account is `user1` and password is `Pwd2` . When you try to enroll with the above domain user account, the test connection fails.

As a workaround, use different user names for the domain user and local user accounts, or use a single user account as local user and during Microsoft console enrollment in OMIMSSC Appliance.

12

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 — **www.dell.com/SoftwareSecurityManuals**
- For Dell EMC OpenManage documents — **www.dell.com/OpenManageManuals**
- For Dell EMC Remote Enterprise Systems Management documents — **www.dell.com/esmmanuals**
- For iDRAC documents — **www.dell.com/idracmanuals**
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- For Dell EMC Serviceability Tools documents — **www.dell.com/ServiceabilityTools**
- 1. Go to **www.support.dell.com** .
  2. Click **Browse all products**.
  3. From **All products** page, click **Software**, and then click the required link from the following:
     - **Analytics**
     - **Client Systems Management**
     - **Enterprise Applications**
     - **Enterprise Systems Management**
     - **Public Sector Solutions**
     - **Utilities**
     - **Mainframe**
     - **Serviceability Tools**
     - **Virtualization Solutions**
     - **Operating Systems**
     - **Support**
  4. To view a document, click the required product and then click the required version.
- Using search engines:
  - Type the name and version of the document in the search box.

Topics:

- Contacting Dell

Contacting Dell

ⓘ **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.**

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:

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.