OpenManage Integration Version 7.0 for Microsoft System Center

Release Notes

DELL EMC

2017 - 09

OpenManage Integration Version 7.0 for Microsoft System Center Release Notes

This document describes the features, known issues, and resolutions in OpenManage Integration Version 7.0 for Microsoft System Center (OMIMSSC).

Topics:

Release type and definition

OpenManage Integration Version 7.0 for Microsoft System Center

OpenManage Integration for Microsoft System Center (OMIMSSC) is an appliance-based integration into the System Center suite of products that enable full lifecycle management of the Dell EMC servers 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 PowerEdge servers in traditional data center, or use the integration with Microsoft System Center Virtual Machine Manager (SCVMM) for managing the Dell EMC PowerEdge servers in virtualized and cloud environments.

Version

7.0 Rev.A00

Release date

August 2017

Previous versions

DLCI for SCCM 3.3 and DLCI for SCVMM 1.3

Importance

OPTIONAL: Dell EMC recommends the customer to review specifics about the software update to determine if it applies to your system. The update contains changes that impact certain configurations, or provides new features that may/may not apply to your environment.

Platform(s) Affected

11th, 12th, 13th, and 14th generation of rack, modular, and tower models of Dell EMC PowerEdge servers.

What's new

- Appliance-based integration into Microsoft System Center.
- Multiple SCCM and SCVMM consoles can be integrated with single OMIMSSC Appliance.
- Support for 14th generation of the Dell EMC PowerEdge servers.
- Support for non-Windows(ESXi and RHEL) operating system deployments.
- Single template (Operational Template) for firmware update, hardware configuration, and operating system deployment.
- Hardware configuration compliance check for servers against operational template with configuration drift reports
- System Lockdown Mode information for 14th generation of the PowerEdge servers
- Management of the OMIMSSC licenses from the OMIMSSC admin portal
- Support for configuring network adapter, fibre channel, and PCIeSSD components of the PowerEdge servers.

Fixes

NA

Important notes

Upgrade scenario

Upgrading from the previous versions of the product is not supported. Alternatively, you can migrate the artifacts of DLCI for SCCM or DLCI for SCVMM. For more information on migrating from DLCI for SCCM 3.3, see *Migration from Dell Lifecycle Controller Integration Version 3.3 for Microsoft System Center Configuration Manager to OpenManage Integration Version 7.0 for Microsoft System Center*, and for migrating from DLCI for SCVMM 1.3, see *Migration from Dell Lifecycle Controller Integration version 1.3 for Microsoft System Center Virtual Machine Manager to OpenManage Integration Version 7.0 for Microsoft System Center*.

Microsoft CAU-based firmware update support

Firmware update is not supported through the Microsoft CAU feature in the OMIMSSC version 7.0 for servers belonging to cluster groups present or discovered in Windows Server 2008.

Installation prerequisites

You can install OMIMSSC on 11th generation and later generation of the PowerEdge rack, modular, and tower servers.

You can manage servers using OMIMSSC if the servers are compliant. The following table lists out the prerequisites for servers to be managed by OMIMSSC.

Managed servers are the servers managed using OMIMSSC.

Table 1. Prerequisites for managed servers

PowerEdge Servers	Lifecycle Controller Version	Integration Dell Remote Access Controller Version	Dell EMC Repository Manager Version	Dell EMC OS Driver Pack Version	Dell EMC OpenManage Deployment Toolkit Version	Chassis Firmware Version
14th generation	3.00.00.00	3.00.00.00	3.0	NA	6.0.1	NA
13th generation	2.40.40.40 or higher	2.40.40.40 or higher	2.2 and 2.2.2	16.08.13	5.5	FX2 -1.4 or higher M1000e -5.2 or higher VRTX-2.2 or higher
12th generation	2.40.40.40 or higher	2.40.40.40 or higher	2.2 and 2.2.2	• For servers R220 and FM120: 16.08.13 • Other supported platforms: 15.07.07	5.5	
11th generation	1.7.5.4 or higher	• For Modular servers: 2.85 or higher • For Monolithic servers: 3.80 or higher	2.2 and 2.2.2	15.04.00	5.5	

For operating system deployment using OMIMSSC, following versions of hypervisors and non-windows operating systems are supported:

- Windows Server 2016
  - Windows Server 2016 Standard Edition
  - Windows Server 2016 Datacenter Edition
- Windows Server 2012
  - Windows Server 2012 R2 Standard Edition
  - Windows Server 2012 R2 Datacenter Edition
  - Windows Server 2012 SP1 Standard Edition
  - Windows Server 2012 SP1 Datacenter Edition
- Windows Server 2008
  - Windows Server 2008 R2 SP1 Standard Edition
  - Windows Server 2008 R2 SP1 Enterprise Edition
  - Windows Server 2008 R2 SP1 Datacenter Edition
- RHEL 7.3(Supported only on 14th generation of the PowerEdge servers)
- RHEL 7.2
- RHEL 6.9
- RHEL 6.9

- ESXi 6.8
- ESXi 6.5
- ESXi 6.0 U3
- ESXi 6.0 U2 (Not supported on 14th generation of the PowerEdge servers)
- ESXi 6.0 U1 (Not supported on 14th generation of the PowerEdge servers)

NOTE: Deploying ESXi and RHEL operating systems are not supported on 11th generation of the PowerEdge servers.

Also, see more system requirements for managed servers listed in *OpenManage Integration for Microsoft System Center User's Guide*.

Known issues and resolutions

- **Issue 1**

  Description: SCVMM creates an account for OMIMSSC with the name OMIMSSC Application Profile in SCVMM. If this profile is deleted, then you cannot work with OMIMSSC.

  Workaround: Recommend you to not delete the account. However, to reinstate the account and start working with OMIMSSC de-enroll and enroll the SCVMM console to OMIMSSC.

- **Issue 2**

  Description: When you restart the server in which OMIMSSC Integration Gateway is installed, connectivity is lost between the Appliance and Integration Gateway. This is because the execution policy of the Integration Gateway for the user is not active.

  Workaround: Log in to the Integration Gateway server using the Integration Gateway user account to make the execution policy active. However, the connection is not restored until the following steps are completed: To set the PowerShell execution policy:

  a Set PowerShell execution policy for local system as **RemoteSigned** and for the Integration Gateway Service Account as **Unrestricted**.

  For information on policy settings, refer the following MSDN articles:

  - PowerShell Execution policy: Technet.microsoft.com/en-us/library/hh847748.aspx
  - PowerShell Group Policy: Technet.microsoft.com/library/jj149004

  b Once the execution policy is set, restart the Integration Gateway server.

- **Issue 3**

  Description: SCVMM displays an error for security reasons when OMIMSSC is installed, and you apply an Update Rollup for SC2012 R2 VMM. As a result you cannot access OMIMSSC.

  Workaround: As a workaround, perform the following steps:

  a Delete the folder at default path: *C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin \AddInPipeline\AddIns\<username>*

  b Close and then open the SCVMM console.

  c Uninstall, and then import the console extension as mentioned in the Importing OMIMSSC console extension for SCVMM section from *OpenManage Integration Version 7.0 for Microsoft System Center Installation Guide*.

- **Issue 4**

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

  Workaround: As a workaround, delete the certificate created from a previous entry of the OMIMSSC admin portal in the browser.

- **Issue 5**

  Description: After installing OMIMSSC console extension for SCVMM in the SCVMM environment, on clicking the OMIMSSC console extension icon the following error is displayed: `Connection to server failed`.

  Workaround: As a workaround, perform the following steps:

- Add the Appliance IP and FQDN as a trusted site.
- Add the Appliance IP and FQDN in Forward Lookup Zones and Reverse Lookup Zones in DNS.
- Check if there are any error messages in **C:\ProgramData\VMMLogs\AdminConsole** file.

- **Issue 6**

  Description: After creating the VM, and starting the OMIMSSC Appliance, the IP address is not assigned or displayed on the black console.

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

- **Issue 7**

  Description: If the SCVMM account that is used to open the SCVMM console, does not meet the prerequisites, you get the following error: `You should be an Administrator/Delegated Administrator to launch the Add-In`.

  Workaround: Add the required privileges to the SCVMM account. For more information, see the Account privileges in OpenManage Integration Version 7.0 for Microsoft System Center User's Guide.

- **Issue 8**

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

  Workaround: As a workaround, 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:

  a Right-click the task sequence, and select **Edit**.

  b Select **Restart** in Windows Preexecution Environment (PE). In the Description section, type any character and delete it so the change is not saved.

  c Click **OK**.

- **Issue 9**

  Description: 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 OMIMSSC.

  Workaround: As a workaround, perform the following steps:

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

  b 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*. After you do the preceding tasks, if there are duplicate entries for chassis groups, then perform the following steps:

    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.

- **Issue 10**

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

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

- **Issue 11**

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

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

- **Issue 12**

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

  Workaround: 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 the iDRAC RACADM CLI Guide.

- **Issue 13**

  Description: After scheduling a firmware update job on a cluster update group, the firmware update job may fail due to 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.

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

- **Issue 14**

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

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

- **Issue 15**

  Description: 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`.

  Workaround: As a workaround, perform the following steps:

  a After creating the repository from DRM, right-click on the folder, click the **Security** tab, and then click **Advanced**.

  b 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.

- **Issue 16**

  Description: After scheduling a job on an update group, if all the servers are moved out of the update group and the update group is empty, then the scheduled job fails.

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

- **Issue 17**

  Description: After submitting the **Deploy** the Operational Template job on the servers, if 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` or `fail` due to invalid .CSV file, or the job cannot be tracked due to the iDRAC changes on the target server.

  Workaround: 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.

- **Issue 18**

  Description: Modular servers cannot use the host name in the path to the CIFS share but monolithic systems can use the host name.

  Workaround: As a workaround, specify the IP address of the CIFS share for modular systems.

- **Issue 19**

Description: After setting up and configuring, or upgrading OMIMSSC, trying to access the FTP site using system created update source—Dell Online Catalog may fail if proxy credentials are required.

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

- **Issue 20**

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

  Workaround: As a workaround, add the Appliance FQDN in the browser under local intranet site. For information about adding the Appliance in local intranet, see *Browser settings* section in *Dell Lifecycle Controller Integration Version 2.0 for Microsoft System Center User's Guide*.

- **Issue 21**

  Description: 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`.

  Workaround: As a workaround, reset iDRAC, and then schedule the export server profile job. For more information, see the *iDRAC RACADM CLI Guide*.

- **Issue 22**

  Description: 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`.

  Workaround: As a workaround, reset iDRAC, and then collect and view the LC Logs. For more information, see the *iDRAC RACADM CLI Guide*.

- **Issue 23**

  Description: 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 the PowerEdge servers with the Enterprise license of iDRAC.

  Workaround: As a workaround, perform one of the following steps:

  - 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.

- **Issue 24**

  Description:

  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.

- **Issue 25**

Description: Hypervisor deployment fails, and the activity log displays the following error:

```
Error: Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""
```

```
Information: Successfully deleted drivers from library share <hostname.domain> 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.

Workaround: To remove files from library share:

a From SCVMM Console, select **Library** > **Library Servers** and then select the Integration Gateway server that was added as the library server.

b In the library server, select and delete the library share.

c After the library share is deleted, connect to the Integration Gateway share using **\\<Integration Gateway server>\LCDriver\.**

d Delete the folder that contains the driver files.

Now, you can deploy operating systems.

- **Issue 26**

Description: 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.

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

- **Issue 27**

Server's iDRAC IP address blocked due to multiple incorrect inputs during discovery.

Workaround: Based on the iDRAC version, the following workarounds are available:

- While discovering a 12th generation PowerEdge server with the 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 the 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 the iDRAC versions prior to 2.10.10.10, blocking of IP addresses is configurable. For more information, see *iDRAC RACADM CLI Guide*. Based on your requirement, you can disable blocking of IP addresses. And you can also check if the **iDRAC.IPBlocking.BlockEnable** feature is enabled in iDRAC.

- **Issue 28**

Description: 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.

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

- **Issue 29**

Description: After submitting the import server profile job to OMIMSSC, it may get timed out after two hours.

Workaround: As a workaround, perform the following steps:

a Press F2 and enter BIOS Settings.

b Click **System Setup,** and select **Miscellaneous Settings**.

c 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.

- **Issue 30**

Description: Even though the firmware update job is complete on an 11th generation of the PowerEdge server, the inventory list in OMIMSSC on **Maintenance Center** page does not display the latest firmware versions.

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

Workaround: 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 on refreshing the inventory, see Viewing and refreshing firmware inventory section in OpenManage Integration for Microsoft System Center User's Guide.

For more information on CSIOR, refer to the Troubleshooting section in the latest version of the Dell Lifecycle Controller GUI User's Guide.

- **Issue 31**

Description: When adding servers to Active Directory, the **SCVMM error 21119** is displayed.

```
Error 21119: The physical computer with <SMBIOS GUID> id not joins Active Directory in time.
The computer was expected to join Active Directory using the computer name <host.domain>
```

Workaround: As a workaround, perform the following steps:

a Wait for some time to see if the server is added to the Active Directory.

b If the server is not added to the Active Directory, then manually add the servers to the Active Directory.

c Add the server in to SCVMM.

d Once the server is added to SCVMM, rediscover the server in the OMIMSSC.

The server is listed under the Host tab.

- **Issue 32**

Description: If the default iDRAC credential profile is changed after a server is discovered and added in OMIMSSC, then no activity can be performed on the server.

Workaround: To work with the server, rediscover the server with the new credential profile.

- **Issue 33**

Description: When you sequentially deploy OS with different flavors of Linux from same share folder the deployment on few of the target servers fail.

- **Issue 34**

Description: 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.

Workaround: As a workaround, perform one of the following steps:

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

- **Issue 35**

The Jobs and Logs Center is not displayed in OMIMSSC.

As a workaround, reenroll the console.

- **Issue 36**
  Description: If you are accessing local FTP using proxy credentials created by CCProxy server, then the local FTP site is not accessible.
- **Issue 37**
  Description: In BIOS Settings, the snoop mode attribute does not support **ClusterOnDie** option.
- **Issue 38**
  Description: The action in comparison report for OS collector component is displayed as **Downgrade** even if it an **upgrade** action.

Download instructions

Download an evaluation version of the product from **http://dell.ly/omimssc**

For a production version, purchase the product license for required number of servers by contacting a local Dell sales representative and import it in the product.

For information on importing a license file, see the *OpenManage Integration for Microsoft System Center User's Guide*.

Installation and configuration notes

For installation and configuration-related information, see the *OpenManage Integration Version 7.0 for Microsoft System Center Installation Guide*.

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.

2017 - 09