OpenManage Integration for VMware vCenter
Version 4.2
Web Client Installation 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.
# Contents

## 1 Introduction

- OpenManage Integration for VMware vCenter licensing ................................................................. 5
- License requirements for hosts and vCenter servers ........................................................................ 6
- Buying and uploading software license ............................................................................................ 6
- Options after uploading licenses ....................................................................................................... 6
- Enforcement .......................................................................................................................................... 7
- Important notes for reference ............................................................................................................. 7

## Hardware requirements

- System requirements for deployment modes ....................................................................................... 8
- BIOS, iDRAC, Lifecycle Controller versions ......................................................................................... 8
- Supported features on PowerEdge servers .......................................................................................... 11
- Supported features on PowerEdge chassis ......................................................................................... 12
- Space required for provisioned storage .............................................................................................. 12

## Software requirements

- OpenManage Integration for VMware vCenter requirements ............................................................... 13

## Port information

- vCenter settings ................................................................................................................................. 14

## Prerequisite checklist

- Virtual appliance and managed nodes ............................................................................................... 14

## Installing, configuring, and upgrading OMIVV

- Deploying OMIVV OVF using vSphere web client ........................................................................... 17
- Uploading HTTPS certificate .............................................................................................................. 18
- Registering vCenter server by nonadministrator user ........................................................................ 19
- Registering OpenManage Integration for VMware vCenter and importing license file .................. 22
- Upgrading registered vCenter ............................................................................................................... 25
- Verifying installation ........................................................................................................................... 25
- Migrating from earlier version to 4.2 .................................................................................................... 26
- Recovering OMIVV after unregistering earlier version of OMIVV .................................................. 27

## 2 Appliance configuration for VMware vCenter

- Configuration tasks through configuration wizard ........................................................................... 28
- Viewing configuration wizard welcome dialog box .......................................................................... 28
- Selecting vCenters ............................................................................................................................. 29
- Creating connection profile ............................................................................................................... 29
- Scheduling inventory jobs ................................................................................................................... 31
- Running warranty retrieval jobs ........................................................................................................ 32
- Configuring events and alarms ............................................................................................................ 32
- Configuring SNMP trap community string ....................................................................................... 33

## Configuration tasks through settings tab

- Appliance settings ............................................................................................................................... 33
- vCenter settings ................................................................................................................................. 35

## Creating chassis profile

- Important notes for reference ............................................................................................................. 37
3 Accessing documents from the Dell EMC support site................................................................................................................................. 39

4 Related Documentation.................................................................................................................................................................................. 40
This guide provides step-by-step instructions for installing and configuring OpenManage Integration for VMware vCenter (OMIVV) for use with PowerEdge servers. After the OMIVV installation, for information about all aspects of administration including—inventory management, monitoring and alerting, firmware updates, and warranty management; see OpenManage Integration for VMware vCenter User's Guide available at Dell.com/support/manuals.

Topics:

- OpenManage Integration for VMware vCenter licensing
- Important notes for reference
- Hardware requirements
- Software requirements
- Port information
- Prerequisite checklist
- Installing, configuring, and upgrading OMIVV

OpenManage Integration for VMware vCenter licensing

The OpenManage Integration for VMware vCenter has two types of licenses:

- Evaluation license—when the OMIVV version 4.x appliance is powered on for the first time, an evaluation license is automatically installed. The trial version contains an evaluation license for five hosts (servers) managed by the OpenManage Integration for VMware vCenter. This is applicable only for 11th and later generations of the Dell EMC servers and is a default license, which is for a 90 days trial period.
- Standard license—the full product version contains a standard license for up to 10 vCenter servers and you can purchase any number of host connections managed by OMIVV.

When you upgrade from an evaluation license to a full standard license, you will receive an email about the order confirmation, and you can download the license file from the Dell Digital Locker. Save the license .XML file to your local system, and upload the new license file by using the Administration Console.

Licensing presents the following information:

- Maximum vCenter Connection Licenses—up to 10 registered and in-use vCenter connections are allowed.
- Maximum Host Connection Licenses—the number of host connections that were purchased.
- In Use—the number of vCenter connection or host connection licenses in use. For host connection, this number represents the number of hosts (or servers) that have been discovered and inventoried.
- Available—the number of vCenter connections or host connection licenses available for future use.

**NOTE:** The standard license period is for three or five years only, and the additional licenses are appended to the existing license and not over written.

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital Locker at http://www.dell.com/support/licensing. If you are unable to download your license key(s), contact Dell Support by going to www.dell.com/support/incidentsonline/in/en/indhs1/email/order-support to locate the regional Dell Support phone number for your product.
License requirements for hosts and vCenter servers

The following are the licensing requirements for hosts and vCenter:

- You can purchase a license to support the quantity of Dell EMC servers to be managed by OMIVV. A license is used only after a host is added to a connection profile. License is not associated with a particular server.
- One instance of OMIVV supports up to 10 instances of vCenter servers. There is no separate license for the number of vCenter servers.

Buying and uploading software license

You are running a trial license until you upgrade to a full product version. Use the Buy License link from the product to navigate to the Dell website and buy a license. After you buy it, upload it using the Administration Console.

About this task

NOTE: The Buy License option is displayed only if you are using a trial license.

Steps

1. In the OpenManage Integration for VMware vCenter, perform one of the following tasks:
   - In the Licensing tab, next to Software License, click Buy License.
   - In the Getting Started tab, under Basic Tasks, click Buy License.
2. Save the license file to a known location that you had downloaded from the Dell Digital Locker.
3. In a web browser, type the Administration Console URL. Use the format: https://<ApplianceIPAddress>
4. In the Administration Console login window, type the password and click Login.
5. Click Upload license.
6. In the Upload License window, to navigate to the license file, click Browse.
7. Select the license file, and then click Upload.

NOTE: The license file might be packaged inside a .zip file. Ensure that you unzip the .zip file and upload only the license .xml file. The license file is likely to be named based on your order number, such as 123456789.xml.

Options after uploading licenses

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 Locker at http://www.dell.com/support/licensing. 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

Starting from the OMIVV version 2.1, OMIVV can stack multiple standard licenses to increase the number of supported hosts to the sum of the hosts in the uploaded licenses. An evaluation license cannot be stacked. The number of supported vCenter servers cannot be increased by stacking, and requires the use of multiple appliances.
There are some restrictions around the functionality of stacking licenses. If a new standard license is uploaded before the existing standard license expires, the licenses stack. Otherwise, if the license expires and a new license is uploaded, only the number of hosts from the new license is supported. If there are already multiple licenses uploaded, the number of supported hosts are the sum of the hosts in the nonexpired licenses at the time the last license was uploaded.

**Expired licenses**

Licenses that are past their support duration, typically three or five years from the date of purchase are blocked from being uploaded. If licenses have expired after being uploaded, functionality for existing hosts continues; however upgrades to new versions of the OMIVV are blocked.

**Replacement of licenses**

If there is a problem with your order and you receive a replacement license from Dell, 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.

**Enforcement**

**Appliance updates**

The appliance does not allow updates to newer versions when all licenses are expired. Obtain and upload a new license before attempting to upgrade the appliance.

**Evaluation License**

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

**Adding hosts to connection profiles**

When you attempt to add a host to a connection profile, if the number of licensed 11th Generation or newer hosts exceeds beyond the number of licenses, adding extra hosts is prevented.

**Important notes for reference**

- From OMIVV 4.0 onwards, only VMware vSphere Web client is supported and the vSphere Desktop client is not supported.
- For vCenter 6.5 and later, the OMIVV appliance is only available for the flash version. The OMIVV appliance is not available for the HTML5 version.
- For using the DNS server, the recommended practices are:
  - OMIVV supports only IPv4 IP addresses. Although both static IP assignment and DHCP assignment are supported, it is recommended that you assign a static IP address. Assign a static IP address and host name when you deploy an OMIVV appliance with a valid DNS registration. A static IP address ensures that during the system restart, the IP address of the OMIVV appliance remains same.
  - Ensure that OMIVV host name entries are present in both forward and reverse lookup zones in your DNS server.

For more information about the DNS requirements for vSphere, see the following VMware links:

- DNS requirements for vSphere 5.5
DNS requirements for vSphere 6.0
- DNS requirements for vSphere 6.5 and Platform Services Controller appliance
  - For the OMIVV appliance mode, ensure that you deploy OMIVV in the appropriate mode based on your virtualization environment. For more information, see System requirements for deployment modes.
  - Configure your network to match the port requirements. For more information, see Port information.

**Hardware requirements**

OMIVV provides full support for several generations of the Dell EMC servers with full feature support for servers with iDRAC Express or Enterprise. Extensive information on the platform requirements is available in OpenManage Integration for VMware vCenter Release Notes available at Dell.com/support/manuals. To verify that your host servers are eligible, see information about the following in the subsequent subsections:

- Supported server and minimum BIOS
- iDRAC supported versions (both deployment and management)
- OMSA support for 11th generation and older servers, and the ESXi version support (both deployment and management)
- Supported memory and space for OMIVV

OMIVV requires LAN on motherboard/Network daughter card that can access both iDRAC/CMC systems management network and the vCenter management network.

**System requirements for deployment modes**

Ensure that the following system requirements for the desired deployment modes are met:

<table>
<thead>
<tr>
<th>Deployment modes</th>
<th>Number of hosts</th>
<th>Number of CPUs</th>
<th>Memory—in GB</th>
<th>Minimum Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>Up to 250</td>
<td>2</td>
<td>8</td>
<td>44 GB</td>
</tr>
<tr>
<td>Medium</td>
<td>Up to 500</td>
<td>4</td>
<td>16</td>
<td>44 GB</td>
</tr>
<tr>
<td>Large</td>
<td>Up to 1000</td>
<td>8</td>
<td>32</td>
<td>44 GB</td>
</tr>
</tbody>
</table>

**NOTE:** For any of the mentioned deployment modes, ensure that you reserve sufficient amount of memory resources to the OMIVV virtual appliance by using reservations. See vSphere documentation for steps about reserving memory resources.

**BIOS, iDRAC, Lifecycle Controller versions**

The BIOS, iDRAC, and the Lifecycle Controller versions required to enable the features of OpenManage Integration for VMware vCenter are listed in this section.

It is recommended that you use the Bootable ISO created by using Repository Manager, or Lifecycle Controller's Platform to update your servers to one of the following base versions before using OMIVV:

<table>
<thead>
<tr>
<th>Server</th>
<th>Minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerEdge R210</td>
<td>1.8.2 or later</td>
</tr>
<tr>
<td>PowerEdge R210II</td>
<td>1.3.1 or later</td>
</tr>
<tr>
<td>Server</td>
<td>Minimum version</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>PowerEdge R310</td>
<td>1.8.2 or later</td>
</tr>
<tr>
<td>PowerEdge R410</td>
<td>1.9.0 or later</td>
</tr>
<tr>
<td>PowerEdge R415</td>
<td>1.8.6 or later</td>
</tr>
<tr>
<td>PowerEdge R510</td>
<td>1.9.0 or later</td>
</tr>
<tr>
<td>PowerEdge R515</td>
<td>1.8.6 or later</td>
</tr>
<tr>
<td>PowerEdge R610</td>
<td>6.1.0 or later</td>
</tr>
<tr>
<td>PowerEdge R710</td>
<td>6.1.0 or later</td>
</tr>
<tr>
<td>PowerEdge R715</td>
<td>3.0.0 or later</td>
</tr>
<tr>
<td>PowerEdge R810</td>
<td>2.5.0 or later</td>
</tr>
<tr>
<td>PowerEdge R815</td>
<td>3.0.0 or later</td>
</tr>
<tr>
<td>PowerEdge R910</td>
<td>2.5.0 or later</td>
</tr>
<tr>
<td>PowerEdge M610</td>
<td>6.1.0 or later</td>
</tr>
<tr>
<td>PowerEdge M610x</td>
<td>6.1.0 or later</td>
</tr>
<tr>
<td>PowerEdge M710HD</td>
<td>5.0.1 or later</td>
</tr>
<tr>
<td>PowerEdge M910</td>
<td>2.5.0 or later</td>
</tr>
<tr>
<td>PowerEdge M915</td>
<td>2.6.0 or later</td>
</tr>
<tr>
<td>PowerEdge T110 II</td>
<td>1.8.2 or later</td>
</tr>
<tr>
<td>PowerEdge T310</td>
<td>1.8.2 or later</td>
</tr>
<tr>
<td>PowerEdge T410</td>
<td>1.9.0 or later</td>
</tr>
<tr>
<td>PowerEdge T610</td>
<td>6.1.0 or later</td>
</tr>
<tr>
<td>PowerEdge T710</td>
<td>6.1.0 or later</td>
</tr>
</tbody>
</table>

Table 3. BIOS for PowerEdge 12th generation servers

<table>
<thead>
<tr>
<th>Server</th>
<th>Minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>T320</td>
<td>1.0.1 or later</td>
</tr>
<tr>
<td>T420</td>
<td>1.0.1 or later</td>
</tr>
<tr>
<td>T620</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>M420</td>
<td>1.2.4 or later</td>
</tr>
<tr>
<td>M520</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>M620</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>M820</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>R220</td>
<td>1.0.3 or later</td>
</tr>
<tr>
<td>R320</td>
<td>1.2.4 or later</td>
</tr>
<tr>
<td>R420</td>
<td>1.2.4 or later</td>
</tr>
<tr>
<td>R520</td>
<td>1.2.4 or later</td>
</tr>
<tr>
<td>Server</td>
<td>Minimum version</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
</tr>
<tr>
<td>R620</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>R720</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>R720xd</td>
<td>1.2.6 or later</td>
</tr>
<tr>
<td>R820</td>
<td>1.7.2 or later</td>
</tr>
<tr>
<td>R920</td>
<td>1.1.0 or later</td>
</tr>
</tbody>
</table>

Table 4. BIOS for PowerEdge 13th generation servers

<table>
<thead>
<tr>
<th>Server</th>
<th>Minimum version</th>
</tr>
</thead>
<tbody>
<tr>
<td>R630</td>
<td>1.0.4 or later</td>
</tr>
<tr>
<td>R730</td>
<td>1.0.4 or later</td>
</tr>
<tr>
<td>R730xd</td>
<td>1.0.4 or later</td>
</tr>
<tr>
<td>R430</td>
<td>1.0.4 or later</td>
</tr>
<tr>
<td>R530</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>R830</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>R930</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>R230</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>R330</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>T630</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>T130</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>T330</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>T430</td>
<td>1.0.2 or later</td>
</tr>
<tr>
<td>M630</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>M830</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>FC430</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>FC630</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>FC830</td>
<td>1.0.0 or later</td>
</tr>
</tbody>
</table>

Table 5. BIOS for PowerEdge 14th generation servers

<table>
<thead>
<tr>
<th>Server</th>
<th>Minimum Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>R940</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>R740</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>R740xd</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>R640</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>M640</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>T640</td>
<td>1.0.0 or later</td>
</tr>
<tr>
<td>T440</td>
<td>1.0.0 or later</td>
</tr>
</tbody>
</table>
## Table 6. iDRAC and Lifecycle Controller for deployment

<table>
<thead>
<tr>
<th>Generation</th>
<th>iDRAC</th>
<th>Lifecycle Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerEdge 11th generation servers</td>
<td>3.35 for Modular, 1.85 for Rack or Tower</td>
<td>1.5.2 or later</td>
</tr>
<tr>
<td>PowerEdge 12th generation servers</td>
<td>1.00.0 or later</td>
<td>1.0.0.3017 or later</td>
</tr>
<tr>
<td>PowerEdge 13th generation servers</td>
<td>2.30.30.30 or later</td>
<td>2.30.30.30 or later</td>
</tr>
<tr>
<td>PowerEdge 14th generation servers</td>
<td>3.00.00.00 and later</td>
<td>3.00.00.00 and later</td>
</tr>
</tbody>
</table>

## Table 7. BIOS and iDRAC requirements for cloud server

<table>
<thead>
<tr>
<th>Model</th>
<th>BIOS</th>
<th>iDRAC with Lifecycle Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>C6320</td>
<td>1.0.2</td>
<td>2.30.30.30 or later</td>
</tr>
<tr>
<td>C4130</td>
<td>1.0.2</td>
<td>2.30.30.30 or later</td>
</tr>
<tr>
<td>C6420</td>
<td>1.0.0 or later</td>
<td>3.00.00.00 or later</td>
</tr>
<tr>
<td>C4140</td>
<td>1.0.0 or later</td>
<td>3.00.00.00 or later</td>
</tr>
</tbody>
</table>

## Supported features on PowerEdge servers

The following features are supported on the hosts managed by OpenManage Integration for VMware vCenter:

## Table 8. Supported features on PowerEdge servers

<p>| Resource                        | Platform          |<br />
|---------------------------------|-------------------|-------------------|-------------------|
|                                 | 11th              | 12th and 13th     | 14th              |
| Hardware Inventory              | Y                 | Y                 | Y                 |
| Events and Alarms               | Y (SNMP v1 only)  | Y (SNMP v1 and v2)| Y (SNMP v1 and v2)|
| Component wise Health Monitoring*| Y                 | Y                 | Y                 |
| BIOS/Firmware Updates**         | Y                 | Y                 | Y                 |
| Proactive HA***                 | N                 | Y                 | Y                 |
| Warranty Information            | Y                 | Y                 | Y                 |
| Host Compliance                 | Y                 | Y                 | Y                 |</p>
<table>
<thead>
<tr>
<th>Resource</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11th</td>
</tr>
<tr>
<td>Auto/Manual discovery of bare-metal server</td>
<td>Y</td>
</tr>
<tr>
<td>Bare-Metal compliance</td>
<td>Y</td>
</tr>
<tr>
<td>Hardware Configuration</td>
<td>Y</td>
</tr>
<tr>
<td>Bare-Metal Hypervisor Deployment</td>
<td>Y</td>
</tr>
<tr>
<td>Blink Server LED</td>
<td>Y</td>
</tr>
<tr>
<td>View/Clear SEL logs</td>
<td>Y</td>
</tr>
<tr>
<td>Link and Launch iDRAC</td>
<td>Y</td>
</tr>
<tr>
<td>iDRAC reset</td>
<td>Y</td>
</tr>
<tr>
<td>System Lockdown Mode</td>
<td>N</td>
</tr>
<tr>
<td>System Profile</td>
<td>N</td>
</tr>
<tr>
<td>Cluster Profile</td>
<td>N</td>
</tr>
</tbody>
</table>

*In Cloud with model number C6320, health monitoring is not supported for the mezzanine cards.

**In Cloud with model number C6320, firmware updates are not supported for the mezzanine cards.

***Proactive HA feature is only applicable on vCenter 6.5 or later that has ESXi 6.0 or later. Also, Proactive HA feature is not supported on servers with embedded PSU and cloud server models.

**** In cluster profile, configuration drift is not supported.

**Supported features on PowerEdge chassis**

This topic provides information about the supported features on the PowerEdge chassis.

**Table 9. Supported features on modular infrastructure**

<table>
<thead>
<tr>
<th>Features</th>
<th>M1000e</th>
<th>VRTX</th>
<th>FX2s</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Alerts</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Hardware Inventory</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Link and Launch CMC</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>License Information</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Warranty Information</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Health Reporting</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Space required for provisioned storage**

The OMIVV virtual appliance requires at least 44 GB of disk space for provisioned storage.
Default virtual appliance configuration

The OMIVV virtual appliance is provisioned with 8 GB of RAM and 2 virtual CPU.

Software requirements

Ensure that the vSphere environment fulfills virtual appliance, port access, and listening port requirements.

Requirements for VMware vSphere web client

- Supports vCenter 5.5 and later
- Requires web client services from vCenter (vSphere Desktop client is not supported)

For specific software requirements, you can also see OpenManage Integration for VMware vCenter Compatibility Matrix available at Dell.com/support/manuals.

OpenManage Integration for VMware vCenter requirements

Supported ESXi versions on managed hosts

The following table provides information about the supported ESXi versions on managed hosts:

Table 10. Supported ESXi versions

<table>
<thead>
<tr>
<th>ESXi version support</th>
<th>11G</th>
<th>12G</th>
<th>13G</th>
<th>14G</th>
</tr>
</thead>
<tbody>
<tr>
<td>v5.0</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.0 U1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.0 U2</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.0 U3</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.1 U1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.1 U2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v5.1 U3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v5.5</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.5 U1</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>v5.5 U2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v5.5 U3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v6.0</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v6.0 U1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v6.0 U2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>v6.0 U3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
The OpenManage Integration for VMware vCenter supports any of the following vCenter server versions:

Table 11. Supported vCenter server versions

<table>
<thead>
<tr>
<th>vCenter version</th>
<th>Web client support</th>
</tr>
</thead>
<tbody>
<tr>
<td>v6.0 U2</td>
<td>Y</td>
</tr>
<tr>
<td>v6.0 U3</td>
<td>Y</td>
</tr>
<tr>
<td>v6.5</td>
<td>Y</td>
</tr>
<tr>
<td>v6.5 U1</td>
<td>Y</td>
</tr>
<tr>
<td>v6.7</td>
<td>Y</td>
</tr>
</tbody>
</table>

NOTE: For more information about registering a vCenter server, see [OpenManage Integration for VMware vCenter Version 4.2 Web Client Install Guide](https://Dell.com/support/manuals).

The OpenManage Integration for VMware vCenter version 4.2 supports VMware vRealize Operations Manager (vROPS) version 1.1 and 1.2.

### Port information

#### Virtual appliance and managed nodes

In OMIVV, when you deploy the OMSA agent by using the Fix non-compliance hosts link available in the Fix Non-compliant vSphere Hosts wizard, OMIVV performs the following action:

- Starts the HTTP Client service
- Enables port 8080
- Makes the port available for ESXi 5.0 or later to download and install OMSA VIB

After the OMSA VIB installation is complete, the service automatically stops and the port is closed.

Table 12. Virtual appliance

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocols</th>
<th>Port Type</th>
<th>Maximum Encryption Level</th>
<th>Direction</th>
<th>Destination</th>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>DNS</td>
<td>TCP</td>
<td>None</td>
<td>Out</td>
<td>OMMVV appliance to DNS server</td>
<td>DNS client</td>
<td>Connectivity to the DNS server or resolving the host names.</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>UDP</td>
<td>None</td>
<td>Out</td>
<td>OMMVV appliance to TFTP server</td>
<td>TFTP Client</td>
<td>Used for firmware update on 11G servers with old firmware.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Protocols</td>
<td>Port Type</td>
<td>Maximum Encryption Level</td>
<td>Direction</td>
<td>Destination</td>
<td>Usage</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-----------</td>
<td>--------------------------</td>
<td>-----------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>TCP</td>
<td>None</td>
<td>Out</td>
<td>OMIVV appliance to internet</td>
<td>Dell Online Data Access</td>
<td>Connectivity to the online (internet) warranty, firmware and latest RPM information.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>TCP</td>
<td>None</td>
<td>In</td>
<td>ESXi server to OMIVV appliance</td>
<td>HTTP server</td>
<td>Used in OS deployment flow for post installation scripts to communicate with the OMIVV appliance.</td>
</tr>
<tr>
<td>162</td>
<td>SNMP Agent</td>
<td>UDP</td>
<td>None</td>
<td>In</td>
<td>iDRAC/ESXi to OMIVV appliance</td>
<td>SNMP Agent (server)</td>
<td>To receive SNMP traps from managed nodes.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>TCP</td>
<td>128-bit</td>
<td>In</td>
<td>OMIVV UI to OMIVV appliance</td>
<td>HTTPS server</td>
<td>Web services offered by OMIVV. These Web services are consumed by vCenter Web Client and Dell Admin portal.</td>
</tr>
<tr>
<td>443</td>
<td>WSMAN</td>
<td>TCP</td>
<td>128-bit</td>
<td>In/Out</td>
<td>OMIVV appliance to/from iDRAC/OMSA</td>
<td>iDRAC/OMSA communication</td>
<td>iDRAC, OMSA, and CMC communication, used to manage and monitor the managed nodes.</td>
</tr>
<tr>
<td>445</td>
<td>SMB</td>
<td>TCP</td>
<td>128-bit</td>
<td>Out</td>
<td>OMIVV appliance to CIFS</td>
<td>CIFS communication</td>
<td>To communicate with windows share.</td>
</tr>
<tr>
<td>4433</td>
<td>HTTPS</td>
<td>TCP</td>
<td>128-bit</td>
<td>In</td>
<td>iDRAC to OMIVV appliance</td>
<td>Auto Discovery</td>
<td>Provisioning server used for auto discovering managed nodes.</td>
</tr>
<tr>
<td>2049</td>
<td>NFS</td>
<td>UDP/TCP</td>
<td>None</td>
<td>In/Out</td>
<td>OMIVV appliance to NFS</td>
<td>Public Share</td>
<td>NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update and OS deployment flows.</td>
</tr>
<tr>
<td>4001 to 4004</td>
<td>NFS</td>
<td>UDP/TCP</td>
<td>None</td>
<td>In/Out</td>
<td>OMIVV appliance to NFS</td>
<td>Public Share</td>
<td>NFS public share that is exposed by OMIVV appliance to the managed nodes and used in Firmware update and OS deployment flows.</td>
</tr>
<tr>
<td>11620</td>
<td>SNMP Agent</td>
<td>UDP</td>
<td>None</td>
<td>In</td>
<td>iDRAC to OMIVV appliance</td>
<td>SNMP Agent (server)</td>
<td>iDRAC, OMSA, and CMC communication, used to manage and monitor the managed nodes.</td>
</tr>
<tr>
<td>User defined</td>
<td>Any</td>
<td>UDP/TCP</td>
<td>None</td>
<td>Out</td>
<td>OMIVV appliance to proxy server</td>
<td>Proxy</td>
<td>To communicate with the proxy server</td>
</tr>
</tbody>
</table>
### Table 13. Managed nodes (ESXi)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocols</th>
<th>Port Type</th>
<th>Maximum Encryption Level</th>
<th>Direction</th>
<th>Destination</th>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>162, 11620</td>
<td>SNMP</td>
<td>UDP</td>
<td>None</td>
<td>Out</td>
<td>ESXi to OMIVV appliance</td>
<td>Hardware Events</td>
<td>Asynchronous SNMP traps sent from ESXi. This port has to open from ESXi.</td>
</tr>
<tr>
<td>443</td>
<td>WSMAN</td>
<td>TCP</td>
<td>128-bit</td>
<td>In</td>
<td>OMIVV appliance to ESXi(OMSA)</td>
<td>IDRAC/OMSA communication</td>
<td>Used to provide information to the management station. This port has to open from ESXi.</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>TCP</td>
<td>128-bit</td>
<td>In</td>
<td>OMIVV appliance to ESXi</td>
<td>HTTPS server</td>
<td>Used to provide information to the management station. This port has to open from ESXi.</td>
</tr>
<tr>
<td>8080</td>
<td>HTTP</td>
<td>TCP</td>
<td>128-bit</td>
<td>Out</td>
<td>ESXi to OMIVV appliance</td>
<td>HTTP server; downloads the OMSA VIB and fixes noncompliant vSphere hosts</td>
<td>Helps ESXi to download the OMSA/driver VIB.</td>
</tr>
</tbody>
</table>

### Table 14. Managed nodes (IDRAC/CMC)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Protocols</th>
<th>Port Type</th>
<th>Maximum Encryption Level</th>
<th>Direction</th>
<th>Destination</th>
<th>Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>WSMAN/HTTPS</td>
<td>TCP</td>
<td>128-bit</td>
<td>In</td>
<td>OMIVV appliance to iDRAC/CMC</td>
<td>IDRAC communication</td>
<td>Used to provide information to the management station. This port has to open from iDRAC and CMC.</td>
</tr>
<tr>
<td>4433</td>
<td>HTTPS</td>
<td>TCP</td>
<td>128-bit</td>
<td>Out</td>
<td>iDRAC to OMIVV appliance</td>
<td>Auto Discovery</td>
<td>For auto discovering iDRAC (managed nodes) in the management station.</td>
</tr>
<tr>
<td>2049</td>
<td>NFS</td>
<td>UDP</td>
<td>None</td>
<td>In/Out</td>
<td>iDRAC to/from OMIVV</td>
<td>Public Share</td>
<td>For iDRAC to access NFS public share that is exposed by OMIVV appliance. That is used for OS deployment and firmware update. To access the iDRAC configurations from the OMIVV. Used in deployment flow.</td>
</tr>
<tr>
<td>4001 to 4004</td>
<td>NFS</td>
<td>UDP</td>
<td>None</td>
<td>In/Out</td>
<td>iDRAC to/from OMIVV</td>
<td>Public Share</td>
<td>For iDRAC to access NFS public share that is exposed by OMIVV appliance. This is used for OS deployment and firmware update. To access the iDRAC configurations from the OMIVV. Used in deployment flow.</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>UDP</td>
<td>128-bit</td>
<td>In/Out</td>
<td>iDRAC to/from OMIVV</td>
<td>Trivial File Transfer</td>
<td>Used for managing the iDRAC successfully from the management station.</td>
</tr>
</tbody>
</table>
**Prerequisite checklist**

Checklist before you start the product installation:

- Verify that you have user name and password for OMIVV to access the vCenter server. The user may have an administrator role that has all necessary permissions or a non-administrator user with the necessary privileges. For more information about the list of privileges required for OMIVV to operate, see Required privileges for non-administrator users.
- Check that you have the root password for the ESXi host systems, or the Active Directory credentials that has administrative rights on the host.
- Check whether you have the user name and password associated with iDRAC Express or Enterprise which have administrative rights on the iDRAC.
- Check if the vCenter server is running.
- Determine the location of the OMIVV installation directory.
- Check to ensure that VMware vSphere environment meet virtual appliance, port access, and listening port requirements. Also, install Adobe Flash Player on a client system, if necessary. For more information on the supported Flash Player version, see OpenManage Integration for VMware vCenter Compatibility Matrix.

**NOTE:** The virtual appliance functions as a regular virtual machine; any interruptions or shut downs impact overall functionality of the virtual appliance.

**NOTE:** The OMIVV shows the VMware tools as, Running (Out-of-date) when deployed on ESXi 5.5 and later. You can upgrade the VMware tools after a successful deployment of the OMIVV appliance or anytime later, if necessary.

**NOTE:** It is recommended that OMIVV and vCenter server are on the same network.

**NOTE:** The OMIVV appliance network should have access to iDRAC, host, and vCenter.

**Installing, configuring, and upgrading OMIVVV**

**Prerequisite**

Ensure that the hardware requirements are met and you are running the required VMware vCenter software.

**About this task**

The following high-level steps outline the overall installation and configuration procedure for OMIVV:

**Steps**

1. Download the DellEMC_OpenManage_Integration_<version number>.<build number>.zip file from the Dell support website at Dell.com/support.
2. Navigate to the location where you have downloaded the file, and extract its contents.
3. Deploy the Open Virtualization Format (OVF) file that contains the OMIVV appliance by using the vSphere web client. See Deploying the OMIVV OVF.
4. Upload the license file. For more information about licensing, see Uploading license.
5. Register the OMIVV appliance with the vCenter server by using Administration Console. See Registering OMIVV and importing the license file.
6. To configure the appliance, complete the Initial Configuration Wizard. See the Configuration tasks through the configuration wizard.

**Deploying OMIVV OVF using vSphere web client**

**Prerequisite**

Ensure that you have downloaded and extracted the product .zip file, Dell_OpenManage_Integration_<version number>.<build number>.zip from the Dell website.

**Steps**

1. Locate the OMIVV virtual disk that you downloaded and extracted, and run Dell_OpenManage_Integration.exe.

The supported client OS version for extracting and running the exe is Windows 7 SP1 and later.
The supported server OS version for extracting and running the exe is Windows 2008 R2 and later.

2 Accept EULA, and save the .OVF file.

3 Copy or move the .OVF file to a location accessible to the VMware vSphere host to which you upload the appliance.

4 Start the VMware vSphere Web Client.

5 From the VMware vSphere Web Client, select a host, and in the main menu click Actions > Deploy OVF Template. You can also right-click Host and select Deploy OVF Template.

The Deploy OVF Template wizard is displayed.

6 In the Select Source window, perform the following subtasks:
   a Select URL if you want to download the OVF package from Internet.
   b Select the Local file and click Browse if you want to select the OVF package from your local system.

   ✅ NOTE: The installation process can take between 10-30 minutes if the OVF package resides on a network share. For a quick installation, it is recommended that you host the OVF on a local drive.

7 Click Next.

The Review Details window is displayed with the following information:
   a Product—The OVF template name is displayed.
   b Version—The version of the OVF template is displayed.
   c Vendor—The vendor name is displayed.
   d Publisher—The publisher details are displayed.
   e Download Size—The actual size of the OVF template in gigabytes is displayed.
   f Size on Disk—Details of thick and thin provisioned details are displayed.
   g Description—The comments are displayed here.

8 Click Next.

The Select Name and Folder window is displayed.

9 In the Select Name and Folder window, perform the following substeps:
   a In Name, enter the name of the template. The name can include up to 80 characters.
   b In the Select a folder or datacenter list, select a location for deploying the template.

10 Click Next.

The Select Storage window is displayed.

11 In the Select Storage window, perform the following substeps:
   a In the Select Virtual Disk Format drop-down list, select either of the following formats:
      • Thick Provision (lazy Zeroed)
      • Thick Provision (Eager zeroed)
      • Thin Provision

      It is recommended that you select, Thick Provision (Eager Zeroed).
   b In the VM Storage Policy drop-down list, select a policy.

12 Click Next.

The Setup Networks window is displayed that includes details about the source and destination networks.

13 In the Setup Networks window, click Next.

   ✅ NOTE: It is recommended that the OMIVV appliance and the vCenter server are located in the same network.

14 In the Ready to Complete window, review the selected options for the OVF deployment task and click Finish.

The deployment job runs and provides a completion status window where you can track the job progress.

Uploading HTTPS certificate

Prerequisite
Ensure that the certificate uses PEM format.
You can use the HTTPS certificates for secure communication between the virtual appliance and host systems. To set up this type of secure communication, a CSR must be sent to a certificate authority and then the resulting certificate is uploaded using the Administration Console. There is also a default certificate that is self-signed and can be used for secure communication; this certificate is unique to every installation.

**NOTE:** You can use the Microsoft internet explorer, Firefox, Chrome to upload certificates.

**Steps**

1. In the **APPLIANCE MANAGEMENT** page, click **Upload Certificate** in the **HTTPS CERTIFICATES** area.
2. Click **OK** in the **UPLOAD CERTIFICATE** dialog box.
3. To select the certificate to be uploaded, click **Browse**, and then click **Upload**.
4. If you want to cancel the upload, click **Cancel**.

**NOTE:** If you want to upload a custom certificate for the appliance, ensure that you upload the new certificate prior to vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed in the web client. To fix this issue, unregister, and re-register the appliance with the vCenter.

**Restoring default HTTPS certificate**

1. In the **APPLIANCE MANAGEMENT** page, click **Restore Default Certificate** in the **HTTPS CERTIFICATES** area.
2. In the **RESTORE DEFAULT CERTIFICATE** dialog box, click **Apply**.

**Registering vCenter server by nonadministrator user**

You can register vCenter servers for the OMIVV appliance with vCenter administrator credentials or a nonadministrator user with the necessary privileges.

**About this task**

To enable a nonadministrator user with the required privileges to register a vCenter server, perform the following steps:

**Steps**

1. To change the privileges selected for a role, add the role and select the required privileges for the role or modify an existing role. See VMware vSphere documentation for the steps required to create or modify a role and select privileges in the vSphere web client. To select all the required privileges for the role, see the Required privileges for nonadministrator users.

   **NOTE:** The vCenter administrator should add or modify a role.

2. Assign a user to the newly created role after you define a role and select privileges for the role. See VMware vSphere documentation for more information about assigning permissions in the vSphere web client.

   **NOTE:** The vCenter administrator should assign permissions in the vSphere Client.

A vCenter server nonadministrator user with the required privileges can now register and/or unregister vCenter, modify credentials, or update the certificate.

3. Register a vCenter server by using a nonadministrator user with the required privileges. See Registering a vCenter server by a nonadministrator user with the required privileges.

4. Assign the Dell privileges to the role created or modified in step 1. See Assigning Dell privileges to the role in vSphere web client.

A nonadministrator user with the required privileges can now use the OMIVV features with the Dell EMC hosts.
Required privileges for nonadministrator users

To register OMIVV with vCenter, a nonadministrator user requires the following privileges:

1️⃣ **NOTE:** While registering a vCenter server with OMIVV by a nonadministrator user, an error message is displayed if the following privileges are not assigned:

- **Alarms**
  - Create alarm
  - Modify alarm
  - Remove alarm

- **Extension**
  - Register extension
  - Unregister extension
  - Update extension

- **Global**
  - Cancel task
  - Log event
  - Settings

2️⃣ **NOTE:** Assign the following health update privileges, if you are using VMware vCenter 6.5 or upgrading to vCenter 6.5 or later:

- **Health Update Provider**
  - Register
  - Unregister
  - Update

- **Host**
  - CIM
    - CIM Interaction
  - Configuration
    - Advanced settings
    - Connection
    - Maintenance
    - Network configuration
    - Query patch
    - Security profile and firewall

3️⃣ **NOTE:** Assign the following privileges, if you are using VMware vCenter 6.5 or upgrading to vCenter 6.5 or later:

- **Host.Config**
  - Advanced settings
  - Connection
  - Maintenance
  - Network configuration
  - Query patch
  - Security profile and firewall

- **Inventory**
  - Add host to cluster
  - Add standalone host
Modify cluster

**NOTE:** Ensure that you assign the modify cluster privilege, if you are using vCenter 6.5 or upgrading to vCenter 6.5 or later.

- Host profile
  - Edit
  - View
- Permissions
  - Modify permission
  - Modify role
- Sessions
  - Validate session
- Task
  - Create task
  - Update task

Registering vCenter server by nonadministrator user with required privileges

You can register a vCenter server for the OMIVV appliance by using a nonadministrator user with the required privileges. See step 5 to step 9 of Registering OpenManage Integration for VMware vCenter and importing license file for information about registering a vCenter server through a nonadministrator user or as an administrator.

Assigning Dell privileges to existing role

About this task
You can edit an existing role to assign the Dell privileges.

**NOTE:** Ensure that you are logged in as a user with Administrator privileges.

**Steps**

1. Log in to the vSphere web client with administrative rights.
2. In the left pane, click Administration → Roles in the vSphere web client.
3. Select a vCenter server system from the Roles provider drop-down list.
4. Select the role from the Roles list, and click ✍.
5. Click Privileges. expand Dell, and then select the following Dell privileges for the selected role and click OK:
   - Dell.Configuration
   - Dell.Deploy-Provisioning
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

See Security roles and permissions in OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals for more information about the available OMIVV roles within vCenter.

The changes to permissions and roles take effect immediately. The user with necessary privileges can now perform the OpenManage Integration for VMware vCenter operations.

**NOTE:** For all vCenter operations, OMIVV uses the privileges of the registered user and not the privileges of the logged-in user.

**NOTE:** If specific pages of OMIVV are accessed with no Dell privileges assigned to the logged-in user, the 2000000 error is displayed.
Registering OpenManage Integration for VMware vCenter and importing license file

Prerequisite
Ensure that your licenses are ready for download at http://www.dell.com/support/licensing. If you have ordered more than one license, they might be shipped separately at different times. You can check the status of other license items at Order status. The license file is available as an .XML format.

NOTE: If you want to upload a custom certificate for your appliance, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed in the web client. To fix this issue, unregister, and re-register the appliance with vCenter.

Steps
1. From the vSphere web client, click Home > Hosts and Clusters; then in the left panel, locate OMIVV that you had deployed, and click Power on the virtual machine.
   During deployment, if you select Power on after Deployment, the VM is powered on automatically after deployment is complete.
2. To run the Administration Console, click the Console tab in the main VMware vCenter window.
3. Allow OMIVV to complete booting up, and then enter the user name as, Admin (the default is Admin), and press Enter.
4. Enter a new admin password. Ensure that the admin password complies with the password complexity rules displayed in the interface. Press Enter.
5. Reenter the password that was provided earlier and press Enter.
   To configure the network and time zone information in the OMIVV appliance, press Enter.
6. To configure the OMIVV time zone information, click Date/Time Properties.

Figure 1. Console tab

In the Date and Time tab, select the Synchronize date and time over the network.
The **NTP Servers** box is displayed.

8 Add valid NTP server details to which your vCenter is synchronized with.

9 Click **Time Zone** and select the applicable time zone, and click **OK**.

10 To configure static IP to the OMIVV appliance, click **Network Configuration**, or skip to step 17.

11 Select **Auto eth0**, and then click **Edit**.

12 Select the **IPV4 Settings** tab, and select **Manual** in the **Method** drop-down.

13 Click **Add**, and then add a valid IP, Netmask, and Gateway information.

14 In the **DNS Servers** field, provide the DNS server detail.

15 Click **Apply**.

16 To change the host name of the OMIVV appliance, click **Change Hostname**.

17 Enter a valid host name, and click the **Update hostname**.

**NOTE:** After host name and NTP are changed, ensure that the system is rebooted.

**NOTE:** If any vCenter servers are registered with the OMIVV appliance, unregister and re-register all the vCenter instances.

Before opening the administration console, ensure that you manually update all references to the appliance such as, provisioning server in iDRAC, DRM.

18 Open **Administration Console** from a supported browser.

To open **Administration Console**, in the **Help and Support** tab of OpenManage Integration for VMware vCenter, click the link under **Administration Console** or start a web browser and provide the `https://<ApplianceIP or Appliance hostname>` url.

The IP address is the IP address of the appliance VM and not the ESXi host IP address. The Administration Console can be accessed by using the URL mentioned at the top of the console.

For example: `Https://10.210.126.120` or `Https://myesxihost`

The URL is not case-sensitive.

![Administration Console](image)

**Figure 2. Administration Console**

19 In the **Administration Console** login window, enter the password, and then click **Login**.
In the vCenter Registration window, click Register a New vCenter Server.

In the Register a New vCenter Server window, perform the following substeps:

- Under vCenter Name, in the vCenter Server IP or Hostname text box, enter the server IP or host name, and then in the Description text box, enter a description. The description is optional.

  **NOTE:** It is recommended that you register OpenManage Integration for VMware vCenter with the VMware vCenter by using Fully Qualified Domain Name (FQDN). Ensure that the host name of the vCenter is properly resolvable by the DNS server for FQDN-based registrations.

- Under vCenter User Account, in vCenter User Name, enter the Admin user name or the user name with necessary privileges. Enter the username as domain\user or domain\user or user@domain. OMIVV uses the Admin user account or the user with necessary privileges for vCenter administration.

- In Password, enter the password.

- In Verify Password, enter the password again.

22 Click Register.

**NOTE:** OpenManage Integration for VMware vCenter currently supports up to 1000 hosts for large deployment mode with a single vCenter instance or multiple vCenter servers by using the linked mode.

Perform one of the following actions:

- If you are using the OMIVV trial version, you can view the OMIVV icon.

- If you are using the full product version, the license file can be downloaded from the Dell Digital Locker at http://www.dell.com/support/licensing, and you can import this license to your virtual appliance. To import the license file, click Upload License.

24 In the Upload License window, click Browse to navigate to the license file, and then click Upload to import the license file.

**NOTE:** If you modify or edit the license file, the license file (.XML file) does not work and you can download the .XML file (license key) through the Dell Digital Locker. 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.

After OMIVV is registered, the OMIVV icon is displayed under the Administration category of the web client home page.
Example
For all vCenter operations, OMIVV uses the privileges of a registered user and not the privileges of a logged-in user.
For example: User X with the necessary privileges registers OMIVV with vCenter, and user Y has only Dell privileges. User Y can now log in to the vCenter and can trigger a firmware update task from OMIVV. While performing the firmware update task, OMIVV uses the privileges of user X to put the machine into maintenance mode or reboot the host.

Upgrading registered vCenter
You can upgrade a registered vCenter for non-administrator users or administrator users. Before upgrading a registered vCenter, see the VMware Documentation if you upgrade to the latest version of the vCenter server, such as vCenter 6.5. Perform the tasks in either of the following options after upgrading a registered vCenter, as applicable:

- For non-administrator users:
  a. Assign extra privileges to non-administrator users, if necessary. See Required privileges for nonadministrator users.
     For example, when you upgrade from vCenter 6.0 to vCenter 6.5, assign the extra privileges.
  b. Reboot the registered OMIVV appliance.
- For administrator users:
  a. Reboot the registered OMIVV appliance.

Verifying installation
About this task
The following steps verify that the OMIVV installation is successful:

Steps
1. Close any vSphere client windows, and start a new vSphere web client.
2. Confirm that the OMIVV icon appears inside vSphere web client.
3. Ensure that vCenter can communicate with OMIVV by attempting a PING command from the vCenter server to the virtual appliance IP address or host name.
In vSphere Web Client, click **Home > Administration > Solutions**, and click **Plug-In Management** (in older vCenter versions) or **Client Plug-ins** (in newer versions).

For more information about the access restrictions for **Plug-In Management** or **Client Plug-ins** page, see VMware documentation.

In the **Plug-In Management** or **Client Plug-Ins** window, verify if OMIVV is installed and enabled.

**Migrating from earlier version to 4.2**

**About this task**
You can start with a fresh deployment of the v4.2 OVF after uninstalling an earlier version and then migrate the data from earlier version to 4.2 version by using backup and restore path.

To migrate from an earlier version to the OMIVV 4.2 version, perform the following steps:

**Steps**

1. Take a backup of the database for an earlier (v4.x) release.
   For more information about backup, see OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals.

2. Power off the older appliance from vCenter.

   **NOTE:** Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes all the alarms registered on vCenter by the OMIVV plug-in and all the customization that is performed on the alarms such as, actions and so on. For more information, see OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2, if you have unregistered the plug-in after the backup.

3. Deploy the new OpenManage Integration version 4.2 OVF.
   For more information about deploying the OVF, see OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2.

4. Power on the OpenManage Integration version 4.2 appliance.

5. Set up the network and time zone on the OMIVV appliance.
   Ensure that the new OpenManage Integration version 4.2 appliance has the same IP address as the old appliance. To set up the network details, see OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2.

   **NOTE:** The OMIVV plug-in might not work properly if the IP address for the OMIVV 4.2 appliance is different from the IP address of the older appliance. In such a scenario, unregister and re-register all the vCenter instances.

6. Restore the database to the new OMIVV appliance.

   **NOTE:** If you have enabled Proactive HA on clusters, OMIVV unregisters the Dell Inc provider for those clusters and re-registers the Dell Inc provider after restore. Hence, health updates for the Dell hosts are not available until restore is complete.

   For more information, see Restoring the OMIVV database from a backup in the OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals.

7. Upload the new license file.
   For more information about licensing, see OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2.

8. Verify the appliance.
   For more information about appliance verification, see the OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 4.2 to ensure that the database migration is successful.

9. Run the **Inventory** on all the hosts.
NOTE:
It is recommended that after the upgrade, you run the inventory again on all the hosts that the OMIVV manages. For more information, see the Running inventory jobs in OpenManage Integration for VMware vCenter User’s Guide.

If the IP address of the new OMIVV version 4.2 appliance is changed from the old appliance, configure the trap destination for the SNMP traps to point to the new appliance. For 12th generation and higher generation servers, the IP change is fixed by running inventory on these hosts. For hosts earlier than 12th generation that were compliant with earlier versions, the IP change is displayed as noncompliant and requires you to configure Dell EMC OpenManage Server Administrator (OMSA). For more information on fixing the host compliance, see Reporting and fixing compliance for vSphere hosts in OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals.

Recovering OMIVV after unregistering earlier version of OMIVV

About this task
If you have unregistered the OMIVV plug-in after taking backup of the database of the earlier version, perform the following steps before proceeding with the migration:

NOTE: Unregistering the plug-in removes all the customization that was implemented on the registered alarms by the plug-in. The following steps do not restore the customization. However, it re-registers the alarms in their default state.

Steps
1. Perform step 3 through step 5 in Migrating from earlier version to 4.2.
2. Register the plug-in to the same vCenter that you had registered in the earlier plug-in.
3. To complete the migration, perform step 6 through step 9 in Migrating from earlier version to 4.2.
Appliance configuration for VMware vCenter

After you complete the basic installation of OMIVV and registration of the vCenters, the Initial Configuration Wizard is displayed when you click the OMIVV icon. You can proceed to configure the appliance by using one of the following methods:

- Configuring the appliance through the **Initial Configuration Wizard**.
- Configuring the appliance through the **Settings** tab in OMIVV.

You can use the **Initial Configuration Wizard** to configure the OMIVV appliance settings on first launch. For subsequent instances, use the **Settings** tab.

**NOTE:** The user interface in both the methods is similar.

Topics:

- Configuration tasks through configuration wizard
- Configuration tasks through settings tab
- Creating chassis profile

### Configuration tasks through configuration wizard

**NOTE:** If you view a web communication error while performing OMIVV-related tasks after changing the DNS settings; clear the browser cache, and log out from the web client and then log in again.

By using the configuration wizard, you can view and perform the following tasks:

- View configuration wizard welcome page
- Select vCenters. See **Selecting vCenters**.
- Create a connection profile. See **Creating a connection profile**.
- Configure events and alarms. See **Configuring events and alarms**.
- Schedule inventory jobs. See **Scheduling inventory jobs**.
- Run a warranty retrieval job. See **Running a warranty retrieval job**.

### Viewing configuration wizard welcome dialog box

To configure OMIVV after installing and registering with the vCenter, perform the following steps to view the **Initial configuration Wizard**:

1. In vSphere web client, click **Home**, and then click the **OpenManage Integration** icon. You can perform any one of the following options to access the initial configuration wizard:
   - The first time you click the **OpenManage Integration** icon, **Initial Configuration Wizard** is displayed automatically.
   - From **OpenManage Integration > Getting Started**, click **Start Initial Configuration Wizard**.

2. In the **Welcome** dialog box, review the steps, and then click **Next**.
Selecting vCenters

About this task
In the vCenter Selection dialog box, you can configure the following vCenters:

• A specific vCenter
• All registered vCenters

To access the vCenter Selection dialog box:

Steps
1. In the Initial Configuration Wizard, in the Welcome dialog box, click Next.
2. Select one vCenter or all registered vCenters from the vCenters drop-down list.
   Select a vCenter that is not configured yet or if you have added a vCenter to your environment. The vCenter selection page allows you to select one or more vCenters to configure settings.
3. To proceed with the Connection Profile Description dialog box, click Next.

NOTE: If you have multiple vCenter servers that are part of the same single sign-on (SSO) registered with the same OMIVV appliance, and if you choose to configure a single vCenter server, repeat steps 1 through 3 until you configure each vCenter.

Creating connection profile

Prerequisites
Before using the Active Directory credentials with a connection profile, ensure that:

• The Active Directory user’s account exists in Active Directory.
• The iDRAC and host are configured for Active Directory based authentication.

About this task
A connection profile stores the iDRAC and host credentials that OMIVV uses to communicate with the Dell EMC servers. Each Dell EMC server must be associated with a connection profile to be managed by OMIVV. You might assign multiple servers to a single connection profile. You can create a connection profile by using the configuration wizard or from the OpenManage Integration for VMware vCenter > Settings tab. You can log in to iDRAC and the host by using the Active Directory credentials.

NOTE: The Active Directory credential can be either same or separate for both iDRAC and the host.

NOTE: You cannot create a connection profile if the number of added hosts exceeds the license limit for creating a connection profile.

Steps
1. In the Connection Profile Description dialog box, click Next.
2. In the Connection Profile Name and Credentials dialog box, enter the connection Profile Name and connection profile Description, which is optional.
3. In the Connection Profile Name and Credentials dialog box, under iDRAC Credentials, do either of the following actions, depending on configuring iDRAC with or without Active Directory:

NOTE: The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, applying system profiles in 14th generation servers, and deploying hypervisor.

• The iDRAC IPs that are already configured and enabled for Active Directory on which you want to use Active Directory, select Use Active Directory; otherwise scroll down to configure the iDRAC credentials.
  1. In Active Directory User Name, type the user name. Type the user name in one of these formats: domain\username or username@domain. The user name is limited to 256.
  2. In Active Directory Password, type the password. The password is limited to 127 characters.
3 In **Verify Password**, type the password again.

4 Depending on your requirement, perform one of the following actions:
   - To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
   - To not store and perform the iDRAC certificate check during all future connections, clear **Enable Certificate Check**.

   • To configure the iDRAC credentials without Active Directory, perform the following tasks:
      1 In **User Name**, type the user name. The user name is limited to 16 characters. See the iDRAC Documentation for information about user name restrictions for the version of iDRAC that you are using.
      2 In **Password**, type the password. The password is limited to 20 characters.
      3 In **Verify Password**, type the password again.
      4 Perform one of the following actions:
         - To download and store the iDRAC certificate, and validate it during all future connections, select **Enable Certificate Check**.
         - To not store and perform the iDRAC certificate check during all future connections, clear **Enable Certificate Check**.

4 In **Host Root**, perform one of the following steps:
   - The hosts that are already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**, and perform the following steps; otherwise configure your host credentials:
      1 In Active Directory **User Name**, type the user name. Type the user name in one of these formats: `domain\username` or `username@domain`. The user name is limited to 256 characters.
         **NOTE:** For host user name and domain restrictions, see the following:
         Host user name requirements:
         - Between 1 and 64 characters long
         - No nonprintable characters
         - No Invalid characters, such as " / \ [ ] : ; | = , + * ? < > @
         Host domain requirements:
         - Between 1 and 64 characters long
         - First character must be alphabetical.
         - Cannot contain a space.
         - No Invalid characters, such as " / \ [ ] : ; | = , + * ? < > @
      2 In Active Directory **Password**, type the password. The password is limited to 127 characters.
      3 In **Verify Password**, type the password again.
      4 Perform one of the following actions:
         - To download and store the host certificate, and validate it during all future connections, select **Enable Certificate Check**.
         - To not store and perform the host certificate check during all future connections, clear **Enable Certificate Check**.

   • To configure host credentials without Active Directory, perform the following tasks:
      1 In **User Name**, the user name is `root`, which is the default user name and you cannot change the user name. However, if the Active Directory is set, you can choose any Active Directory user and not root.
      2 In **Password**, type the password. The password is limited to 127 characters.
         **NOTE:** The OMSA credentials are the same credentials that are used for the ESXi hosts.
      3 In **Verify Password**, type the password again.
      4 Perform one of the following actions:
         - To download and store the host certificate, and validate it during all future connections, select **Enable Certificate Check**.
         - To not store and perform the host certificate check during all future connections, clear **Enable Certificate Check**.

5 Click **Next**.

6 In the **Connection Profile Associated Hosts** dialog box, select the hosts for the connection profile and click **OK**.

7 To test the connection profile, select one or more hosts and click **Test Connection**.
NOTE: This step is optional, and checks the host and iDRAC credentials. Although this step is optional, it is recommended that you test the connection profile.

NOTE: The test connection fails for all hosts running ESXi 6.5 and/or later that has the WBEM service disabled. For such hosts, WBEM service is automatically enabled when you perform inventory on those hosts. Although the test connection fails, it is recommended that you complete the connection profile wizard actions, run the inventory on the hosts, and then test the connection profile again.

To complete the creation of profile, click Next. After you click next, all details that you provide in this wizard is saved and you cannot modify the details from the wizard. You can modify or create more connection profiles for this vCenter detail from the Manage > Profiles Connection Profiles page after completing the configuration from the configuration wizard. See Modifying connection profile topic in this guide. Modifying connection profile in OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals.

NOTE: The servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result is not applicable for this system.

After hosts are added to connection profile, the IP address of OMIVV is automatically set to SNMP trap destination of host’s iDRAC, and OMIVV automatically enables the Web-Based Enterprise Management (WBEM) service for ESXi 6.5 hosts. OMIVV uses the WBEM service to properly synchronize the ESXi host and the iDRAC relationships. If configuring the SNMP trap destination fails for particular hosts, and/or enabling the WBEM service fails for particular hosts, those hosts are listed as noncompliant. To view the noncompliant hosts that require SNMP trap destination to be reconfigured and/or WBEM services to be enabled, see Reporting and fixing compliance for vSphere hosts topic in OpenManage Integration for VMware vCenter User’s Guide available at Dell.com/support/manuals.

## Scheduling inventory jobs

**About this task**

You can configure inventory schedule by using the configuration wizard or OpenManage Integration under the OpenManage Integration > Manage > Settings tab.

**NOTE:** To ensure that OMIVV continues to display updated information, it is recommended that you schedule a periodic inventory job. The inventory job consumes minimal resources and does not degrade host performance.

**NOTE:** The chassis gets discovered automatically after the inventory for all hosts is run. If the chassis is added to a chassis profile, the chassis inventory automatically runs. In an SSO environment with multiple vCenter servers, the chassis inventory runs automatically with every vCenter when the inventory for any vCenter is run at a scheduled time.

**NOTE:** The settings in this page are reset to default each time the configuration wizard is invoked. If you have previously configured a schedule for inventory, ensure that you replicate the previous schedule in this page before completing the wizard functions so that the previous schedule is not overridden by the default settings.

**Steps**

1. In the Initial Configuration Wizard, from the Inventory Schedule dialog box, select Enable Inventory Data Retrieval, if it is not enabled. By default, Enable Inventory Data Retrieval is enabled.

2. Under Inventory Data Retrieval Schedule, perform the following steps:
   a. Select the check box next to each day of the week that you want to run the inventory. By default, all the days are selected.
   b. In Data Retrieval Time, enter the time in HH:MM format.

   The time you enter is your local time. Therefore, if you want to run the inventory at the virtual appliance time zone, calculate the time difference between your local and virtual appliance time zone, and then enter the time appropriately.
   c. To apply the changes and continue, click Next.

   Once you click next, all details that you provide in this wizard is saved and you cannot modify the details from this wizard. You can modify inventory schedule details of the hosts from the Manage > Settings tab after completing the configuration from the configuration wizard. See Modifying inventory job schedules in the OpenManage Integration for VMware vCenter User’s Guide at Dell.com/support/manuals.
Running warranty retrieval jobs

About this task
The warranty retrieval job configuration is available from the Settings tab in OMIVV. In addition, you can also run or schedule warranty retrieval job from Job Queue > Warranty. The scheduled jobs are listed in the job queue. In an SSO environment with multiple vCenter servers, the chassis warranty runs automatically with every vCenter when the warranty for any vCenter is run. However, warranty does not automatically run if it is not added to chassis profile.

NOTE: The settings in this page are reset to default each time the configuration wizard is invoked. If you have previously configured a warranty retrieval job, ensure that you replicate that schedule warranty retrieval job in this page before completing the wizard functions so that the previous warranty retrieval is not overridden by the default settings.

Steps
1. In the Warranty Schedule dialog box, select Enable Warranty Data Retrieval.
2. In Warranty Data Retrieval Schedule, do the following:
   a. Select the check box next to each day of the week that you want to run the warranty.
   b. Enter the time in HH:MM format.
      The time you enter is your local time. Therefore, if you want to run the inventory at the virtual appliance time zone, calculate the time difference between your local and virtual appliance time zone, and then enter the time appropriately.
3. To apply the changes and continue, click Next, and then proceed with the Event and Alarm settings.

Configuring events and alarms

You can configure events and alarms by using the Initial Configuration Wizard or from the Settings tab for events and alarms. To receive events from the servers, OMIVV is configured as trap destination. For 12th generation hosts and later, ensure that the SNMP trap destination is set in iDRAC. For hosts earlier than 12th generation, ensure that the trap destination is set in OMSA.

About this task

NOTE: OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later and supports only SNMP v1 alerts for hosts earlier than 12th generation.

Steps
1. In the Initial Configuration Wizard, under Event Posting Levels, select one of the following:
   - Do not post any events—block hardware events
   - Post all events—post all hardware events
   - Post only Critical and Warning events—post only critical or warning level hardware events
   - Post only Virtualization-Related Critical and Warning Events—post only virtualization-related critical and warning event, which is the default event posting level
2. To enable all hardware alarms and events, select Enable Alarms for all Dell EMC Hosts.
   NOTE: The Dell EMC hosts that have alarms enabled respond to some specific critical events by entering in to maintenance mode and you can modify the alarm, when required.

The Enabling Dell EMC Alarm Warning dialog box is displayed.
3. To accept the change, click Continue, or to cancel the change, click Cancel.
   NOTE: Ensure that you complete this step only if you select Enable Alarms for all Dell EMC Hosts.
4. To restore the default vCenter alarm settings for all managed Dell EMC servers, click Restore Default Alarms.
   It might take up to a minute before the change takes effect.
NOTE: After restoring the appliance, the events and alarms settings are not enabled even if the GUI shows as enabled. You can enable the Events and Alarms settings again from the Settings tab.

NOTE: BMC Traps do not have Message IDs, so alerts will not have these details in OMIVV.

5 Click Apply.

Configuring SNMP trap community string

1 In the OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under Appliance Settings, click against the OMSA SNMP Trap Community String.

The OMSA SNMP Trap Community String Settings dialog box is displayed. By default, 'public' is displayed in the SNMP trap community string.

2 Customize the 'public' text to any string, and click Apply.

NOTE: The SNMP trap community string configuration for 11th generation of PowerEdge servers is set while installing or upgrading OMSA through OMIVV.

Configuration tasks through settings tab

By using the settings tab, you can view and perform the following configuration tasks:

- Enable the OMSA link. See Enabling OMSA link.
- Configure warranty expiration notification settings. See the Configuring warranty expiration notification settings.
- Set up the firmware update repository. See Setting up the firmware update repository.
- Configure the latest appliance version notification. See Configuring the latest appliance version notification.
- Configure and view events and alarms. See the Configuring events and alarms.
- View data retrieval schedules for inventory and warranty. See the Viewing data retrieval schedules for inventory and warranty.

Appliance settings

In this section, configure the following for the OMIVV appliance:

- Warranty expiration notification
- Firmware update repository
- Latest appliance version notification
- Deployment credentials

Configuring warranty expiration notification settings

1 In OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under Appliance Settings, click Warranty Expiration Notification.

2 Expand Warranty Expiration Notification to view the following:
   - Warranty Expiration Notification—whether the setting is enabled or disabled
   - Warning—number of days for the first warning setting
   - Critical—number of days for the critical warning setting

3 To configure warranty expiration thresholds for warning about warranty expiration, click the pencil icon at the right side of Warranty Expiration Notification.

4 In the Warranty Expiration Notification dialog box, do the following:
a. If you want to enable this setting, select the **Enable warranty expiration notification for hosts.** Selecting the check box enables warranty expiration notification.

b. Under **Minimum Days Threshold Alert**, do the following:
   1. In the **Warning** drop-down list, select the number of days before you want to be warned of the warranty expiration.
   2. In the **Critical** drop-down list, select the number of days before you want to be warned of the warranty expiration.

5. Click **Apply**.

### Setting up firmware update repository

**About this task**
You can set up the firmware update repository on the OMIVV **Settings** tab.

**Steps**
1. In OpenManage Integration for VMware vCenter, on the **Manage > Settings** tab, under **Appliance Settings** at the right side of **Firmware Update Repository**, click the **icon**.
2. In the **Firmware Update Repository** dialog box, select one of the following:
   - **Dell Online**—you can access the location that uses the firmware update repository of Dell (Ftp.dell.com). The OpenManage Integration for VMware vCenter downloads selected firmware updates from the Dell repository and updates the managed hosts.
   - **Shared Network Folder**—you can have a local repository of the firmware in a CIFS-based or NFS-based network share. This repository can either be a dump of Server Update Utility (SUU) that Dell releases periodically or a custom repository created using DRM. This network share should be accessible by OMIVV.

   **NOTE:** Based on the network settings, enable proxy settings if network needs proxy.

   **NOTE:** If you are using CIFS share, the repository passwords cannot exceed 31 characters.

   **NOTE:** Ensure that you use the latest DRM version (3.x) and later.

3. If you select **Shared Network Folder**, enter the **Catalog File Location** by using the following format:
   - NFS share for .XML file—host:/share/filename.xml
   - NFS share for .gz file—host:/share/filename.gz
   - CIFS share for .XML file—\host\share\filename.xml
   - CIFS share for .gz file—\host\share\filename.gz

   **NOTE:** OMIVV supports only Server Message Block (SMB) version 1.0 and SMB version 2.0 based CIFS shares.

   **NOTE:** If you are using CIFS share, OMIVV prompts you to enter the user name and password. The @, %, and , characters are not supported for use in shared network folder user names or passwords.

4. Click **Apply** after downloading is complete.

**NOTE:** It might take up to 60 to 90 minutes to read the catalog from the source and update the OMIVV database.

### Configuring latest appliance version notification

**About this task**
To receive periodic notification about the availability of latest version (RPM, OVF, RPM/OVF) of OMIVV, perform the following steps to configure the latest version notification:

**Steps**
1. In the OpenManage Integration for VMware vCenter, on the **Manage > Settings** tab, under **Appliance Settings**, at the right side of **Latest Version Notification**, click the **icon**.
   By default, the latest version notification is disabled.

2. In the **Latest Version Notification and Retrieval Schedule** dialog box, perform the following actions:
   a. If you want to enable latest version notification, select the **Enable Latest Version notification** check box.
b. Under Latest Version Retrieval Schedule, select the days of the week for this job.

c. In Latest Version Retrieval Time, specify the required local time.

   The time you provide is your local time. Ensure that you calculate any time difference for running this task at a proper time on the OMIVV appliance.

To save the settings, click Apply, to reset the settings, click Clear, and to abort the operation, click Cancel.

### Configuring deployment credentials

The deployment credentials allow you to set up credentials to communicate securely with a bare-metal system that is discovered using auto discovery until the OS deployment is complete. For secure communication with iDRAC, OMIVV uses deployment credentials from initial discovery until the end of the deployment process. Once the OS deployment process is successfully complete, OMIVV changes the iDRAC credentials as provided in the connection profile. If you change the deployment credentials, all newly discovered systems from that point onwards are provisioned with the new credentials. However, the credentials on servers that are discovered prior to the change of deployment credentials are not affected by this change.

**About this task**

**NOTE:** OMIVV acts as a provisioning server. The deployment credentials allow you to communicate with iDRAC that uses the OMIVV plug-in as a provisioning server in the auto discovery process.

**Steps**

1. In OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under Appliance Settings, at the right side of Deployment Credentials, click the pencil icon.
2. In Credentials for Bare Metal Server Deployment, under Credentials, enter the values for the following:
   - In the User Name text box, enter the user name.
     The user name should be 16 characters or less (only ASCII printable characters).
   - In the Password text box, enter the password.
     The password should be 20 characters or less (only ASCII printable characters).
   - In the Verify Password text box, enter the password again.
     Ensure that the passwords match.
3. To save the specified credentials, click Apply.

### vCenter settings

In this section, configure the following vCenter settings:

- Enable the OMSA link. See Enabling the OMSA link.
- Configure events and alarms. See the Configuring events and alarms.
- Configure the data retrieval schedules for inventory and warranty. See the Viewing data retrieval schedules for inventory and warranty.

### Enabling OMSA link

**Prerequisite**

Install and configure an OMSA web server before enabling the OMSA link. See the OpenManage Server Administrator Installation Guide for the version of OMSA in use and for instructions on how to install and configure the OMSA web server.

**About this task**

**NOTE:** OMSA is only required on PowerEdge 11th generation servers or earlier.
Steps

1. In the OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under vCenter Settings and at the right side of the OMSA web server URL, click the icon.

2. In the OMSA Web Server URL dialog box, type the URL.
   Ensure that you include the complete URL, along with the HTTPS and port number 1311.
   
   \[https://<OMSA \text{server IP or fqdn}:1311]\]

3. To apply the OMSA URL to all vCenter servers, select Apply these settings to all vCenters.

   Notes: If you do not select the check box, the OMSA URL is applied only to one vCenter.

4. To verify that the OMSA URL link that you provided works, navigate to the Summary tab of the host and check that the OMSA console link is live within the Dell EMC Host Information section.

### Configuring events and alarms

About this task

The Dell EMC Management Center events and alarms dialog box enables or disables all hardware alarms. The current alert status is displayed on the vCenter alarms tab. A critical event indicates actual or imminent data loss or system malfunction. A warning event is not necessarily significant, but can indicate a possible future problem. The events and alarms can also be enabled by using the VMware Alarm Manager. The events are displayed on the vCenter tasks and events tab in the hosts and clusters view. To receive the events from the servers, OMIVV is configured as the SNMP trap destination. For 12th generation hosts and later, the SNMP trap destination is set in iDRAC. For hosts earlier than 12th generation, trap destination is set in OMSA. You can configure events and alarms using the OpenManage Integration for VMware vCenter from the Management > Settings tab. Under vCenter Settings, expand the Events and Alarms heading to display the vCenter alarms for Dell EMC Hosts (Enabled or Disabled), and the Event Posting Level.

Notes:

- OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later. For hosts earlier than 12th generation, OMIVV supports SNMP v1 alerts.
- To receive the Dell events, enable both alarms and events.

Steps

1. In the OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under vCenter settings, expand Events and Alarms.
   The current vCenter Alarms for Dell EMC Hosts (Enabled or Disabled) or all vCenter alarms, and Event Posting Level are displayed.

2. Click the icon at the right side of Events and Alarms.

3. To enable all hardware alarms and events, select Enable Alarms for all Dell EMC Hosts.

   Notes: The Dell EMC hosts that have alarms enabled respond to critical events by entering into maintenance mode and you can modify the alarm, as needed.

4. To restore the default vCenter alarm settings for all managed Dell servers, click Restore Default Alarms.
   This step can take up to a minute before the change takes effect and is available only if Enable Alarms For Dell EMC Hosts is selected.

5. In Event Posting Level, select either “Do not post any events”, “Post All Events”, “Post only Critical and Warning Events”, or “Post only Virtualization-Related Critical and Warning Events”. For more information, see the Events, alarms, and health monitoring section in OpenManage Integration for VMware vCenter User’s Guide.

6. If you want to apply these settings to all vCenters, select Apply these settings to all vCenters.

   Notes: Selecting the option overrides the existing settings for all vCenters.

7. To save, click Apply.
Viewing data retrieval schedules for inventory and warranty

1 In the OpenManage Integration for VMware vCenter, on the Manage > Settings tab, under vCenter Settings, click Data Retrieval Schedule.

On clicking, data retrieval schedule expands to expose the edit options for inventory and warranty.

2 Click the icon against Inventory Retrieval or Warranty Retrieval.

In the Inventory/Warranty Data Retrieval dialog box, you can view the following information for inventory or warranty retrieval:

• Whether the inventory and/or warranty retrieval option is enabled or disabled?
• The weekdays for which it is enabled.
• The time of day it is enabled.

3 To edit the data retrieval schedules, perform the following steps:
   a Under Inventory/Warranty Data, select the Enable Inventory/Warranty Data Retrieval check box.
   b Under Inventory/Warranty Data Retrieval Schedule, select the days of the week for your job.
   c In the Inventory/Warranty Data Retrieval Time text box, type the local time for this job.
      You might need to consider the time difference between job configuration and job implementation.
   d To save the settings, click Apply, to reset the settings, click Clear, and to abort the operation, click Cancel.

4 Click Data Retrieval Schedule again to contract the inventory and warranty schedules and display a single line.

Creating chassis profile

A chassis profile is required to monitor the chassis. A chassis credential profile can be created and associated with a single or multiple chassis.

About this task
You can log in to iDRAC and the host by using Active Directory credentials.

Steps
1 In OpenManage Integration for VMware vCenter, click Manage.
2 Click Profiles, and then click Credential Profiles.
3 Expand Credential Profiles, and click the Chassis Profiles tab.
4 In the Chassis Profiles page, click the icon to create a New Chassis Profile.
5 In the Chassis Profile Wizard page, do the following:
   a In the Name and Credentials section, under Chassis Profile:
      a In the Profile Name text box, enter the profile name.
      b In the Description text box, enter description, which is optional.

   Under the Credentials section:
      a In the User Name text box, type the user name with administrative rights, which is typically used to log in to the Chassis Management Controller.
      b In the Password text box, type the password for the corresponding user name.
      c In the Verify Password text box, enter the same password you have entered in the Password text box. The passwords must match.

   NOTE: The credentials can be a local or the Active Directory credentials. Before using the Active Directory credentials with a Chassis Profile, the Active Directory user’s account must exist in Active Directory and the Chassis Management Controller must be configured for Active Directory based authentication.
6 Click Next.

The Select Chassis page is displayed which shows all the available chassis.

NOTE: Chassis are discovered and available to be associated with the chassis profile only after the successful inventory run of any modular host present under that chassis.
To select either an individual chassis or multiple chassis, select the corresponding check boxes next to the **IP/Host Name** column. If the selected chassis is already a part of another profile, then a warning message is displayed, stating that the selected chassis is associated with a profile.

For example, you have a profile **Test** associated with Chassis A. If you create another profile **Test 1** and try to associate Chassis A to **Test 1**, a warning message is displayed.

Click **OK**.

The **Associated Chassis** page is displayed.

To test the chassis connectivity, select the chassis and click the **icon**, which verifies the credentials, and the result is displayed in the **Test Result** column as **Pass** or **Fail**.

To complete the profile, click **Finish**.
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

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.
In addition to this guide, you can access the other guides available at Dell.com/support. Click **Choose from all products**, then click **Software and Security > Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 4.2** to access the following documents:

- **OpenManage Integration for VMware vCenter Version 4.2 Web Client User’s Guide**
- **OpenManage Integration for VMware vCenter Version 4.2 Release Notes**
- **OpenManage Integration for VMware vCenter Version 4.2 Compatibility Matrix**

You can find the technical artifacts including white papers at delltechcenter.com. On the Dell TechCenter Wiki home page, click **Systems Management > OpenManage Integration for VMware vCenter** to access the articles.