# OpenManage Integration for VMware vCenter Version 4.3

## Web Client User's Guide

October 2018
Rev. A00

## 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

**Chapter 1: Introduction.......... 9**
Whats new in this release..........9
OpenManage Integration for VMware vCenter features..........9

**Chapter 2: About Administration Console.......... 11**
Using Administration Portal..........11
Registering vCenter server..........11
Registering vCenter Server by non-administrator user..........13
Uploading license to Administration Portal.......... 15
Managing the virtual appliance.......... 15
Setting up global alerts..........20
Managing backup and restore..........20
About vSphere client console..........21

**Chapter 3: Managing multiple appliances..........24**

**Chapter 4: Accessing OpenManage Integration from web client.......... 25**
Navigating in VMware vCenter web client.......... 25
Icons in web client..........26
Locating software version..........26
Refreshing screen content..........26
Viewing Dell EMC hosts..........26
Viewing OEM hosts..........27
Viewing Dell EMC chassis..........27
Viewing OpenManage Integration for VMware vCenter licensing tab..........28
Accessing help and support..........28
Downloading troubleshooting bundle..........29
Resetting iDRAC..........29
Opening online help..........30
Launching Administration Console.......... 30
Viewing log history..........30
Viewing logs..........31
Exporting log files..........31

**Chapter 5: OpenManage Integration for VMware vCenter licensing.......... 32**
Buying and uploading software license..........32

**Chapter 6: Appliance configuration for VMware vCenter.......... 33**
Configuration tasks through configuration wizard..........33
Viewing configuration wizard welcome dialog box..........33
Selecting vCenters..........33
Creating connection profile..........34
Scheduling inventory jobs .......... 36
Running warranty retrieval jobs..........36

Configuring events and alarms ........ 37
Configuration tasks through settings tab ........ 37
Appliance settings ........ 37
vCenter settings ........ 40

**Chapter 7: Using Baseline tab ........ 42**
Repository profile ........ 42
Creating repository profile ........ 43
Editing repository profile ........ 43
Deleting repository profile ........ 44
Cluster profile ........ 44
Creating cluster profile ........ 44
Editing cluster profile ........ 45
Deleting cluster profile ........ 46

**Chapter 8: Profiles ........ 47**
About connection profile ........ 47
Viewing connection profiles ........ 47
Creating connection profile ........ 48
Modifying connection profile ........ 50
Deleting connection profile ........ 51
Testing connection profile ........ 51
About chassis profile ........ 52
Viewing chassis profiles ........ 52
Creating chassis profile ........ 53
Editing chassis profile ........ 54
Deleting chassis profiles ........ 54
Testing chassis profile ........ 55

**Chapter 9: Inventory and warranty management ........ 56**
Inventory jobs ........ 56
Viewing host inventory ........ 56
Viewing chassis inventory ........ 57
Modifying inventory job schedules ........ 58
Running inventory jobs ........ 58
Running chassis inventory job now ........ 59
Warranty jobs ........ 59
Viewing warranty history ........ 59
Viewing chassis warranty ........ 60
Modifying warranty job schedules ........ 61
Running host warranty job now ........ 61
Running chassis warranty job now ........ 61
Monitoring single host ........ 61
Viewing host summary details ........ 61
Viewing hardware details for a single host ........ 64
Viewing storage details for a single host ........ 65
About system event logs in web client ........ 68
Viewing additional hardware details for a single host ........ 69
Monitoring hosts on clusters and data centers ........ 70

Viewing overview of data centers and clusters..... 70
Viewing hardware details for data centers and clusters..... 71
Viewing storage details for data center and clusters..... 73
Viewing additional hardware details for data center and clusters..... 75
Setting up physical server blink indicator light..... 76
Configuring System Lockdown Mode..... 76

**Chapter 10: Events, alarms, and health monitoring..... 78**
About events and alarms for hosts..... 78
About events and alarms for chassis..... 79
Viewing chassis events..... 79
Viewing chassis alarms..... 79
Virtualization-related events..... 80
Proactive HA events..... 87
Viewing alarms and events setting..... 88
Viewing events..... 89
Hardware component redundancy health—Proactive HA..... 89
Configuring Proactive HA for Rack and Tower servers ..... 90
Enabling Proactive HA on clusters..... 90
Overriding severity of health update notification..... 91
Launching management consoles..... 91
Launching Remote Access console..... 92
Launching OMSA console..... 92
Launching the Chassis Management Controller or Management Module console..... 92

**Chapter 11: About firmware updates..... 93**
Updating firmware for an MX server managed using chassis..... 93
Running firmware update wizard for non-vSAN host..... 94
Running firmware update wizard for vSAN host..... 95
Running firmware update wizard for non-vSAN clusters..... 97
Running firmware update wizard for vSAN clusters..... 99

**Chapter 12: Chassis management..... 101**
Managing MX7000X Chassis..... 101
Chassis and host management using the Unified Chassis Management IP ..... 102
Adding an MX Chassis ..... 102
Viewing chassis summary details..... 103
Viewing hardware inventory information for chassis..... 103
Viewing additional hardware configuration for chassis..... 106
Viewing associated host for chassis..... 108
Viewing related chassis information..... 108

**Chapter 13: Deploying hypervisor..... 110**
Device discovery..... 111
Manual discovery..... 111
Auto discovery in OpenManage Integration for VMware vCenter..... 111
Removing bare-metal server..... 114
Provisioning..... 114
System profiles..... 115

Creating system profile......116
Managing System profiles...... 117
Configuring hardware profile...... 117
Enabling CSIOR on reference server......118
Creating or customizing hardware profile ......118
Creating or cloning hardware profile......120
Managing hardware profiles......120
Creating hypervisor profile......121
Managing hypervisor profiles......121
Creating deployment templates...... 122
Managing deployment templates......122
About deployment wizard......123
VLAN support...... 123
Running Deployment Wizard......124
Managing deployment jobs using Job Queue......126
Managing firmware update jobs......128
Deployment job timing......129
Downloading custom Dell EMC ISO images...... 129

**Chapter 14: About host, bare-metal, and iDRAC compliance......130**
Reporting and fixing compliance for vSphere hosts...... 130
Fixing iDRAC license compliance for vSphere hosts......132
Support for OEM servers...... 132
Adding OEM hosts......132
Viewing baseline compliance......133
Using OMSA with 11th generation servers...... 134
Deploying OMSA agent on the ESXi system......134
Setting up OMSA trap destination...... 134
Reporting and fixing compliance for bare-metal servers......135
Fixing iDRAC license compliance for bare-metal servers......136
Refreshing bare-metal servers...... 136

**Chapter 15: Security roles and permissions...... 137**
Data integrity...... 137
Access control authentication, authorization, and roles...... 137
Dell Operational role......138
Dell Infrastructure Deployment role...... 138
About privileges......138

**Chapter 16: Frequently Asked Questions-FAQ...... 140**
Frequently Asked Questions-FAQ...... 140
Export All button fails to export to .CSV file in Google chrome......140
iDRAC license type and description are displayed incorrectly for non-compliant vSphere hosts......140
Dell provider is not displayed as health update provider......140
Inventory failing when performing firmware update task on ESXi 5.x host......141
Host inventory or test connection fails due to invalid or unknown iDRAC IP. ...... 141
On running fix noncompliant vSphere hosts wizard, the status of a specific host is displayed as Unknown......141
Dell privileges that are assigned while registering the OMIVV appliance are not removed after unregistering OMIVV...... 141

OMIVV does not display all the relevant logs when trying to filter a severity category.......... 142
How do I resolve error code 2000000 caused by VMware Certificate Authority-VMCA..........142
In Administration Console, **Update Repository Path** is not set to default path after I reset appliance to factory settings.......... 146
Warranty and inventory schedule for all vCenters is not applying when selected from the job queue page.......... 146
What should I do when a web communication error in the vCenter web client appears after changing the DNS settings in OMIVV.......... 146
The settings page fail to load, if I navigate away and again go back to the settings page.......... 146
Task cannot be scheduled for the time in the past- error in inventory schedule and warranty schedule page of Initial Configuration Wizard appear.......... 146
Installation date appears as 12-31-1969 for some of the firmware on the firmware page..........147
Successive global refresh cause exception to be thrown in the recent task window. ..........147
Why is web client UI distorted for few Dell screens in IE 10.......... 147
I am not seeing OpenManage Integration icon in web client even if registration of plug-in to vCenter was successful.......... 147
Even if repository has bundles for selected 11G system, firmware update displaying that there are no bundles for firmware update.......... 147
Why is DNS configuration settings restored to original settings after appliance reboot if appliance IP and DNS settings are overwritten with DHCP values.......... 148
Using OMIVV to update the Intel network card with firmware version of 13.5.2 is not supported...... 148
Using OMIVV to update Intel network card from 14.5 or 15.0 to 16.x fails due to staging requirement from DUP.......... 148
Why trying firmware update with invalid DUP, hardware update job status on vCenter console neither fails nor times-out for hours, although job status in LC prompts as FAILED.......... 148
Why does Administration Portal display unreachable update repository location..........148
Why did system not enter maintenance mode when I performed one-to-many firmware update........149
Chassis global health still healthy when some of power supply status has changed to critical............149
Processor version is displayed as “Not Applicable” in processor view in system overview page..........149
Does OMIVV support vCenter in linked mode.......... 149
What are required port settings for OMIVV..........149
Password is not changed for user used for bare-metal discovery after successfully applying hardware profile or system profile that has same user with new changed credentials in iDRAC user list..........151
Unable to view new iDRAC version details listed on vCenter hosts and clusters page..........151
How can I test event settings by using OMSA to simulate temperature hardware Fault.......... 151
Although OMSA agent is installed on OMIVV host system, I still get error message that OMSA is not installed. .......... 152
Can OMIVV support ESXi with lockdown mode enabled..........152
When I tried to use lockdown mode, it fails.......... 152
Creation of hardware profile fails if I am using reference server..........152
Attempting to deploy ESXi on server fails..........153
Hypervisor deployments failing on Dell PowerEdge R210 II machines..........153
Auto discovered systems are displayed without model information in Deployment wizard.......... 153
NFS share is set up with ESXi ISO, but deployment fails with errors mounting share location............153
How do I force remove virtual appliance from vCenter.......... 153
Entering a Password in the Backup Now Screen Receives an Error Message.......... 153
In vSphere web client, clicking Dell server management portlet or Dell icon returns 404 error........... 154
What should I do as firmware update failed..........154
What should I do as vCenter registration failed..........154
Performance during connection profile test credentials is slow or unresponsive.......... 154

Does OMIVV support VMware vCenter server appliance....154
Firmware level not updated when I have performed firmware update with Apply on Next reboot option and system was rebooted....154
Host still displayed under chassis even after removing host from vCenter tree....155
In Administration Console, **Update Repository Path** is not set to default path after I reset appliance to factory settings....155
After backup and restore of OMIVV, alarm settings are not restored ....155
Hypervisor deployment fails when NPAR is enabled on a target node and disabled in System Profile....155
Available virtual appliance version displays wrong information when the available version is lesser than the current version....155
**The 267027 exception is thrown while adding a 12G bare-metal server with an Express license** ....155
During OS deployment on 14G, hardware profile apply fails due to iDRAC error....156
OMIVV RPM upgrade fails when proxy is configured with domain user authentication....156
Unable to apply System Profile that has PCIe card in the FX chassis....156
Drift Detection shows noncompliant for Modular servers that has PCIe card in the FX chassis ....156
Unable to deploy an OS on PowerEdge serves when the iDRAC does not populate the MAC address of the selected NIC ....156
When deploying an OS, the Hardware Profile cannot be applied and the boot order cannot be configured without restarting the host....157
When creating a connection profile for the host having ESXi 6.5U1, the Service Tag of the host is not displayed on the Select Hosts page....157
Chassis object is not displayed on the left Navigator pane of the Dell EMC Chassis page....157
Dell icon is not displayed after backup and restore from an earlier OMIVV version to a later OMIVV version....157
When upgrading or downgrading some iDRAC firmware versions using OMIVV, even when the actual firmware update is successful, OMIVV may indicate that the job is failed. ....158
The deployment job fails when a server is in the UEFI mode and Secure boot feature is enabled....158
Configuring the System Lockdown mode at a cluster level sometimes displays a message "No hosts under the cluster has successful inventory"....158
Sometimes post RPM upgrade of OMIVV appliance, multiple entries in the logs are seen in vCenter Recent Tasks....158
Bare-metal deployment issues....158
Enabling auto discovery on newly purchased system....159

**Chapter 17: Related Documentation....160**
Accessing documents from the Dell EMC support site....160

**Appendix A: System specific attributes.... 161**

**Appendix B: Customization attributes....165**

**Appendix C: Additional information....166**

**Appendix D: Component vs. baseline version comparison matrix.... 167**

# 1

# Introduction

IT administrators use VMware vCenter as the primary console to manage and monitor VMware vSphere ESX/ESXi hosts. OpenManage Integration for VMware vCenter (OMIVV) enables you to manage the Dell hosts better from the VMware web client by providing enhanced capabilities for deployment, manage, monitor and upgrade.

**Topics:**

- Whats new in this release
- OpenManage Integration for VMware vCenter features

## Whats new in this release

This release of OpenManage Integration for VMware vCenter provides the following features:

- Support for the following:
  - PowerEdge MX7000 modular infrastructure
    - PowerEdge MX740c and PowerEdge MX840c servers.
    - Chassis and Servers management using unified Chassis Management IP
    - Standalone and Multi-Chassis Configuration deployment modes of PowerEdge MX7000 chassis.
  - PowerEdge R940 XA
- Enhancement in Chassis Profile test connection flow to make it automated.
- Support for OEM servers for OMIVV workflows.
- Support for vSphere 6.7U1 and vSphere 6.5U2.
- The following enhancements in the Firmware Update workflow:
  - Support to perform Clear Job Queue and reset iDRAC while creating a Firmware Update job.
  - Support to provide Custom Online Catalog location for a firmware update.
  - Support for HTTPS as default communication with Dell.com domains.
- Enhanced support in the OS deployment workflow:
  - OS deployment management network on PCI NICs.
  - OS deployment on the BOSS disk.
- Support to report Remaining Rated Write Endurance metrics for SSD in OMIVV.

## OpenManage Integration for VMware vCenter features

Following are the OpenManage Integration for VMware vCenter (OMIVV) appliance features:

**Table 1. OMIVV features**

| Features | Description |
|---|---|
| Inventory | The inventory feature provides the following:<br>● PowerEdge server details, such as memory—quantity and type, NIC, PSU, processors, RAC, warranty information, server, cluster, and data center level view<br>● Chassis details, such as Chassis Management Controller (CMC) or Management Module information, chassis power supply, KVM status, fan or thermal details, warranty information, switch, or server, or storage details.<br>● Support for an MX chassis relationship in the Multi-Chassis Management (MCM) configuration. |

Table 1. OMIVV features (continued)

| Features | Description |
|---|---|
| | ● Fabric information for an MX chassis MCM configuration.<br>● QuickSync hardware information for an MX chassis. |
| Monitor and send alerts | The monitoring and alerting includes the following functionalities:<br>● Detect key hardware faults and perform virtualization-aware actions. For example, migrate workloads or place host in a maintenance mode.<br>● Provide intelligence such as inventory, events, alarms to diagnose server and chassis problems.<br>● Support for VMware Proactive HA feature. |
| Firmware updates | The cluster-aware firmware update includes the following:<br>● Update supported servers to the most recent version of BIOS and firmware.<br>● BIOS and firmware update for vSAN clusters. |
| Drift detection for vSAN clusters | ● Firmware compliance for vSAN clusters.<br>● Driver compliance for vSAN clusters. |
| Driver updates | Driver updates for vSAN clusters. |
| Deployment and provisioning | Create hardware profiles (11th to 14th Gen PowerEdge servers), System profiles (14th Gen servers), hypervisor profiles, and remotely deploy an operating system on the bare-metal servers using VMware vCenter without using PXE. |
| Service Information | Retrieve warranty information for the Dell EMC servers and its associated chassis from Dell's warranty database and enable for easy online warranty upgrading. |
| Security role and permissions | Security role and permissions include the following functionalities:<br>● Integrate with standard vCenter authentication, rules, and permissions.<br>● Support for iDRAC Lockdown Mode in 14th Gen servers. |
| Support for OEM server | The following OMIVV features are supported:<br>● Inventory<br>● Monitor and send alerts<br>● Firmware update<br>● Deployment and provisioning<br>● Service Information<br>● Security role and permissions |

ⓘ **NOTE:** From OMIVV 4.0 onwards, only VMware vSphere Web Client is supported, and the vSphere desktop client is not supported.

ⓘ **NOTE:** For vCenter 6.5 and later, the OMIVV appliance is available only for the flash version. The OMIVV appliance is not available for the HTML5 version.

# About Administration Console

You can achieve the administration of OpenManage Integration for VMware vCenter and its virtual environment using the following two administration portals:

- Web-based Administration Console
- Console view for an individual server—the virtual machine console of the OMIVV appliance

**Topics:**

- Using Administration Portal

# Using Administration Portal

You can use the administration portal to perform the following tasks:

- Register a vCenter server. See Registering a vCenter server.
- Modify vCenter login credentials. See Modifying the vCenter login credentials.
- Update SSL certificates. See Updating the SSL certificates for registered vCenter servers.
- Upload or buy a license. If you are using a Evaluation license, the **Buy Software** link is displayed. By clicking this link, you can purchase a full-version license for managing multiple hosts. See Uploading license to the Administration Portal.
- Update OMIVV. See Updating virtual appliance repository location and virtual appliance on page 16.
- Generate troubleshooting bundle. See Downloading troubleshooting bundle on page 29.
- Restart OMIVV. See Restarting virtual appliance on page 15.
- Perform backup and restore. See Updating appliance through backup and restore on page 17.
- Configure alerts. See Setting up global alerts on page 20.
- Configure the deployment mode, see Configuring deployment mode on page 18.

## Registering vCenter server

You can register the OMIVV appliance after the OpenManage Integration for VMware vCenter is installed. OpenManage Integration for VMware vCenter uses the administrator user account or a non-administrator user account with necessary privileges for vCenter operations. A single OMIVV appliance instance can support a total of 10 vCenter servers and up to 1000 ESXi hosts.

To register a new vCenter server, perform the following steps:

1. Open **Administration Portal** from a supported browser.
   To open Administration Portal, 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|hostname>`.
2. In the left pane, click **VCENTER REGISTRATION**, and then click **Register a New vCenter Server**.
3. In the **REGISTER A NEW VCENTER** dialog box, under **vCenter Name**, perform the following steps:
   a. In the **vCenter Server IP or Hostname** text box, enter the vCenter IP address or FQDN of the host.

      > **NOTE:** Dell recommends that register OMIVV with the VMware vCenter using Fully Qualified Domain Name (FQDN). For all registrations, the hostname of vCenter should be properly resolvable by the DNS server. The following are the recommended practices for using the DNS server:
      >
      > - Assign a static IP address and hostname 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 hostname entries are present in both forward and reverse lookup zones in your DNS server.

   b. In the **Description** text box, enter a description—optional.
4. Under **vCenter User Account**, perform the following steps:
   a. In the **vCenter User Name** text box, enter the administrator's user name or a non-administrator user name with the required privileges.

b. In the **Password** text box, enter the password.
c. In the **Verify Password** text box, enter the password again.

5. Click **Register**.

After registering the vCenter server, OMIVV is registered as a vCenter plug-in, and “Dell EMC OpenManage Integration” icon is visible in the vSphere web client from which you can access the OMIVV functionalities.

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

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 host into maintenance mode or reboot the host.

## Modifying vCenter login credentials

The vCenter login credentials can be modified by a user with administrative privileges or a non-administrator user with necessary privileges.

1. To open Administration Portal, 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|hostname>` url.
2. In the **Login** dialog box, type the password, and click **Login**.
3. In the left pane, click **VCENTER REGISTRATION**.
   The registered vCenter servers are displayed in the right pane of the **MANAGE VCENTER SERVER CONNECTIONS** window. To open the **MODIFY USER ACCT** window, under **Credentials**, click **Modify** for a registered vCenter.
4. Enter the vCenter **User name**, **Password**, and **Verify Password**; the passwords must match.
5. To change the password, click **Apply**, or to cancel the change, click **Cancel**.

ⓘ **NOTE:** An error message is displayed, if the provided user credentials do not have necessary privileges.

ⓘ **NOTE:** If a Proactive HA feature is enabled on a cluster, you must not change the user associated to it. Modifying the registration with a different vCenter user will break the Proactive HA functionality. If the credentials require modification, unregister the old credentials and register by using the new credentials.

## Updating SSL certificates for registered vCenter servers

The OpenManage Integration for VMware vCenter uses the OpenSSL API to create the Certificate Signing Request (CSR) by using the RSA encryption standard with a 2048–bit key length. The CSR generated by OMIVV gets a digitally signed certificate from a trusted certification authority. The OpenManage Integration for VMware vCenter uses the digital certificate to enable SSL on the web server for secure communication.

If the SSL certificate is changed on a vCenter server, use the following steps to import the new certificate for OpenManage Integration for VMware vCenter:

1. To open Administration Portal, 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|hostname>` url.
2. In the left pane, click **VCENTER REGISTRATION**.
   The registered vCenter servers are displayed in the right pane.
3. To update the certificate for a vCenter server IP or host name, click **Update**.

## Uninstalling OpenManage Integration for VMware vCenter

To remove OpenManage Integration for VMware vCenter, unregister OMIVV from the vCenter server by using the Administration Console.

ⓘ **NOTE:** Ensure that you do not unregister OMIVV from the vCenter server when an inventory, a warranty, or a deployment job is running.

1. To open Administration Portal, 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|hostname>` url.
2. In the **VCENTER REGISTRATION** page, from the **vCenter Server IP or Hostname** table, click **Unregister**.

**NOTE:** Since there can be more than one vCenter, ensure that you select the correct vCenter.

3. To confirm the unregistration of the selected vCenter server, in the **UNREGISTER VCENTER** dialog box, click **Unregister**.

**NOTE:** If you have enabled Proactive HA on clusters, ensure that Proactive HA is disabled on the clusters. For disabling Proactive HA, access the **Proactive HA Failures and Responses** screen of a cluster by selecting **Configure** > **Services** > **vSphere Availability**, and then clicking **Edit**. To disable Proactive HA:

In the **Proactive HA Failures and Responses** screen, clear the check box against **Dell Inc** provider.

## Registering vCenter Server by non-administrator user

You can register vCenter servers for the OMIVV appliance with vCenter administrator credentials or a non-administrator user with the Dell privileges.

To enable a non-administrator user with the required privileges to register a vCenter Server, perform the following 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 non-administrator 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 non-administrator user with the required privileges can now register and/or unregister vCenter, modify credentials, or update the certificate.

3. Register a vCenter Server using a non-administrator 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 non-administrator user with the required privileges can now use the OMIVV features with the Dell EMC hosts.

## Required privileges for non-administrator users

To register OMIVV with vCenter, a non-administrator user requires the following privileges:

**NOTE:** While registering a vCenter server with OMIVV by a non-administrator 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

  **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

    > **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

> **NOTE:** If a non-administrator user is trying to register vCenter server, it is mandatory to add Dell privileges to the existing role. For more information about assigning Dell privileges, see Assigning Dell privileges to existing role on page 14.

## Assigning Dell privileges to existing role

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

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

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 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.

## Uploading license to Administration Portal

You can upload an OMIVV license to change the number of supported concurrent registered vCenter instances and managed hosts. You can also add licenses if you need to add more hosts by perform the following steps:

1. To open Administration Portal, 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|hostname>` url.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **VCENTER REGISTRATION**.
   The registered vCenter servers are displayed in the right pane.
4. Click **Upload License**.
5. In the **UPLOAD LICENSE** dialog box, click **Browse** to navigate to the license file, and then click **Upload**.

   **NOTE:** If the license file is modified or edited, the OMIVV appliance views it as corrupted and the license file does not work.

## Managing the virtual appliance

The virtual appliance management enables you to manage the OpenManage Integration for VMware vCenter network, version, NTP, and HTTPS information, and enables an administrator:

- Restart the virtual appliance. See Restarting the virtual appliance.
- Update the virtual appliance, and configure an update repository location. Updating the virtual appliance repository location and virtual appliance.
- Set up NTP servers. See Setting up the Network Time Protocol servers.
- Upload HTTPS certificates. See Uploading an HTTPS certificate.

In OpenManage Integration for VMware vCenter, perform the following steps to access the **APPLIANCE MANAGEMENT** page through the Administration Portal:

1. To open Administration Portal, 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|hostname>` url.
2. In the **Login** dialog box, type the password.
3. To configure the appliance management section, in the left pane, click **APPLIANCE MANAGEMENT**.

### Restarting virtual appliance

1. In the **APPLIANCE MANAGEMENT** page, click **Restart the Virtual Appliance**.
2. To restart the virtual appliance, in the **Restart Virtual Appliance** dialog box, click **Apply**, or to cancel, click **Cancel**.

### Changing host name of virtual appliance

Perform the following steps:

1. On the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** page, click **Change Hostname**.
2. Enter an updated host name.
   Type the domain name in the format: *<hostname>*.
3. Click **Update Hostname**.

The appliance hostname is updated, and you return to the main menu.

4. To reboot the appliance, click **Reboot Appliance**.

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

ⓘ **NOTE:** Ensure that you manually update all references to the virtual appliance across its environment such as provisioning server in iDRAC, DRM.

## Updating virtual appliance repository location and virtual appliance

To ensure that all data is protected, perform a backup of the OMIVV database prior to an update of the virtual appliance. See Managing backup and restore on page 20.

1. In the **APPLIANCE UPDATE** section of the **APPLIANCE MANAGEMENT** page, verify the current and available version.

   ⓘ **NOTE:** The OMIVV appliance requires internet connectivity to display available upgrade mechanisms and perform the RPM upgrade. Ensure that the OMIVV appliance has internet connectivity. Depending on the network settings, enable proxy and provide proxy settings, if the network needs proxy. See Setting up the HTTP proxy.

   ⓘ **NOTE:** Ensure that the **Update Repository Path** is valid.

   For the available virtual appliance version, the applicable RPM and OVF virtual appliance upgrade mechanisms are displayed with a tick symbol. The following are the possible upgrade mechanism options, and you can perform either of the tasks for the upgrade mechanism:

   - If a tick symbol is displayed against RPM, you can do an RPM upgrade from the existing version to the latest available version. See Upgrading from an existing version to the latest version.
   - If a tick symbol is displayed against OVF, you can take a back up of the OMIVV database from the existing version, and restore it in the latest available appliance version. See Updating the appliance through back up, and restore.
   - If a tick symbol is displayed against both RPM and OVF, you can perform either of the mentioned options to upgrade your appliance. In this scenario, the recommended option is RPM upgrade.

2. To update the virtual appliance, perform the mentioned tasks for the upgrade mechanisms as applicable from the version of OMIVV.

   ⓘ **NOTE:** Ensure that you log out from all web client sessions to the registered vCenter servers.

   ⓘ **NOTE:** Ensure that you update all appliances simultaneously under the same Platform Service Controller (PSC) before logging in to any of the registered vCenter servers. Else, you may see inconsistent information across OMIVV instances.

3. Click **APPLIANCE MANAGEMENT**, and verify the upgrade mechanisms.

## Upgrading OMIVV from existing version to current version

1. In the **APPLIANCE MANAGEMENT** page, depending on your network settings, enable proxy and provide proxy settings if your network needs proxy. See Setting up HTTP proxy .
2. To upgrade the OpenManage Integration plug in from an existing version to the current version, perform one of the following steps:

   - To upgrade using RPM that is available in **Update Repository Path**, ensure that **Update Repository Path** is set to the path: https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/.

     If the path is different, in the **Appliance Management** window, in the **APPLIANCE UPDATE** area, click **Edit** to update the path to https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ in the **Update Repository Path** text box, and click **Apply**.

   - To upgrade using the latest downloaded RPM folders or files if there is no internet connectivity, download all the files and folders from the https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ path and copy them to an HTTP share.

     In the **Appliance Management** window, in the **APPLIANCE UPDATE** section, click **Edit**, and then in the **Update Repository Path** text box, include the path to the offline HTTP share, and click **Apply**.

3. Compare the available virtual appliance version and current virtual appliance version and ensure that the available virtual appliance version is greater than the current virtual appliance version.

4. To apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
5. In the **UPDATE APPLIANCE** dialog box, click **Update**.
   After you click **Update**, you are logged off from the **ADMINISTRATION CONSOLE** window.
6. Close the web browser.

ⓘ **NOTE:** During the upgrade process, the appliance restarts once or twice.

ⓘ **NOTE:** Once the appliance is RPM upgraded, ensure that you do the following:

- Clear the browser cache before logging in to the Dell admin portal.
- Reinstall the VMware tools.

  To reinstall the VMware tools:

  1. Right-click the OMIVV appliance.
  2. Hover over **Guest**, and then click **Install/Upgrade VMware Tools**.
  3. On the **Install/Upgrade VMware Tools** dialog box, click **Automatic Tools Upgrade**, and then click **OK**.

     You can view the installation status in the **Recent Tasks**.

ⓘ **NOTE:** After the RPM upgrade is complete, you can view the login screen in the OMIVV console. Open a browser, provide the *https:\\<ApplianceIP|hostname>* link, and navigate to the **APPLIANCE UPDATE** area. You can verify that the available and current virtual appliance versions are same. 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 upgrade. Hence, health updates for the Dell EMC hosts are not available until upgrade is complete.

## Updating appliance through backup and restore

To update the OMIVV appliance from an older version to current version, perform the following steps:

1. Take a backup of the database for the older release.
2. Turn off the older OMIVV appliance from vCenter.

   ⓘ **NOTE:** Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes all the alarms that are registered on vCenter by the OMIVV plug-in and all the customization that is performed on the alarms, such as actions, and so on.

3. Deploy the new OpenManage Integration appliance OVF.
4. Power on the OpenManage Integration new appliance.
5. Set up the network, time zone, and so on, for the new appliance.

   ⓘ **NOTE:** Ensure that the new OpenManage Integration appliance has the same IP address as the old appliance.

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

6. The OMIVV appliance comes with default certificate. If you want to have a custom certificate for your appliance, update the same. See Generating Certificate Signing Request on page 19 and Uploading HTTPS certificate on page 19. Else, skip this step.
7. Restore the database to the new OMIVV appliance. See Restoring the OMIVV database from a backup .
8. Verify the appliance. See the Installation verification in *OpenManage Integration for VMware vCenter Installation Guide* available at Dell.com/support/manuals.
9. Run the **Inventory** on all the registered vCenter servers.

   ⓘ **NOTE:** Dell EMC recommends that after the upgrade, you run the inventory again on all the hosts that the plug-in manages. To run the inventory on demand, see the Scheduling inventory jobs.

   ⓘ **NOTE:** If the IP address of the new OMIVV version y is changed from the OMIVV version x, configure the trap destination for the SNMP traps to hover over the new appliance. For 12th and later Gen servers, the IP change is fixed by running the inventory on these hosts. While running the inventory on 12th Gen hosts, if SNMP traps do not hover over the new IP, those hosts are listed as noncomplaint. For hosts earlier than 12th Gen that were compliant with earlier versions, the IP change is displayed as noncompliant and requires you to configure Dell EMC OpenManage Server Administrator (OMSA). To fix vSphere host compliance issues, see Running the fix noncompliant vSphere hosts wizard.

ⓘ **NOTE:** After backup and restore from an earlier OMIVV version to a later OMIVV version, if you observe 2000000 error or Dell EMC logo is not displayed at vCenter, do the following:

- Restart vSphere Web Client on the vCenter server.
- If the issue persists:
  - For VMware vCenter Server Appliance, go to `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` and for Windows vCenter, go to `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance and see if the old data exists, such as: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
  - Manually delete the folder corresponding to the earlier OMIVV version.

## Downloading the troubleshooting bundle

1. In the **APPLIANCE MANAGEMENT** page, click **Generate Troubleshooting Bundle**.
2. Click the **Download Troubleshooting Bundle** link.
3. Click **Close**.

## Setting up HTTP proxy

1. In the **APPLIANCE MANAGEMENT** page, scroll down to **HTTP PROXY SETTINGS**, and then click **Edit**.
2. Perform the following steps in edit mode:
   a. Select **Enabled** to enable the use of HTTP proxy settings.
   b. Enter the proxy server address in **Proxy Server Address**.
   c. Enter the proxy server port in **Proxy Server Port**.
   d. Select **Yes** to use proxy credentials.
   e. If using proxy credentials, enter the user name in **Username**.
   f. Type password in **Password**.
   g. Click **Apply**.

## Setting up Network Time Protocol servers

You can use Network Time Protocol (NTP) to synchronize the virtual appliance clocks to that of an NTP server.

1. In the **APPLIANCE MANAGEMENT** page, click **Edit** in the **NTP Settings** area.
2. Select **Enabled**. Enter the host name or IP address for a preferred and secondary NTP server and click **Apply**.

ⓘ **NOTE:** It might take around 10 minutes for the virtual appliance clocks to synchronize with the NTP server.

## Configuring deployment mode

Ensure that the following system requirements for the desired deployment modes are met by assigning these resources to the virtual machine containing OMIVV:

**Table 2. System requirements for deployment modes**

| Deployment modes | Number of hosts | Number of CPUs | Memory—in GB | Minimum Storage |
|---|---|---|---|---|
| Small | Up to 250 | 2 | 8 | 44 GB |
| Medium | Up to 500 | 4 | 16 | 44 GB |
| Large | Up to 1000 | 8 | 32 | 44 GB |

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

You can select an appropriate deployment mode to scale OMIVV to match the number of nodes in your environment.

1. In the **APPLIANCE MANAGEMENT** page, scroll down to **Deployment Mode**.
   The configuration values of the deployment mode such as **Small**, **Medium**, or **Large** is displayed and by default, the deployment mode is set to **Small**.
2. Click **Edit** if you want to update the deployment mode based on the environment.
3. In the **Edit** mode, select the desired deployment mode after ensuring that the prerequisites are met.
4. Click **Apply**.
   The allocated CPU and memory are verified against the required CPU and memory for the set deployment mode and either of the following situations happen:
   - If the verification fails, an error message is displayed.
   - If the verification is successful, the OMIVV appliance restarts and the deployment mode are changed after you confirm the change.
   - If the required deployment mode is already set, a message is displayed.
5. If the deployment mode is changed, confirm the changes, and then proceed with rebooting the OMIVV appliance to allow the deployment mode to be updated.

ⓘ **NOTE:** During the OMIVV appliance boot up, the allocated system resource is verified against the set deployment mode. If the allocated system resources are less than the set deployment mode, the OMIVV appliance does not boot up to the login screen. To boot up the OMIVV appliance, shut down the OMIVV appliance, update the system resources to the existing set deployment mode, and follow the downgrade deployment mode task.

### Downgrading deployment mode

1. Log in to the Administration Console.
2. Change the deployment mode to the desired level.
3. Shut down the OMIVV appliance and change the system resources to the desired level.
4. Turn-on the OMIVV appliance.

## Generating Certificate Signing Request

Ensure that you upload the certificate before registering OMIVV with the vCenter.

Generating a new Certificate Signing Request (CSR) prevents certificates that were created with the previously generated CSR from being uploaded to the appliance. To generate a CSR, do the following:

1. In the **APPLIANCE MANAGEMENT** page, click **Generate Certificate Signing Request** in the **HTTPS CERTIFICATES** area.
   A message is displayed stating that if a new request is generated, certificates created using the previous CSR can no longer be uploaded to the appliance. To continue with the request, click **Continue**, or to cancel, click **Cancel**.
2. If you continue with the request, in the **GENERATE CERTIFICATE SIGNING REQUEST** dialog box, enter the **Common Name**, **Organizational Name**, **Organizational Unit**, **Locality**, **State Name**, **Country**, and **Email** for the request. Click **Continue**.
3. Click **Download**, and then save the resulting certificate request to an accessible location.

## Uploading HTTPS certificate

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.

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**.

# Setting up global alerts

Alert management enables you to configure global settings for how alerts are stored for all vCenter instances.

1. To open Administration Portal, 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|hostname>` url.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **ALERT MANAGEMENT**. To enter new vCenter alert settings, click **Edit**.
4. Enter numeric values for the following fields:
   - **Maximum number of alerts**
   - **Number of days to retain alerts**
   - **Timeout for duplicate alerts (seconds)**
5. To save your settings, click **Apply**, or to cancel, click **Cancel**.

# Managing backup and restore

Managing backup and restore is accomplished from the Administrative Console. The tasks on this page include:

- Configuring backup and restore
- Scheduling automatic backups
- Performing an immediate backup
- Restoring the database from backup

In OpenManage Integration for VMware vCenter, perform the following steps to access the **BACKUP AND RESTORE SETTINGS** page through the Administration Console:

1. To open Administration Portal, 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|hostname>` url.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **BACKUP AND RESTORE**.

## Configuring backup and restore

The backup and restore function backs up the OMIVV database to a remote location from which it can be restored later. The profiles, templates, and host information are included in the backup. Dell recommends that you schedule automatic backups to guard against data loss.

ⓘ **NOTE:** NTP Settings are not saved and restored.

1. In the **BACKUP AND RESTORE SETTINGS** page, click **Edit**.
2. In the highlighted **SETTINGS AND DETAILS** area, perform the following steps:
   a. In **Backup Location**, type the path of the backup files.
   b. In **Username**, type the user name.
   c. In **Password**, type the password.
   d. In **Enter the password used to encrypt backups**, type the encrypted password in the text box.

      The encryption password can contain alphanumeric characters and special characters, such as, “!@#$%*”.

   e. In **Verify Password**, retype the encrypted password.
3. To save these settings, click **Apply**.
4. Configure the backup schedule. See Scheduling automatic backups.

After this procedure, configure a backup schedule.

## Scheduling automatic backups

For more information about configuring the backup location and credentials, see Configuring backup and restore.

1. In the **BACKUP AND RESTORE SETTINGS** page, click **Edit Automatic Scheduled Backup**.
   The relevant fields are enabled.
2. To enable the backups, click **Enabled**.
3. Select the **Days for Backup** check boxes for the days of the week for which you want to run the backup.
4. In **Time for Backup (24 Hour, HH: mm)**, enter the time in HH: mm format.
   The **Next Backup** is populated with the date and time of the next scheduled backup.
5. Click **Apply**.

## Performing immediate backup

1. In the **BACKUP AND RESTORE SETTINGS** page, click **Backup Now**.
2. To use location and encryption password from the backup settings, in the **BACKUP NOW** dialog box, select the **BACKUP NOW** check box.
3. Enter values for **Backup Location**, **Username**, **Password**, and **Password for Encryption**.
   The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, $, %, *”. There is no length restriction.
4. Click **Backup**.

## Restoring OMIVV database from backup

The restore operation causes the virtual appliance to reboot after restoration is complete.

1. Open the **BACKUP AND RESTORE SETTINGS** page. See the Managing backup, and restore.
2. In the **BACKUP AND RESTORE SETTINGS** page, click **Restore Now**.
3. In the **RESTORE NOW** dialog box, enter the path for **File Location** along with the backup .gz file in CIFS/NFS format.
4. Enter the **Username**, **Password**, and **Encryption Password** for the backup file.
   The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, $, %, *”. There is no restriction on length.
5. To save your changes, click **Apply**.
   The appliance is rebooted.

**NOTE:** Ensure that you register the OMIVV appliance again if the appliance is reset to the factory settings.

# About vSphere client console

The vSphere client console is found within the vSphere client on a virtual machine. The console works in close association with the Administration Console. You can use the console to perform the following tasks:

- Configuring network settings
- Changing the virtual appliance password
- Configuring NTP and setting the local time zone
- Rebooting the virtual appliance
- Resetting the virtual appliance to factory settings
- Logging out from console
- Using read-only user role

## Opening OMIVV virtual machine console

1. From the vSphere web client **Home**, click **vCenter**.
2. In **Inventory Lists**, click **Virtual Machines**, and then select the OMIVV virtual appliance.
3. Perform one of the following steps:
   - In the **Object** tab, select **Action** → **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.

After opening the virtual machine console and providing the credentials (user name: admin and password: the password that you had set while deploying the appliance), you can configure the console.

## Configuring network settings

You can change the network settings in the vSphere client console.

1. Open the virtual machine console. See Opening vSphere client console.
2. In the **Console** window, select **Configure Network**, and then press **ENTER**.
3. Enter the desired network settings under **Edit Devices** or under **Edit DNS**, then click **Save & Quit**. To abort any changes, click **Quit**.

## Changing virtual appliance password

You can change the virtual appliance password in the vSphere web client by using the console.

1. Open the virtual machine console. See Opening vSphere client console.
2. In the **Console** window, use the arrow keys to select **Change Admin Password** and press **ENTER**.
3. In **Current Admin Password**, enter the value and press **ENTER**.

   The admin password should be at least eight characters and should include one special character, one number, one uppercase, and one lowercase.
4. Enter a new password for **Enter new Admin Password**, and press **ENTER**.
5. Retype the new password in **Please Confirm Admin Password**, and press **Enter**.

## Configuring NTP and setting local time zone

1. Open the virtual machine console. See Opening vSphere client console.
2. To configure the OMIVV time zone information, click **Date/Time Properties**.
3. In the **Date and Time** tab, select **Synchronize date and time over the network**.
   The **NTP Servers** window is displayed.
4. To add the NTP server IP or host name, click the **Add** button, and then press **TAB**.
5. Click **Time Zone**, select the applicable time zone, and then click **OK**.

## Rebooting virtual appliance

1. Open the virtual machine console. See Opening vSphere client console.
2. Click **Reboot Appliance**.
3. To reboot the appliance, click **`Yes`**, or to cancel, click **`No`**.

## Resetting virtual appliance to factory settings

1. Open the virtual machine console. See Opening vSphere client console.
2. Click **Reset Settings**.

The following message is displayed:

```
All the settings in the appliance will be Reset to Factory Defaults and the appliance
will be rebooted. Do you still wish to continue?
```

3. To reset the appliance, click `Yes`, or to cancel, click `No`.
   If you click yes, the OMIVV appliance is reset to the original factory settings and all other settings and existing data is lost.

**NOTE:** When the virtual appliance is reset to factory settings, any updates that you had done on the network configuration are preserved; these settings are not reset.

## Logging out from vSphere console

To log out from the vSphere console, click **Log out**.

## Read-only user role

There is a read-only unprivileged user role with shell access for diagnostic purposes. The read-only user has limited privileges to run the mount. The read-only user's password is set as **readonly**.

3

# Managing multiple appliances

You can manage and monitor multiple OMIVV appliances that you register with vCenter servers that belong to the same Platform Service Controller (PSC) or to a different PSC. Dell EMC recommends to use the similar vCenter versions.

Dell EMC recommends that you perform a global refresh if page is cached.

1. In VMware vCenter home page, click the **OpenManage Integration** icon.
2. In **Navigator**, under the **Dell EMC** group, click **OMIVV Appliances**.
3. In the **OMIVV Appliances** tab, view the following information and monitor appliances:

   ⓘ **NOTE:** In the Dell appliance tab, the precedence of the appliances appearing in the list is predetermined and the highlighted appliance is the active appliance.

   - **Name**—displays a link using the IP address or FQDN for each OMIVV appliance. To view and monitor appliance-specific information, click a specific appliance name link. Clicking an appliance name link takes you to the main content pane of the OMIVV appliance. You can manage the OMIVV operations and monitor hosts, data centers, and clusters for the specific appliance.

     ⓘ **NOTE:** A message box is displayed after clicking **Name** that prompts you to perform a global refresh on the cached pages if you are using multiple appliances.

     To know the appliance on which you are managing the OMIVV operations, perform the following actions:

     a. In OpenManage Integration for VMware vCenter, click the **Help and Support** tab.
     b. Under Administration Console, view the specific OMIVV appliance IP.
   - **Version**—displays version of each OMIVV appliance.
   - **Compliance Status**—specifies whether the appliance is compliant with the loaded plug-in.

     ⓘ **NOTE:** The compliance status of an appliance is displayed as **Not-compliant** when the OMIVV appliance is not complaint with the plug-in and the **Name** link is disabled.
   - **Availability Status**—displays a status specifying if you can reach the appliance from the plug-in and the required web services are running in the OMIVV appliance.

     ⓘ **NOTE:** You can select an appliance when the appliance compliance status is **Complaint** and appliance availability status is **OK**.
   - **Registered vCenter Servers**—displays all vCenters that you can access for the logged-in session and are registered with appliances. If you register an appliance with multiple vCenters, the vCenters are displayed as an expandable and collapsible list. Clicking a vCenter link takes you to the **vCenter Servers** page where all the vCenters are listed in the Navigator pane.

4

# Accessing OpenManage Integration from web client

When you log in to VMware vCenter after installing OMIVV, under the **Home** tab, the **OpenManage Integration** icon is located in the main content area under the **Administration** group. You can use the **OpenManage Integration** icon to navigate to the **OpenManage Integration for VMware vCenter** page. The **Dell EMC** group is displayed in the **Navigator** pane.

VMware vCenter layout has the following three main panes:

**Table 3. OpenManage Integration for VMware vCenter panes**

| Panes | Description |
|---|---|
| Navigator | Accesses different views in the console. The OpenManage Integration for VMware vCenter has a special group under the vCenter menu that serves as the primary access point for OpenManage Integration for VMware vCenter. |
| Main Content | Displays the views selected in the Navigator pane. The main content pane is the area where most of the content is displayed. |
| Notifications | Displays vCenter alarms, task and work in progress. The OpenManage Integration for VMware vCenter integrates with the alarm, event, and task systems in vCenter to display the information in the Notification pane. |

**Topics:**

- Navigating in VMware vCenter web client
- Icons in web client
- Locating software version
- Refreshing screen content
- Viewing Dell EMC hosts
- Viewing OEM hosts
- Viewing Dell EMC chassis
- Viewing OpenManage Integration for VMware vCenter licensing tab
- Accessing help and support
- Viewing log history

## Navigating in VMware vCenter web client

The **OpenManage Integration for VMware vCenter** is located in a special **Dell EMC** group within VMware vCenter.

1. Log in to VMware vCenter.
2. In the VMware vCenter home page, click the **OpenManage Integration** icon.

   Here you can:

   - Manage OpenManage Integration for VMware vCenter connection profiles, product settings, view the summary page, and perform other tasks from the tabs in the main content pane.
   - Monitor hosts, data centers, and clusters from the Navigator pane, under **vCenter Inventory Lists**. Select the host, data center, or cluster that you want to investigate, and then on the **Objects** tab, click the object you choose to monitor.

# Icons in web client

The product user interface uses many icon-based action buttons for the actions you take.

**Table 4. Icon buttons defined**

| Icon buttons | Definition |
|---|---|
| ➕ | Add or create something new |
| 🖥 | Add a server to a connection profile, data center, and cluster |
| 🛑 | Abort a job |
| ⊢ | Collapse a list |
| ☰ | Expand a list |
| ❌ | Delete an object |
| 📅 | Change a schedule |
| ✏ | Edit |
| 🧹 | Purge a job |
| 📤 | Export a file |
| 👁 | View System Profile |
| ▽ | Filter |
| ▶ | Run now |

# Locating software version

The software version is found on the OpenManage Integration for VMware vCenter **Getting Started** tab.

1. In VMware vCenter home page, click the **OpenManage Integration** icon.
2. In the OpenManage Integration for VMware vCenter **Getting Started** tab, click **Version Information**.
3. In the **Version Information** dialog box, view the version information.
4. To close the dialog box, click **OK**.

# Refreshing screen content

Refresh a screen by using the VMware vCenter **Refresh** icon.

1. Select a page that you want to refresh.
2. In the VMware vCenter title bar, click the **Refresh (Ctrl+Alt+R)** icon.

   The **Refresh** icon is at the right of the Search area and looks like a clockwise arrow.

# Viewing Dell EMC hosts

When you want to quickly view only Dell EMC hosts, in OpenManage Integration for VMware vCenter, in the Navigator pane, select **Dell EMC Hosts**.

1. In VMware vCenter home page, click the **OpenManage Integration** icon.

2. In the **Navigator**, under **OpenManage Integration**, click **Dell EMC Hosts**.
3. In the **Dell EMC Hosts** tab, view the following information:
    - **Host Name**—displays a link using the IP address for each Dell EMC host. To view Dell EMC host information, click a specific host link.
    - **vCenter**—displays the vCenter IP address of the Dell EMC host.
    - **Cluster**—displays the cluster name, if the Dell EMC host is in a cluster.
    - **Connection Profile**—displays the name of the connection profile.

# Viewing OEM hosts

1. On the **OpenManage Integration for VMware vCenter** page, in the left pane, click **OEM Hosts**.
   The **OEM Hosts** page is displayed.
2. On the **OEM Hosts** page, view the following information:
    - **Host Name**—displays a link using the IP address for each OEM host. To view OEM host information, click a specific host link.
    - **vCenter**—displays the vCenter IP address of the OEM host.
    - **Cluster**—displays the cluster name, if the OEM host is in a cluster.
    - **Connection Profile**—displays the name of the connection profile.

# Viewing Dell EMC chassis

You can view the Dell EMC chassis on the **Dell EMC chassis** page.

1. On the **OpenManage Integration for VMware vCenter** page, in the left pane, click **Dell EMC Chassis**.
2. On the **Dell EMC chassis** page, in the **Objects** tab, the following information is displayed:
    - **Name**: Displays an IP address link for each Dell EMC chassis.
    - **IP Address/FQDN**: Displays the vCenter IP address.
    - **Service Tag**: Displays the Service Tag of the chassis.
    - **Chassis URL**: Displays the chassis URL.
    - **Model**: Displays the model name.
    - **Location**: Displays the location of the chassis.
    - **Last Inventory**: Displays the last inventory information.
    - **Available Slots**: Displays the available slots in chassis.
    - **Profile Name**: Displays the chassis profile name in which the chassis is associated.
    - **Role**: Displays the role of the chassis.

   To add an MX chassis, click **Add MX Chassis**. For more information about manually adding an MX chassis, see Adding an MX Chassis on page 102.

   **NOTE:** There are instances when the **Role** column is not displayed on the **Dell EMC Chassis** page. In such a case, do the following:

   a. From the login user name list in **vSphere Web Client**, select **Remove Stored Data**.
   b. In the **User Preferences <user name>** dialog box, select the **User preferences for columns in list views** check box.
   c. Click **Clear selected data**.

      The **Dell EMC Chassis** page is refreshed and the **Role** column is displayed.

   **NOTE:** The order in which the IPs of the discovered chassis are listed in the left pane and the IP column of the Objects tab is not same. The order of sorting IPs in the left pane is based on the string sorting and the order of sorting in the right pane is based on the chassis role (lead and member).

   **NOTE:** When operations such as removal, addition, or update of a chassis are performed, refresh the **Dell EMC Chassis** page to view the latest data.

**NOTE:** For an MX chassis in an MCM configuration, the entire MCM infrastructure is managed using the lead chassis. If the member chassis IPs and iDRAC IPs are disabled and chassis role is changed, it is recommended to remove the existing lead chassis and add the new lead chassis IP again, and then associate to the chassis profile.

# Viewing OpenManage Integration for VMware vCenter licensing tab

When you install OpenManage Integration for VMware vCenter license, the number of supported hosts and vCenter servers are displayed in this tab. You can also view the version of the OpenManage Integration for VMware vCenter at the top of the page.

The page under licensing displays the **Buy License** link.

The **License Management** section displays:

- **Product Licensing Portal (Digital Locker)**
- **iDRAC Licensing Portal**
- **Administration Console**

The OpenManage Integration for VMware vCenter **Licensing** tab displays the following information:

| Licensing tab information | Description |
|---|---|
| **Host Licenses** | ● Licenses Available<br>Displays the number of available licenses<br>● Licenses In Use<br>Displays the number of licenses in use |
| **vCenter Licenses** | ● Licenses Available<br>Displays the number of available licenses<br>● Licenses In Use<br>Displays the number of licenses in use |

# Accessing help and support

To provide the information you need about your product, OpenManage Integration for VMware vCenter offers the **Help and Support** tab. In this tab, you can find the following information:

**Table 5. Information in the help and support tab (continued)**

| Name | Description |
|---|---|
| **Product Help** | Provides the following links:<br>● **OpenManage Integration for VMware vCenter Help** — provides a link to the product help, which is located inside the product. Use the table of contents or search to find the information that you need.<br>● **About** — This link displays the **Version Information** dialog box. You can view the product version here. |
| **Dell EMC Manuals** | Provides live links to:<br>● **Server Manuals**<br>● **OpenManage Integration for VMware vCenter Manuals** |
| **Administration Console** | Provides a link to the Administration Console. |
| **Additional Help and Support** | Provides live links to: |

Table 5. Information in the help and support tab

| Name | Description |
|---|---|
| | ● **iDRAC with Lifecycle Controller Manuals**<br>● **Dell VMware Documentation**<br>● **OpenManage Integration for VMware vCenter Product Page**<br>● **Dell Help and Support Home**<br>● **Dell TechCenter** |
| **Support Call Tips** | Offers tips on how to contact Dell Support and route your calls correctly. |
| **Troubleshooting Bundle** | Provides a link to create and download the troubleshooting bundle. You can provide or view this bundle when you contact technical support. For more information, see Downloading the troubleshooting bundle. |
| **Dell EMC Recommends** | Provides a link to Dell EMC Repository Manager (DRM). Use DRM to find and download all firmware updates available for your system. |
| **iDRAC Reset** | Provides a link to reset iDRAC that can be used when iDRAC is not responsive. This reset performs a normal iDRAC reboot. |

# Downloading troubleshooting bundle

**NOTE:** To generate the troubleshooting bundle, ensure that you log in to the vSphere web client as a user with write permission on OMIVV.

You can use the troubleshooting bundle information to help you with troubleshooting or send the information to Technical Support. To get the troubleshooting information, perform the following steps:

1. In OpenManage Integration for VMware vCenter, click the **Help and Support** tab.
2. Under **Troubleshooting Bundle**, click **Create and Download Troubleshooting Bundle**.
3. Click the **Create** button.
4. To save the file, click **Download**.
5. In the **File Download** dialog box, click **Save**.
6. In the **Save As** dialog box, browse to where you want to save the file, and click **Save**.
7. To exit, click **Close**.

# Resetting iDRAC

You can find the reset iDRAC link on the **Help and Support** tab. Resetting iDRAC performs a normal iDRAC reboot. The iDRAC reboot does not reboot the host. After you perform a reset, it takes up to 2 minutes to return to a usable state. Use reset in cases where the iDRAC is not responsive in the OpenManage Integration for VMware vCenter.

**NOTE:** It is recommended that you place the host in maintenance mode before resetting iDRAC. You can apply the reset action on a host that is part of a connection profile and has been inventoried at least once. The reset action might not return the iDRAC to a usable state. In such a scenario, a hard reset is required. To learn more about a hard reset, see iDRAC documentation.

While iDRAC is rebooting, you might view the following:

- A slight delay of communication error while the OpenManage Integration for VMware vCenter obtains its health status.
- All open sessions with iDRAC close.
- The DHCP address for iDRAC might change.

  If iDRAC uses DHCP for its IP address, there is a chance that the IP address changes. If the IP address changes, rerun the host inventory job to capture the new iDRAC IP address in the inventory data.

1. In the OpenManage Integration for VMware vCenter, click the **Help and Support** tab.

2. Under iDRAC Reset, click **Reset iDRAC**.
3. In the **iDRAC Reset** dialog box, under iDRAC Reset, type the host IP address/name.
4. To confirm that you understand the iDRAC reset process, select **I understand iDRAC reset. Continue iDRAC reset**.
5. Click **Reset iDRAC**.

## Opening online help

You can open the online help from the **Help and Support** tab. You can search the document for help on understanding a topic or a procedure.

1. In OpenManage Integration for VMware vCenter, in the **Help and Support**, under **Product Help**, click **OpenManage Integration for VMware vCenter Help**.
   The online help content is displayed in the browser window.
2. Use the left-pane table of contents or search to find the topic of your choice.
3. To close the online help, click **X** at the top-right corner of the browser window.

## Launching Administration Console

You can start OpenManage Integration for VMware vCenter from within the VMware vCenter web client, and open the Administration Console from the **Help and Support** tab.

1. In OpenManage Integration for VMware vCenter, in the **Help and Support** tab, under the **Administration Console**, click the link to the console.
2. In the **Administration Console** login dialog box, use the administrator password to log in.

   You can perform the following operations in the Administration console:

   - Register or unregister a vCenter, modify credentials, or update a certificate.
   - Upload the license.
   - View summary about the number of vCenters registered and available, and about maximum host license that are in use and available.
   - Restart the virtual appliance.
   - Update or upgrade to the latest version.
   - Display network settings (read only mode).
   - Configure HTTP proxy settings that connects to the Dell EMC server for appliance upgrade or for connectivity to `https://downloads.dell.com`
   - Configure NTP settings, which allow you to enable or disable NTP server, and configure preferred and secondary NTP server.
   - Generate a certificate signing request (CSR), upload a certificate, or restore the default certificate for the HTTPS certificates.
   - Configure global settings on how alerts are stored for all vCenter instances. You can configure the maximum numbers of alerts to be stored, numbers of days to retain them, and time out for duplicate alerts.
   - Configure global settings on how alerts are stored for all vCenter instances.
   - Initiate backup, or restore.
   - Configure backup location to a network share and the encryption password for the backed-up files (along with test network connection).
   - Schedule a recurring backup.

# Viewing log history

The log page enables you to view the logs that OMIVV generates.

You can filter and sort the content on this page by using the two drop-down lists. The first drop-down list allows you to filter and view log details based on the following log types:

- All Categories
- Info
- Warning
- Error

The second drop-down list helps you to sort logs details based on the following date and time frequency:

- Last Week
- Last Month
- Last Year
- Custom Range
  - If you select **Custom Range**, you can specify the start and end date based on what you want to filter, and then click **Apply**.

The grid table displays the following information:

- Category — displays the type of log category
- Date and Time — displays the date and time of user action
- Description — displays a description of the user action

You can sort the data grid columns in ascending or descending order by clicking the column header. Use the **Filter** text box to search within your content. At the bottom of the page grid, the following information is displayed:

**Table 6. Log history**

| **Log information** | **Description** |
|---|---|
| **Total items** | Displays the total count of all log items |
| **Items per screen** | Displays the number of log items on the displayed page. Use the drop-down box to set the number of items per page. |
| **Page** | Displays the page you are in while viewing the log information. You can also type a page number in the text box or use the **Previous** and **Next** buttons to navigate to the page you want. |
| **Previous or Next buttons** | Guides you to the next or previous pages |
| **Export All icon** | Exports log content to a CSV file |

## Viewing logs

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. In the **Log** tab, view the user actions logs for OpenManage Integration for VMware vCenter. For information about the displayed logs, see Log history.
3. To sort the data in the grid, click a column header.
4. To sort using categories or time blocks, use the drop-down lists preceding the grid.
5. To navigate between pages of log items, use the **Previous** and **Next** buttons.

## Exporting log files

The OpenManage Integration for VMware vCenter uses a comma-separated values (CSV) file format for exporting information from data tables.

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. To export the log contents to a CSV file, in the lower right-hand corner of the screen, click the 📤 icon.
3. In the **Select location for download** dialog box, browse to the location to save the log information.
4. In the **File name** text box, either accept the default name `ExportList.csv` or type your own file name with the .CSV extension.
5. Click **Save**.

5

# OpenManage Integration for VMware vCenter licensing

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

- Evaluation license—when the OMIVV 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 90-day trial version is the default license that is supplied when shipped.
- 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 that are managed by OMIVV.

When you upgrade from an evaluation license to a full standard license, you 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 using the **Administration Console**.

Licensing presents the following information:

- Maximum vCenter Connection Licenses—up to 10 registered and in-use vCenter connections are enabled.
- 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 Dell Digital Locker. If you are unable to download your license key(s), contact Dell Support by going to Order Support to locate the regional Dell Support phone number for your product.

**Topics:**

- Buying and uploading software license

# 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**.

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

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.

# 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

## 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.

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.
- Create a chassis profile. The hosts present in an MX chassis with an iDRAC IPv4 disabled has to be managed using a chassis profile. See Creating chassis profile on page 53.
- Configure events and alarms. See the Configuring events and alarms.
- Schedule inventory jobs. See the 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

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:

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

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

- The Active Directory user's account exist in Active Directory.
- The iDRAC and host are configured for Active Directory based authentication.

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 using the configuration wizard or from the **OpenManage Integration for VMware vCenter** > **Settings** tab. You can log in to iDRAC and the host 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.

**NOTE:** An MX chassis host can be managed using a single unified chassis management IP. To manage an MX chassis using a chassis profile, see Creating chassis profile. Dell EMC recommends managing an MX chassis hosts with an iDRAC IP to get complete OMIVV functions.

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 Gen 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.
     a. In Active Directory **User Name**, type the username. Type the username in one of these formats: `domain\username` or username@domain. The username is limited to 256.
     b. In Active Directory **Password**, type the password. The password is limited to 127 characters.
     c. In **Verify Password**, type the password again.
     d. 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:
     a. In **User Name**, type the username. The username is limited to 16 characters. See the iDRAC Documentation for information about username restrictions for the version of iDRAC that you are using.
     b. In **Password**, type the password. The password is limited to 20 characters.
     c. In **Verify Password**, type the password again.
     d. 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:

a. In Active Directory **User Name**, type the username. Type the username in one of these formats: `domain\username` or username@domain. The username is limited to 256 characters.

> **NOTE:** For host username and domain restrictions, see the following:
>
> Host username requirements:
>
> - Between 1 and 64 characters long
> - No nonprintable characters
>
> Host domain requirements:
>
> - Between 1 and 64 characters long
> - First character must be alphabetical.
> - Cannot contain a space.

b. In Active Directory **Password**, type the password. The password is limited to 127 characters.

c. In **Verify Password**, type the password again.

d. 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 iDRAC certificate check during all future connections, clear **Enable Certificate Check**.

- To configure host credentials without Active Directory, perform the following tasks:

a. In **User Name**, the username is `root`, which is the default username and you cannot change the username. However, if the Active Directory is set, you can choose any Active Directory user and not root.

b. 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.

c. In **Verify Password**, type the password again.

d. 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**.

> **NOTE:** If the OEM hosts are not displayed on the Select Hosts window, add the OEM hosts using the Add OEM Hosts wizard, see Adding OEM hosts.

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, Dell EMC recommends that you test the connection profile.

> **NOTE:** If the WBEM service is disabled for all hosts running ESXi 6.5 or later, WBEM is automatically enabled when you perform the test connection and inventory on those hosts.

> **NOTE:** If you select **All Registered vCenter** while creating the connection profile, test connection fails for all hosts running ESXi 6.5 or later that has the WBEM service disabled. In such case, it is recommended to complete the connection profile wizard actions, run the inventory on hosts, and then test the connection profile again.

> **NOTE:** You may see that test connection is failing for the host and indicating that invalid credentials are entered, even after entering valid credentials. It may happen because the ESXi is blocking the access. Wait for 15 minutes and retry the test connection.

8. 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 on page 50 topic in this guide..

> **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 hosts running ESXi 6.5 and later. 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 noncomplaint. To view the noncomplaint hosts that require SNMP trap destination to be reconfigured and/or WBEM services to be enabled, see Reporting and fixing compliance for vSphere hosts on page 130.

## Scheduling inventory jobs

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.

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 on page 58.

## Running warranty retrieval jobs

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.

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.
   Once 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 warranty job schedules from the **Settings** tab after completing the configuration from the configuration wizard. See Modifying warranty job schedules on page 61.

## 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.

ⓘ **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.

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**.

# 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 ✏ 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:
      i. In the **Warning** drop-down list, select the number of days before you want to be warned of the warranty expiration.
      ii. 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

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

**NOTE:** You can update firmware for only non-vSAN host and clusters using this repository.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings** on 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**—the firmware updates default repository is set to Dell Online (`https://downloads.dell.com`). The OMIVV downloads selected firmware update from the Dell repository and updates the managed hosts.
   - **Dell Custom Online**—the OMIVV downloads the selected firmware updates from the Dell Custom Online, and applies to the managed hosts as necessary.

     **NOTE:** Based on the network settings, enable proxy settings if the network needs a proxy.
   - **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:** If you are using CIFS share, the repository passwords cannot exceed 31 characters.

     **NOTE:** Ensure that you use the latest Dell EMC Repository Manager(DRM) version (3.0) and later.

   a. If you select **Dell Custom Online**, enter the **Catalog Online Path** in the following format:
      - `http://share/filename.xml.gz`
      - `http://share/filename.gz`
      - `https://share/filename.xml.gz`
      - `https://share/filename.gz`

   b. If you select **Shared Network Folder**, enter the **Catalog File Location** in 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. Dell EMC recommends using SMB version 2.0 based CIFS shares.

      **NOTE:** If you are using CIFS share, OMIVV prompts you to enter the username and password.

   c. To validate the given catalog file location, click **Begin Test**. This validation is mandatory to continue further.

✓

—Indicates that the test connection is successful.

✖—Indicates that the test connection is failed.

3. Click **Apply**.

> ⓘ **NOTE:** It might take up to 10 minutes to read the catalog from the source and update the OMIVV database.

## Creating catalog in DRM using OMIVV

This section describes the process to create a catalog in DRM version 3.0 and later.

1. On the Home page, click **Add New Repository**.
   The **Add Repository** window is displayed.
2. In the **Add Repository** window, do the following:
   a. Enter **Repository Name** and **Description**.
   b. From the **Base Catalog** drop-down menu, select a catalog.
   c. From the **Integration Type** drop-down menu, select **OpenManage Integration for VMware vCenter**.
3. In the **OpenManage Integration for VMware vCenter** window, enter **Virtual Appliance IP**, **vCenter Server IP**, **Username**, and **Password**, and click **Connect**.
   The created catalog is displayed on the home page.
4. To export the catalog, select a catalog and click **Export**.

## Configuring latest appliance version notification

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:

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.
3. 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.

> ⓘ **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.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings**, at the right side of **Deployment Credentials**, click the ✎ 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

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.

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

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 server IP or fqdn>:1311*
3. To apply the OMSA URL to all vCenter servers, select **Apply these settings to all vCenters**.

   **NOTE:** 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 **OMIVV Host Information** section.

## Configuring events and alarms

The **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 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.

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

**NOTE:** To receive the Dell events, enable both alarms and events.

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**.

   > **NOTE:** 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 Events, alarms, and health monitoring.
6. If you want to apply these settings to all vCenters, select **Apply these settings to all vCenters**.

   > **NOTE:** Selecting the option overrides the existing settings for all vCenters.

   > **NOTE:** The option is not available, if you have already selected **All Registered vCenters** from the drop-down list on the **Settings** tab.

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, see the Modifying inventory job schedules or the Modifying warranty job schedules.
4. Click **Data Retrieval Schedule** again to contract the inventory and warranty schedules and display a single line.

## Configuring SNMP trap community string

1. On the **OpenManage Integration for VMware vCenter** page, 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.

7

# Using Baseline tab

You can use the Baseline tab to create repository profile and cluster profile.

**Topics:**

- Repository profile
- Creating repository profile
- Editing repository profile
- Deleting repository profile
- Cluster profile
- Creating cluster profile
- Editing cluster profile
- Deleting cluster profile

## Repository profile

Repository profile allows you to create or maintain multiple driver or firmware repository profiles. These driver or firmware repository profiles can be used in:

- Baseline profile to identify drift for vSAN cluster.
- Update driver or firmware for vSAN clusters or vSAN cluster nodes.

> **NOTE:**
>
> - Use a custom firmware catalog created specific to your vSAN environments.
> - Driver repository profile can have a maximum of 10 drivers.
>
>   > **NOTE:** Ensure that you do not have more than 10 offline bundles (.zip files). If more files are present, the selection of drivers is random.
> - For driver repository profile, only VIB-formatted asynchronous drivers from offline bundles are used (.zip files).
>
>   > **NOTE:** Only the necessary asynchronous VIB drivers that are validated against the vSAN requirements. For information, see VMware Hardware Compatibility Matrix.
> - For driver repository profile, OMIVV requires write access to the CIFS or NFS.
> - For driver repository profile, files within the subfolders or files exceeding 10 MB sizes are ignored.
> - Only after successful parsing, the repository profiles are available for use in the **Baseline Profile** or for running a job to update the vSAN driver or firmware.
> - If more than one version of firmware is available, the latest firmware version is always used for compliance comparison.

To launch the repository profile page, perform the following steps:

1. On the **OpenManage Integration for VMware vCenter** page, click the **Manage** > **Baseline** tab, expand **Baseline Info**, and then click **Repository Profile**.
    a. On the **Repository Profile** page, view the list of repository profiles that you have created.

       A table is displayed, that lists the repository profiles along with **Profile Name**, **Description**, **Type**, **Share Path**, **Last Successfully Updated Time**, and **Last Refresh Status**.

    b. To view further details of a repository profile, select the desired repository profile.

       View the repository profile information that displays such as **Profile Name**, **Share Path**, **Date Created**, **Date Modified**, and **Last Modified By**.

    c. To swap the columns within the data grid, drag columns within the data grid.
    d. To filter or search the content of the data grid, type the filter criteria in the **Filter** field.

e. To export the repository profile information to a .CSV file, select a repository profile, and click 📤 in the right-hand corner of the data grid.

# Creating repository profile

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Repository Profile**.
2. Click ➕.
3. On the **Welcome** page, read the instructions, and click **Next** to add further details:
   a. In the **Profile Name** box, type the repository profile name.
   b. In the **Profile Description** field, type a description, which is optional.
   c. Click **Next**.
4. In the **Profile Settings** dialog box, select one of the following repository types:
   - Firmware (By default, this option is selected)
   - Driver

   a. In the **Repository Share Location** field, type the repository share location (CIFS or NFS).
   b. For CIFS share, type the user name and password.

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

   c. To validate the access for the given repository path and existence of the catalog file for firmware and driver repository, click **Begin Test**. This validation is mandatory to continue further.

   ✅: Indicates that the test connection is successful.

   ❌: Indicates that the test connection is failed.

   d. Click **Next**.

   ⓘ **NOTE:** For driver repository, download the offline driver .zip files and save to the shared location and provide the full path of the shared location. OMIVV automatically creates the catalog inside the OMIVV appliance. VIB driver bundles are available at https://my.vmware.com/web/vmware/downloads.
5. Click **Next**.

   The **Summary** page is displayed that provides the information about the repository profile.
6. Click **Finish**.
   After creating the catalog, the catalog download and parsing will start and status will be displayed on the home page of the repository profile.

   Successfully parsed repository profiles are available during the cluster profile creation, and during the vSAN firmware update.

# Editing repository profile

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Repository Profile**.
2. Select a repository profile that you want to edit and click ✎.
3. On the **Repository Profile** wizard, you can edit the **Profile Name** and **Description**, which is optional, and then click **Next**.
4. In the **Profile Settings** dialog box, do the following:
   a. You can edit the CIFS credentials.
   b. To validate the access for the given repository path and existence of the catalog file for firmware and driver repository, click **Begin Test**. This validation is mandatory to continue further.

   ✅: Indicates that the test connection is successful.

   ❌: Indicates that the test connection is failed.

   c. To refresh the repository with latest content in the specified location, click **Synchronize with Repository Location**.

      Ensure that **Synchronize with repository Location** option is selected if you want to refresh your Repository Profile of OMIVV from the latest driver or firmware catalog.

5. Click **Next**.
   The **Summary** page is displayed that provides the information about the repository profile.
6. Click **Finish**.

# Deleting repository profile

Before deleting the repository profile, ensure that you unlink the repository profile from the associated cluster profiles.

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Repository Profile**.
2. Select a repository profile that you want to delete, then click ✖.
3. To remove the profile, in the confirmation dialog box, click **Yes**, or to cancel, click **No**.

# Cluster profile

Cluster profile enables you to capture the baseline configuration such as hardware configuration (only for 14th generation servers), firmware, or driver versions and maintain the desired state for vSAN clusters by identifying the drift against the baseline.

**NOTE:**
- Firmware and Driver Repository Profiles must be parsed after being created before it can be used for a cluster profile creation.
- Once the cluster profile is created, it triggers the Drift Detection job.
- When a cluster is associated to a cluster profile, it overrides previous cluster profile associations.

To launch the cluster profile page, perform the following steps:

1. On the **OpenManage Integration for VMware vCenter** page, click the **Manage** > **Baseline** tab, expand the **Baseline Info**, and then click **Cluster Profile**.
   a. On the **Cluster Profile** page, view the list of cluster profiles that you have created.

      A table is displayed, that lists the cluster profiles along with **Profile Name**, **Description**, **Associated System Profile**, **Associated Firmware Repository Profile**, **Associated Driver Repository Profile**, **Last Successfully Updated Time**.

      **NOTE:** If any latest version of repository profile is available for an existing cluster profile, a warning symbol is displayed against the associated firmware or driver profile.

   b. To view further details of a cluster profile, select the desired cluster profile.

      View the cluster profile information that displays the details of **Profile Name**, **Date Created**, **Date Modified**, and **Last Modified By**.

   c. To swap the columns within the data grid, drag columns within the data grid.
   d. To filter or search the content of the data grid, use **Filter**.
   e. To export the repository profile information to a .CSV file, select a repository profile, and then in the right-hand corner of the data grid, click 📤.

# Creating cluster profile

1. System profile, Repository profile for both firmware and drivers, homogeneous server models for the cluster.
2. vSAN cluster must be present in the vCenter.
3. Connection profile must be created for at least one host in vSAN cluster and inventory should be run successfully.

**NOTE:** For an MX host managed using a chassis profile, even if the cluster profile has defined system profile, firmware, and driver repository, only the firmware and driver compliance levels are calculated.

**NOTE:** If multiple standalone vCenters are registered to OMIVV, it is recommended to create distinct Cluster profiles for each vCenter.

**NOTE:** At the creation of the cluster profile, a current snapshot of the associated Firmware and Driver Repository is created for the baseline. If the repositories change, the cluster profile would need to be updated again to reflect the changes. Otherwise, any updates performed on the repositories will not be updated to original cluster profile snapshot.

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Cluster Profile**.
2. Click ✚.
3. On the **Welcome** page, read the instructions, and click **Next** to add further details:
   a. In the **Profile Name** field, type the cluster profile name.
   b. In the **Profile Description** field, type description of the cluster profile. The profile description is optional.
   c. Click **Next**.
4. In the **Profile Settings** dialog box, do the following:
   a. Select the system profile, or repository profile (Firmware Repository Profile or Driver Repository Profile), or its combinations.

      **NOTE:** System profile is applicable only for 14th generation servers.

      **NOTE:** Dell EMC recommends you to create baseline with System profile, Firmware and Driver repository.

   b. Click **Next**.
5. In the **Profile Association** dialog box, do the following:
   a. Select the registered vCenter server from the drop-down list.
   b. Click **Browse** to associate the required vSAN clusters.
   c. Click **Next**.
6. In the **Drift Detection Schedule** dialog box, select the day and time, and click **Next**.

   The **Summary** page is displayed that provides the information about the cluster profile.
7. Click **Finish**.

   The cluster profile is automatically saved, and is displayed on the **Cluster Profile** page.

   **NOTE:** The Drift Detection job runs immediately after the cluster profile is saved and later runs during the scheduled time.

# Editing cluster profile

**NOTE:** Editing cluster profile changes the baseline, which may result in the recalculation of a compliance level.

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Cluster Profile**.
2. Select a cluster profile that you want to edit and click ✏.
3. On the **Cluster Profile** wizard, you can edit the **Description**, which is optional, and then click **Next**.

   **NOTE:** You cannot edit the profile name.

4. In the **Profile Settings** dialog box, you can change the profile combinations.
5. In the **Profile Association** dialog box, you can change the associations and configurations required in the cluster profile.
6. In the **Profile Configuration** dialog box, you can edit the **Drift Detection Schedule**, and click **Next**.

   The **Summary** page is displayed that provides the updated information about the cluster profile.
7. Click **Finish**.

   The updated cluster profile is automatically saved, and is displayed on the cluster profiles window.

**NOTE:** The Drift Detection job runs immediately after the cluster profile is saved and later runs during the scheduled time.

# Deleting cluster profile

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Baseline**, expand **Baseline Info**, and then click **Cluster Profile**.
2. Select a cluster profile that you want to delete, click ✖.
3. To remove the profile, in the confirmation dialog box, click **Yes**, or to cancel, click **No**.
   If the cluster profile is deleted, the corresponding Drift Detection job is also deleted.

8

# Profiles

**Credential Profiles** allows you to manage and configure the connection profiles, and the chassis profiles while **Deployment Template** allows you to manage and configure hardware and hypervisor profiles.

**Topics:**

- About connection profile
- About chassis profile

## About connection profile

The **Connection Profiles** tab lets you manage and configure connection profiles that contain credentials that are in use by the virtual appliance to communicate with the servers. Associate each OMIVV-managed server with only one connection profile for management by the OpenManage Integration for VMware vCenter. You can assign multiple servers to a single connection profile. After you run the **Initial Configuration Wizard**, you can manage connection profiles from OpenManage Integration for VMware vCenter by performing the following tasks:

- Viewing connection profile
- Creating a connection profile
- Modifying connection profile
- Deleting connection profile
- Testing connection profile

## Viewing connection profiles

A connection profile must be created and/or exist before it can be viewed. After one or more connection profiles are created, they can be viewed in the **Connection Profiles** page. The OpenManage Integration for VMware vCenter uses the credentials that are provided in the profiles to communicate with Dell EMC hosts.

1. In OpenManage Integration for VMware vCenter, click **Manage**.
2. Click **Profiles** and then click **Credential Profiles**.
3. Expand **Credential Profiles** and click **Connection Profiles** tab.

   You can view all the connection profiles that you have created.

   **NOTE:** If an MX host is managed using the chassis IP, the OMIVV indicates it as associated to a chassis profile. For more information, see Viewing chassis profiles on page 52.

**Table 7. Connection profile information**

| Connection profile fields | Description |
|---|---|
| **Profile Name** | Displays the name of the connection profile |
| **Description** | Displays a description, if provided |
| **vCenter** | Displays the FQDN or hostname, or else IP address of the vCenter as per the context. |
| **Associated Hosts** | Displays the hosts that are associated with the connection profile. If more than one, use the expand icon to display all. |
| **iDRAC Certificate Check** | Displays whether the iDRAC Certificate Check is enabled or disabled. |
| **Host Root Certificate Check** | Displays whether the Host Root Certificate Check is enabled or disabled. |

**Table 7. Connection profile information**

| Connection profile fields | Description |
|---|---|
| **Date Created** | Displays the date when the connection profile was created. |
| **Date Modified** | Displays the date when the connection profile was modified. |
| **Last Modified By** | Displays the details of the user who modified the connection profile. |

## Creating connection profile

You can associate multiple hosts to a single connection profile. To create a connection profile, perform the following steps:

> **NOTE:** The vCenter hosts that are listed during this procedure are authenticated using the same Single Sign On (SSO). If you do not see a vCenter host, it might be on a different SSO or you might be using a VMware vCenter version that is less than version 5.5.

> **NOTE:** An MX chassis hosts can be managed using a single unified chassis management IP. To manage an MX chassis using a chassis profile, see Creating chassis profile. It is recommended to manage MX chassis hosts with iDRAC IP to get complete OMIVV functions.

1. In OpenManage Integration for VMware vCenter, from the **Manage** → **Profiles** → **Credential Profiles** → **Connection Profiles** tab, click +.
2. On the **Welcome** page, read the instructions, and click **Next**.
3. In the **Connection Profile** page, enter the following details:
    a. Under **Profile**, type the **Profile Name** and optional **Description**.
    b. Under **vCenter**, select vCenter servers from the drop-down list on which to create the profile.
    This option enables you to create one connection profile for each vCenter.
    c. In the **iDRAC Credentials** area, perform one of the following tasks:

    > **NOTE:** The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.

    - For iDRAC that is already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**; otherwise skip to the next option.
        - In the **Active Directory User Name** text box, type the user name. Type the user name in one of the formats, such as `domain\username` or `username@domain`. The user name is limited to 256 characters. See the Microsoft Active Directory Documentation for user name restrictions.
        - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
        - In the **Verify Password** text box, type the password again.
        - For verifying the iDRAC certificate, select one of the following:
            - To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
            - To not perform any verification and not store the certificate, clear **Enable Certificate Check**.
    - To configure the iDRAC credentials without Active Directory, perform the following actions:
        - In the **User Name** text box, type the user name. The user name is limited to 16 characters. See the iDRAC Documentation for information about user name restrictions for your version of iDRAC.

            > **NOTE:** The local iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.
        - In the **Password** text box, type the password. The password is limited to 20 characters.
        - In the **Verify Password** text box, type the password again.
        - For verifying the iDRAC certificate, select one of the following:
            - To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
            - To not perform any verification and not store the certificate, do not select **Enable Certificate Check**.

    d. In the **Host Root** area, do one of the following:

    - For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip to configure your host credentials.

        - In the **Active Directory User Name** text box, type the user name. Type the user name in either of the formats, such as `domain\username` or `username@domain`. The user name is limited to 256 characters. See the Microsoft Active Directory Documentation for user name restrictions.
        - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
        - In the **Verify Password** text box, type the password again.
        - For certificate check, select one of the following:
            - To download and store the host certificate and validate it during all future connections, select **Enable Certificate Check**.
            - To not perform any check and not store the host certificate, do not select **Enable Certificate Check**.
    - To configure host credentials without Active Directory, perform the following actions:
        - In the **User Name** text box, the user name is root.

          The root user name is the default user name, and you cannot change it.

          **NOTE:** If Active Directory is set, you can choose any Active Directory user name and not root.
        - In the **Password** text box, type the password. The password is limited to 127 characters.
        - In the **Verify Password** text box, type the password again.
        - For certificate check, select one of the following:
            - To download and store the host certificate and validate it during all future connections, select **Enable Certificate Check**.
            - To not perform any check and not store the host certificate, do not select **Enable Certificate Check**.

    **NOTE:** The OMSA credentials are the same credentials used for the ESXi hosts.

4. Click **Next**.
5. In the **Select Hosts** window, select hosts for this connection profile and click **OK**.
6. In the **Associated Hosts** page, add one or more hosts for the connection profile, if required.

   To add hosts, click ✚, select hosts, and then click **OK**.

   **NOTE:** If the OEM hosts are not displayed on the **Select Hosts** window, add the OEM hosts using the **Add OEM Hosts** wizard. For more information about adding OEM hosts, see Adding OEM Hosts.

7. To test the connection profile, select one or more hosts and click .

   **NOTE:** This step is optional and verifies whether the host and iDRAC credentials are correct. Although this step is optional, it is recommended that you to test the connection profile.

   **NOTE:** If the WBEM service is disabled for all hosts running ESXi 6.5 or later, WBEM is automatically enabled when you perform the test connection and inventory on those hosts.

   **NOTE:** If you select **All Registered vCenter** while creating the connection profile, test connection fails for all hosts running ESXi 6.5 or later that has the WBEM service disabled. In such case, it is recommended to complete the connection profile wizard actions, run the inventory on hosts, and then test the connection profile again.

   **NOTE:** : Do not add an MX server having iDRAC IPv4 disabled to a connection profile. These servers can be managed using a chassis profile.

   **NOTE:** You may see test connection is failing for the host and indicating that invalid credentials are entered, even after entering valid credentials. It may happen because the ESXi is blocking the access. At this point, wait for 15 minutes and retry the test connection.

8. To complete the profile creation, click **Next**.
   For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states **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 hosts running ESXi and later. 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 noncomplaint. To view the noncomplaint hosts that require SNMP trap destination to be reconfigured and/or WBEM services to be enabled, see Running the fix noncompliant vSphere hosts wizard.

## Modifying connection profile

After you create a connection profile, you can edit the profile name, description, associated hosts and iDRAC, and host credentials.

**NOTE:** The **vCenters** listed during this procedure are authenticated using the same Single Sign On (SSO). If you cannot view a vCenter host, it might be on a different SSO or you might be using a VMware vCenter version earlier than version 5.5.

**NOTE:** Ensure that you do not update a connection profile when an inventory, a warranty, or a deployment job is running.

**NOTE:** Ensure that you do not move a host that is associated with a connection profile to another connection profile or remove a host from a connection profile when an inventory, a warranty, or a deployment job is running.

1. In OpenManage Integration for VMware vCenter, click **Manage**.
2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand **Credential Profiles**, and then click **Connection Profiles**.
4. Select a profile, and click ✎.
5. In the **Welcome** tab of the **Connection Profile** window, read the information and click **Next**.
6. In the **Name and Credentials** tab, perform the following steps:
   a. Under **Profile**, type the **Profile Name** and **Description**, which is optional.
   b. Under **vCenter**, view the associated hosts for this connection profile. See the note preceding about why you see the hosts displayed here.
   c. Under **iDRAC Credentials**, perform one of the following steps:
      - For the iDRAC accounts that are already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**.
        - In the **Active Directory User Name** text box, type the user name. Type the user name in one of these formats; `domain\username` or `domain/username`, or `username@domain`. The user name is limited to 256 characters. See the Microsoft Active Directory Documentation for user name restrictions.
        - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
        - In the **Verify Password** text box, type the password again.
        - For certificate check, select one of the following:
          - To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
          - To perform no check and not store the certificate, do not select **Enable Certificate Check**.
      - To configure the iDRAC credentials without Active Directory, enter the following:
        - **User Name**—type the user name in one of these formats, such as `domain\username`, or `domain@username`. See the iDRAC Documentation for information aboutuser name restrictions for your versionof iDRAC.
        - **Password**—type the password.
        - **Verify password**—retype your password.
        - **Enable Certificate Check**—by default, the check box is clear. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**. To perform no certificate check and not store the certificate, do not select the **Enable Certificate Check** check box.

          **NOTE:** Select **Enable Certificate Check** if you are using Active Directory.
   d. Under **Host Root**, do the following tasks:
      - To access all the consoles associated with the Active Directory, select the **Use Active Directory** check box.
      - **User Name**—the default user name is root and cannot be modified. If **Use Active Directory** is selected, you can use any Active Directory user name.

        **NOTE:** The **User Name** is root and this entry cannot be modified if you do not select **Use Active Directory**. It is not compulsory for the iDRAC user to use the root credential, and it can be any administrator privilege if Active Directory is set.
      - **Password**—type the password.
      - **Verify password**—retype your password.
      - **Enable Certificate Check**—by default, the check box is clear. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**. To perform no certificate check and not store the certificate, clear the **Enable Certificate Check** check box.

        **NOTE:** Select **Enable Certificate Check** if you are using Active Directory.

**NOTE:** The OMSA credentials are the same credentials as used for the ESXi hosts.

**NOTE:** For hosts that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states **Not Applicable** for this system.

7. Click **Next**.
8. In the **Select Hosts** dialog box, select hosts for this connection profile.
9. Click **OK**.

   The **Associated Host** dialog box lets you test the iDRAC and host credentials on the selected servers.
10. Perform one of the following steps:
    - To begin the test, select the hosts and then click

      . The other options are inactive.

      **NOTE:** : Do not add an MX server having iDRAC IPv4 disabled to a connection profile. These servers can be managed using a chassis profile.

      **NOTE:** If the WBEM service is disabled for all hosts running ESXi 6.5 or later, WBEM is automatically enabled when you perform the test connection and inventory on those hosts.

      When the test is complete, click **Finish**.
    - To stop the tests, click **Abort All Tests**. In the **Abort Tests** dialog box, click **OK**, and then click **Finish**.

**NOTE:** The **Date Modified** and **Last Modified By** fields include changes that you perform through the web client interface for a connection profile. Any changes that the OMIVV appliance performs on the respective connection profile do not affect these two field details.

## Deleting connection profile

**NOTE:** Ensure that you do not delete a connection profile that is associated with a host when an inventory, a warranty, or a deployment job is running.

1. In OpenManage Integration for VMware vCenter, click **Manage**.
2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand **Credential Profiles**, click the **Connection Profiles** tab, and select the profiles to delete.
4. Click ✖.
5. To remove the profile, click **Yes** for the delete confirmation message, or to cancel the delete action, click **No**.

**NOTE:** OMIVV does not manage the hosts that are part of the connection profile that you deleted, until those hosts are added to another connection profile.

## Testing connection profile

1. In OpenManage Integration for VMware vCenter, click **Manage**.
2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand **Credential Profiles**, click the **Connection Profiles** tab, and select a connection profile.
4. In the **Test Connection Profile** dialog box, select the hosts you want to test, and then click the icon.

   If you do not select a connection profile, running test connection takes some time.
5. To stop all selected tests and cancel the testing, click **Abort All Tests**. In the **Abort Tests** dialog box, click **OK**.
6. To exit, click **Cancel**.

# About chassis profile

OMIVV can monitor all Dell EMC Chassis associated with the Dell EMC servers. A chassis profile is required to monitor the chassis. You can manage chassis profile by performing the following tasks:

- View chassis profile. See Viewing chassis profile.
- Create chassis profile. See Creating chassis profile.
- Edit chassis profile. See Editing chassis profile.
- Delete chassis profile. See Deleting chassis profile.
- Test chassis profile. See Testing chassis profile.

# Viewing chassis profiles

Ensure that you create a chassis profile or a chassis profile exists before viewing.

After one or more chassis profiles are created, you can view the chassis and associated hosts on the chassis profiles page.

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.
   The chassis profiles are displayed.
4. To display all the associated chassis, click the ☰ icon, if multiple chassis are associated with the chassis profile.
5. In the **Chassis Profiles** page, view the chassis information.

### Table 8. Chassis profile information

| Chassis fields | Description |
|---|---|
| **Profile Name** | Displays the name of the chassis profile. |
| **Description** | Displays a description, if provided. |
| **Chassis IP/Host Name** | Displays the IP address of the chassis or the host name<br>For an MCM group, the lead chassis (▥) and the member chassis (▥) are listed in hierarchy.<br>**NOTE:** For a member chassis in the MCM group where IPv4 is disabled, an IPv4 address of the lead is displayed with the Service Tag of the member chassis in brackets. |
| **Chassis Service Tag** | Displays the unique identifier that is assigned to a chassis. |
| **Date Modified** | Displays the date when the chassis profile was modified. |

The following information about the associated hosts is displayed in the lower grid:

- **Profile Name**
- **Associated Hosts**
- **Service Tag**
- **Chassis IP/Host name**
- **Chassis Service Tag**

**NOTE:** For an MX chassis in MCM configuration, OMIVV will manage all the lead and member chassis using lead chassis only and all the lead and members will be associated to the same chassis profile to which lead chassis is associated.

## Creating chassis profile

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

You can log in to iDRAC and the host using Active Directory credentials.

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:

   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 + to associate the chassis with the chassis profile.

   > ⓘ **NOTE:** The chassis which are discovered, available, and manually added using **Add MX Chassis** is associated with the chassis profile only after the successful inventory run of any modular host present under that chassis.

7. 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, and 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.

8. Click **OK**.

   The **Associated Chassis** page is displayed.

9. Test connection is mandatory and runs automatically for the selected chassis.

   Test connection runs automatically:

   - For the first time after the chassis is selected
   - When you change the credentials
   - If the chassis is newly selected

   > ⓘ **NOTE:** For an MX chassis configured with an MCM group, Dell EMC recommends managing all the lead and member chassis using the lead chassis. The member chassis test connection operation will fail and test result status that is indicated as **Fail**. Click the lead chassis IP link to discover the complete MCM group.

   The test result is displayed in the **Test Result** column as **Pass** or **Fail**. To test the chassis connectivity manually, select the chassis and click .

   > ⓘ **NOTE:** If there are no hosts present in the registered vCenters which are associated to the added MX chassis, the respective chassis test connection fails.

   > ⓘ **NOTE:** Only successfully validated chassis is associated with a chassis profile.

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

    > ⓘ **NOTE:** Ensure that you have at least one successfully validated chassis to complete the wizard.

To add an MX chassis management module IP, see Adding an MX Chassis on page 102.

## Editing chassis profile

After you have created a chassis profile, you can edit the profile name, description, associated chassis, and credentials.

1. On the **OpenManage Integration for VMware vCente**r page, click **Manage**.
2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand **Credential Profiles**, click the **Chassis Profiles** tab, and select a chassis profile.
4. Click the ✎ icon on the main menu.
   The **Edit Chassis Profile** window is displayed.
5. In **Chassis Profile**, you can edit the **Profile Name** and **Description**, which is optional.
6. Under the **Credentials** area, you can edit the **User Name**, **Password**, and **Verify Password**.
   The password that you type in **Verify Password** must be same as the one you entered in the **Password** field. The credentials entered must have administrator rights on the chassis.
7. Click ✚ to associate the chassis with the chassis profile.

   **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.

8. 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.
9. Click **OK**.

   The **Associated Chassis** page is displayed.
10. Test connection is mandatory and runs automatically for the selected chassis.

    Test connection runs automatically:

    - For the first time after the chassis is selected
    - When you change the credentials
    - If the chassis is newly selected

    **NOTE:** For an MX chassis configured with an MCM group, the member chassis test connection operation will fail and test result status indicated as **Fail**. Click the lead chassis IP link to discover the complete MCM group.

    The test result is displayed in the **Test Result** column as **Pass** or **Fail**. To test the chassis connectivity manually, select the chassis and click .

    **NOTE:** If there are no hosts present in the registered vCenters which are associated to the added MX chassis, the respective chassis test connection fails.

    **NOTE:** Only successfully validated chassis is associated with a chassis profile.
11. To complete the profile, click **Finish**.

    **NOTE:** Ensure that you have at least one successfully validated chassis to complete the wizard.

    To add the MX chassis management module IP, see Adding MX Chassis IP or FQDN.

## Deleting chassis profiles

**NOTE:** Before deleting the chassis profile, ensure that the chassis instances are not part of other vCenters which OMIVV is registered with.

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. Select a chassis profile that you want to delete and click ✖.
   A warning message is displayed.
5. To proceed with deletion, click **Yes**, or to cancel deletion, click **No**.

   If all the chassis that is associated to a chassis profile is cleared or moved to different profiles, a delete confirmation message is displayed stating that the chassis profile does not have any associated chassis and is deleted. To delete the chassis profile, click **OK** for the delete confirmation message.

ⓘ **NOTE:** OMIVV does not monitor the chassis that are associated with the chassis profiles that you have deleted, until those chassis are added to another chassis profile.

## Testing chassis profile

1. In OpenManage Integration for VMware vCenter, click **Manage**.
2. Click **Profiles**, and then click **Credential Profiles**.
3. Expand the **Credential Profiles**, click the **Chassis Profiles** tab, and then select a single or multiple chassis profile to test.
   This action may take several minutes to complete.
4. In the **Test Chassis Profile** dialog box, select the chassis you want to test and then click .
5. To abort all selected tests and cancel the testing, click **Abort All Tests**. In the **Abort Tests** dialog box, click **OK**.
6. To exit, click **Cancel**.

9

# Inventory and warranty management

After you configure OMIVV, you can monitor the inventory, warranty jobs, manage deployment jobs, and manage firmware update jobs under the **Monitor** tab. The inventory and warranty are set up in the **Initial Configuration Wizard** or from the **Settings** tab.

The job queue page manages the following jobs:

- Displaying the submitted server deployment or firmware update jobs.
- Refreshing the firmware update or deployment jobs, or inventory/warranty history queues.
- Scheduling an inventory or warranty job.
- Purging the firmware update or deployment job queue entries.

ⓘ **NOTE:** To ensure the inventory/warranty contains up-to-date information, schedule the inventory/warranty job to run once a week at a minimum.

The tasks that you can perform in this page include:

- Managing deployment jobs
- Managing firmware update jobs
- Managing inventory jobs
- Managing warranty jobs

ⓘ **NOTE:** For all the mentioned jobs, ensure that they are scheduled again if the appliance time is changed to a future date and reverted.

ⓘ **NOTE:** For Basic Health Monitoring, ensure that you reboot the OMIVV appliance. For Extended Health Monitoring, ensure that you disable **Extended Monitoring**, and then enable it from the OMIVV Administration Console.

**Topics:**

- Inventory jobs
- Warranty jobs
- Monitoring single host
- Monitoring hosts on clusters and data centers
- Setting up physical server blink indicator light
- Configuring System Lockdown Mode

# Inventory jobs

The inventory jobs are set up by using the **Settings** tab or the **Initial Configuration Wizard**. Use the **Inventory History** tab to view all the inventory jobs. The tasks that you can perform from this tab include:

- Viewing hosts or chassis inventory
- Modifying inventory job schedules
- Running a chassis inventory job now

## Viewing host inventory

A successfully completed inventory is required to gather the data. Once the inventory is complete, you can view the inventory results for the entire data center or for an individual host system. You can sort the columns of the inventory view in ascending and/or descending order.

ⓘ **NOTE:** The following are several possible causes when the host data cannot be retrieved and displayed:

- The host is not associated with a connection profile, and therefore you cannot run an inventory job.
- An inventory job has not been run on the host to collect the data, and therefore there is nothing to display.

- The number of host licenses exceeds, and you must have additional licenses available for the inventory task to complete.
- The host does not have the correct iDRAC license required for 12th and later generation of PowerEdge servers and hence, purchase the correct iDRAC license.
- The credentials might be wrong.
- The host might not be reachable.

To view the host inventory details:

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, expand **Inventory History**, and then click **Host Inventory**.
   The vCenter information is displayed in the upper grid.
3. To view the host information on a selected vCenter, select a vCenter to display all associated host details.
4. Review the host inventory information.

Table 9. vCenter, host information

| vCenter | |
|---|---|
| **vCenter** | Displays vCenter address |
| **Hosts Passed** | Displays any hosts, which have passed |
| **Last Inventory** | Displays the date and time when the last inventory schedule was run |
| **Next Inventory** | Displays the date and time when the next inventory schedule will run |
| **Hosts** | |
| **Host** | Displays the host address. |
| **Status** | Displays the status. The options include:<br>● Successful<br>● Failed<br>● In Progress<br>● Scheduled |
| **Duration (MM: SS)** | Displays the duration of the job in minutes and seconds |
| **Start Date and Time** | Displays the date and time when the inventory schedule started |
| **End Date and Time** | Displays the time the inventory schedule ended |

## Viewing chassis inventory

A successfully completed inventory is required to gather the data. You can sort the columns of the inventory view in ascending and/or descending order.

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, expand **Inventory History**, and then click **Chassis Inventory**.
3. Review the chassis inventory information.

   In an MCM group, inventory runs only on lead chassis. Inventory information provides data about both lead and member chassis.

Table 10. Chassis information

| Chassis inventory | |
|---|---|
| **Chassis IP** | Displays the chassis IP address |
| **Service Tag** | Displays the Service Tag of the chassis. The Service Tag is a unique identifier that is provided by the manufacturer for support and maintenance. |

Table 10. Chassis information

| Chassis inventory | |
|---|---|
| **Status** | Displays the status of the chassis. |
| **Duration (MM: SS)** | Displays the duration of the job in minutes and seconds. |
| **Start Date and Time** | Displays the date and time when the inventory schedule started. |
| **End Date and Time** | Displays the time the inventory schedule ended. |

**NOTE:** The chassis inventory is not supported on the following PowerEdge servers: C6320P, C6320, C4130, and C6420.

**NOTE:** MX chassis blade servers are supported only with ESXi versions 6.5U2 and later. If the earlier ESXi versions are deployed on these hosts, the inventory job fails in OMIVV.

## Modifying inventory job schedules

To ensure that there is up-to-date host information, schedule the inventory job to run at a minimum frequency of once a week. The inventory job consumes minimal resources and does not degrade host performance. You can change the inventory job schedule from the **Initial Configuration Wizard** or from the **Monitor** tab.

The inventory job schedule sets the time or day for running inventory jobs, such as:

- Weekly at a specific time and on selected days
- At a set time interval

To perform an inventory on host systems, create a connection profile that provides communication and authentication information.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, **Inventory History**, and then click **Host Inventory**.
3. Select a vCenter, and then click 📅.
4. In the **Inventory Data Retrieval** dialog box, do the following:
    a. Under **Inventory Data**, select the **Enable Inventory Data Retrieval** check box.
    b. Under **Inventory Data Retrieval Schedule**, select the days of the week for your job.
    c. In the **Inventory 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.
5. To save the settings, click **Apply**, to reset the settings, click **Clear**, and to abort the operation, click **Cancel**.
6. To run the job now, from the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Inventory History** > **Hosts Inventory**.
7. Click ▶, and in the **Success** dialog box, click **Close**.

**NOTE:** When you run a modular host inventory, the corresponding chassis are discovered automatically. The chassis inventory runs automatically after host inventory if chassis is already part of a chassis profile.

After scheduling an inventory job now, the inventory job is now in a queue. You cannot run an inventory for a single host. An inventory job starts for all hosts.

## Running inventory jobs

1. Once the **Configuration Wizard** is complete, inventory is triggered automatically for all hosts which are added to a Connection Profile. For a subsequent inventory run on-demand, click **Job Queue** > **Inventory** > **Run Now** to run an inventory job.
2. To see the status of the inventory job, click **Refresh**.
3. Navigate to the **Host and Cluster** view, click on any **Dell EMC host**, then click the **OpenManage Integration** tab. The following information should be available:
    - Overview Page
    - System Event Log

- Hardware Inventory
- Storage
- Firmware

  **NOTE:** When the hosts are managed using the Chassis Profile, the firmware inventory data will show few extra components such as Lifecycle Controller and Software RAID.

- Power Monitoring

**NOTE:** Inventory job for hosts exceeding the license limit will be skipped and marked as Failed.

The following host commands work within the OpenManage Integration tab:

- Blink Indicator Light
- Run Firmware Update Wizard
- Launch Remote Access
- Launch OMSA
- Launch CMC/Management Module
- Configure System Lockdown Mode

**NOTE:** When the hosts are managed using chassis, Configure System Lockdown Mode is not supported.

## Running chassis inventory job now

You can view and run a chassis inventory job in the **Chassis Inventory** tab.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, **Inventory History**, and then click **Chassis Inventory**.
   The list of chassis and its status for the last inventory job is displayed.

   **NOTE:** The scheduled chassis inventory is run the same time as the scheduled host inventory.

3. Click ▶.
   The lists of updated inventoried chassis are displayed with the status against each chassis as **Success** or **Failure**.

   **NOTE:** During the inventory, the trap destination and alert policies are configured by OMIVV on the lead chassis in an MCM group.

   **NOTE:** When the hosts are managed using chassis, running chassis inventory will also trigger the host inventory for the hosts. Also, running host inventory will trigger the chassis inventory.

# Warranty jobs

Hardware warranty information is retrieved from Dell online and is displayed by OMIVV. The service tag of the server is used to gather warranty information about the server. The warranty data retrieval jobs are set up by using the **Initial Configuration Wizard**.

The tasks you can perform in this tab include:

- Viewing warranty history
- Modifying a warranty job schedule
- Running a hosts warranty job now
- Running a chassis warranty job now

## Viewing warranty history

A warranty job is a scheduled task to get warranty information from `Support.dell.com` on all systems. You can sort the columns of the inventory view in ascending and/or descending order.

**NOTE:** The OMIVV appliance requires internet connectivity to extract warranty information. Ensure that the OMIVV appliance has internet connectivity. Depending on the network settings, OMIVV might require proxy information for internet reachability and fetch warranty information. The proxy details can be updated in the Administration Console. See Setting up HTTP proxy on page 18.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, and then click **Warranty History**.
3. Expand **Warranty History** to display **Hosts Warranty** and **Chassis Warranty**.
4. To view your corresponding warranty job history information, select **Hosts Warranty**, and then select a vCenter to display all associated hosts details.

**Table 11. vCenter, hosts history information**

| vCenter history | |
|---|---|
| **vCenters** | Displays lists of vCenters |
| **Hosts Passed** | Displays the number of vCenter hosts that passed |
| **Last Warranty** | Displays the date and time when the last warranty job was run |
| **Next Warranty** | Displays the date and time when the next warranty job will run |
| **Hosts history** | |
| **Host** | Displays the host address |
| **Status** | Displays the status. The options include:<br>● Successful<br>● Failed<br>● In Progress<br>● Scheduled |
| **Duration (MM:SS)** | Displays the duration of the warranty job in MM:SS |
| **Start Date and Time** | Displays the date and time when the warranty job started |
| **End Date and Time** | Displays the time the warranty job ended |

## Viewing chassis warranty

A warranty job is a scheduled task to get warranty information from `Support.dell.com` on all systems. You can sort the columns of the inventory view in ascending and/or descending order.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, and then click **Warranty History**.
3. Expand **Warranty History** to display **Hosts Warranty** and **Chassis Warranty**.
4. Click **Chassis Warranty**.
5. View the chassis warranty details.

**Table 12. Chassis information**

| Chassis history | |
|---|---|
| **Chassis IP** | Displays the chassis IP address |
| **Service Tag** | Displays the service tag of the chassis. The service tag is a unique identifier provided by the manufacturer for support and maintenance |
| **Status** | Displays the status of the chassis |
| **Duration (MM: SS)** | Displays the duration of the warranty job in MM:SS |
| **Start Date and Time** | Displays the date and time when the warranty job started |
| **End Date and Time** | Displays the time the warranty job ended |

## Modifying warranty job schedules

The warranty jobs are originally configured in the **Initial Configuration Wizard**. You can modify warranty job schedules from the **Settings** tab.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, and then click **Warranty History**.
3. Expand **Warranty History** to display **Hosts Warranty** and **Chassis Warranty**.
4. To view your corresponding warranty job history information, select either **Hosts Warranty** or **Chassis Warranty**.
5. Click 📅.
6. In the **Warranty Data Retrieval** dialog box, do the following:
   a. Under **Warranty Data**, select the **Enable Warranty Data Retrieval** check box.
   b. Under **Warranty Data Retrieval Schedule**, select the days of the week for the warranty job.
   c. In the **Warranty Data Retrieval Time** text box, type the local time for this job.
      You might need to calculate the time difference required to run this job at the proper time.
7. Click **Apply**.

## Running host warranty job now

Run a warranty job at least once a week.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue**, and then click **Warranty History**.
3. Expand **Warranty History** to display **Hosts Warranty** and **Chassis Warranty**.
4. To view your corresponding warranty job history information, select either **Hosts Warranty** or **Chassis Warranty**.
5. Select the warranty job you want to run, and then click ▶.
6. In the **Success** dialog box, click **Close**.
   A warranty job is now in queue.

ⓘ **NOTE:** Chassis warranty is run automatically for all the chassis once the host warranty is run. In an SSO environment having multiple vCenters, the chassis warranty runs automatically with every vCenter when the warranty for any vCenter is run manually.

## Running chassis warranty job now

Run a warranty job at least once a week.

1. In the OpenManage Integration for VMware vCenter, navigate to the **Monitor** > **Job Queue** tab.
2. To select the warranty job you want to run, click **Warranty History**, and then **Chassis Warranty**.
3. Click ▶.
4. In the **Success** dialog box, click **Close**.
   A warranty job is now in queue.

# Monitoring single host

The OpenManage Integration for VMware vCenter enables you to view detailed information for a single host. You can access hosts in VMware vCenter from the Navigator pane, which displays all hosts for all vendors. To find more detailed information, click a specific OMIVV-managed host. To view a list of Dell EMC hosts, from OpenManage Integration for VMware vCenter, in the Navigator pane, click **Dell EMC hosts**.

## Viewing host summary details

You can view the host summary details for an individual host on the **Host Summary** page, where various portlets are displayed. Two of the portlets are applicable to the OpenManage Integration for VMware vCenter. The two portlets are:

- OMIVV Host Health
- OMIVV Host Information

You can drag and drop the two portlets to the position you want and can format and customize the two portlets like other portlets as per your requirement. To view the host summary details:

1. In the OpenManage Integration for VMware vCenter, in the Navigator pane, click **Hosts**.
2. In the **Objects** tab, select the specific host that you want to review.
3. Click the **Summary** tab.
4. View the host summary details:

**Table 13. Host summary information**

| Information | Description |
|---|---|
| **Alternating system** | Displays alerts for OpenManage Integration for VMware vCenter in a yellow box under the status area and preceding the portlets. |
| **Notification area** | Displays the Dell products integration information in the right side-panel area, where you can find information about:<br>● Recent Tasks<br>● Work In Progress<br>● Alarms<br>The Dell alarm information is displayed in the notification area portlet. |

5. Scroll down to view the OMIVV Server Management portlet.

**Table 14. OMIVV server Management portlet (continued)**

| Information | Description |
|---|---|
| **Service Tag** | Displays the service tag for your PowerEdge server. Use this ID when you call for support. |
| **Model Name** | Displays the server's model name. |
| **Fault Resilient Memory** | Displays the status of a BIOS attribute. The BIOS attribute is enabled in the BIOS during initial setup of the server and displays the memory operational mode of the server. Restart your system when you change the memory operational mode value. This is applicable for 12th Gen of the PowerEdge servers and later that support Fault Resilient Memory (FRM) option, running ESXi 5.5 or later version. The four different values of BIOS attribute are:<br>● Enabled and Protected: This value indicates that the system is supported and the operating system version is ESXi 5.5 or later and the memory operational mode in BIOS is set to FRM.<br>● NUMA Enabled and Protected: This value indicates that the system is supported and the operating system version is ESXi 5.5 or later and the memory operational mode in BIOS is set to NUMA.<br>● Enabled and Not Protected: This value indicates that it supports the system with operating system version lesser than ESXi 5.5.<br>● Disabled: This value indicates that it supports valid systems with any operating system version and the memory operational mode in BIOS is not set to FRM.<br>● Blank: If memory operational mode in BIOS is not supported, the FRM attribute is not displayed. |
| **System Lockdown Mode** | Displays the status of the iDRAC Lockdown Mode for 14th Gen PowerEdge servers. A closed lock represents the iDRAC |

### Table 14. OMIVV server Management portlet

| Information | Description |
|---|---|
| | Lockdown Mode is turned on whereas an opened lock represents the iDRAC Lockdown Mode is turned off. |
| **Identification** | Displays the following:<br>● Hostname—Displays name of the OMIVV-managed host<br>● Power State—Displays if power is ON or OFF<br>● iDRAC IP—Displays the iDRAC IP address<br>● Management IP—Displays the management IP address<br>● Connection Profile—Displays the connection profile name for this host<br>● Model—Displays the Dell EMC server model<br>● Service Tag—Displays the Service tag for the server<br>● Asset Tag—Displays the Asset tag<br>● Warranty Days Left—Displays the days left for the warranty<br>● Last Inventory Scan—Displays the date and time of the last inventory scan |
| **Hypervisor & Firmware** | Displays the following:<br>● Hypervisor—Displays the Hypervisor version<br>● BIOS Version—Displays the BIOS version<br>● Remote Access Card Version—Displays the remote access card version |
| **Management Consoles** | The management consoles are used to launch external system management consoles, such as:<br>● Launching the Remote Access Console (iDRAC)—launches the integrated Dell Remote Access Controller (iDRAC) web user interface.<br>● Launching OMSA console—launches the OMSA console to access the OpenManage Server Administrator user interface. |
| **Host Actions** | To blink at various time intervals, set up the physical server to blink at various time intervals. See Blink indicator light. |

6. View the OMIVV Host Health portlet:

### Table 15. OMIVV host health

| Information | Description |
|---|---|
| OMIVV Host Health | Component health is a graphical representation of the status of all major host server components: Server Global status, Server, Power supply, Temperature, Voltages, Processors, Batteries, Intrusion, Hardware log, Power management, Power and Memory. The chassis health parameters are applicable for models VRTX version 1.0 and later, M1000e version 4.4 and later. For versions less than 4.3 only two health indicators are displayed, namely Healthy and Warning or Critical (Inverted triangle with an exclamatory mark in orange color). The overall health indicates the health based on the chassis with the least health parameter. The options include:<br>● Healthy (green check mark)—component operating normally<br>● Warning (yellow triangle with exclamation point)—component has a noncritical error.<br>● Critical (red X)—component has a critical failure. |

Table 15. OMIVV host health

| Information | Description |
|---|---|
| | - Unknown (question mark)—status is unknown for the component. |

For example, if there are five healthy signs and one warning sign, the overall health is shown as warning.

ⓘ **NOTE:** Power monitoring information will not be available for hosts with cabled PSU or for modular servers.

# Viewing hardware details for a single host

You can view hardware details for a single host on the **OMIVV Host Information** tab. For information to appear on this page, run an inventory job. The hardware views directly report data from OMSA and iDRAC. See Running inventory jobs.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **Hosts**.
2. In the **Host** tab, select the specific host for which you want to view Hardware: `<Component Name>` details.
3. In the **Monitor** tab, select the **OMIVV Host Information** tab.

   ⓘ **NOTE:** If System Lockdown Mode is turned on for 14th generation host, a yellow band is displayed at the top with a closed lock icon .

   On the Hardware: `<Component Name>` tab, view the following information for each of the components.

Table 16. Hardware information for a single host (continued)

| Hardware: *Component* | Information |
|---|---|
| **Hardware: FRU** | ● **Part Name**—displays the FRU part name<br>● **Part Number**—displays the FRU part number<br>● **Manufacturer**—displays the manufacturer's name<br>● **Serial Number**—displays the manufacturer's serial number<br>● **Manufacture Date**—displays the manufacture date |
| **Hardware: Processor** | ● **Socket**—displays the slot number<br>● **Speed**—displays the current speed<br>● **Brand**—displays the processor brand<br>● **Version**—displays the processor version<br>● **Cores**—displays the number of cores in this processor |
| **Hardware: Power Supply** | ● **Type**—displays the type of power supply. The power supply types include:<br>○ UNKNOWN<br>○ LINEAR<br>○ SWITCHING<br>○ BATTERY<br>○ UPS<br>○ CONVERTER<br>○ REGULATOR<br>○ AC<br>○ DC<br>○ VRM<br>● **Location**—displays the location of the power supply, such as slot 1<br>● **Output (Watts)**—displays the power in watts |
| **Hardware: Memory** | ● **Memory Slots**—displays the Used, Total, and Available memory count<br>● **Memory Capacity**—displays the Installed Memory, Total Memory Capacity, and Available Memory<br>● **Slot**—displays the DIMM slot |

**Table 16. Hardware information for a single host**

| Hardware: *Component* | Information |
|---|---|
| | ● **Size**—displays the memory size<br>● **Type**—displays the memory type |
| **Hardware: NICs** | ● **Total**—displays the total count of available network interface cards<br>● **Name**—displays the NIC name<br>● **Manufacturer**—displays only the manufacturer name<br>● **MAC Address**—displays the NIC MAC address |
| **Hardware: PCI Slots** | ● **PCI Slots**—displays the Used, Total, and Available PCI slots<br>● **Slot**—displays the slot<br>● **Manufacturer**—displays the manufacturer name of the PCI slot<br>● **Description**—displays the description of the PCI device<br>● **Type**—displays the PCI slot type<br>● **Width**—displays the data bus width, if available |
| **Hardware: Remote Access Card** | ● **IP Address**—display the IP address for the remote access card<br>● **MAC Address**—displays the MAC address for the remote access card<br>● **RAC Type**—displays the type of the remote access card<br>● **URL**—displays the live URL for the iDRAC associated with this host |

# Viewing storage details for a single host

You can view storage details for a single host on the **OMIVV Host Information** tab. For information to be displayed on this page, run an inventory job. The hardware reports data directly from OMSA and iDRAC. See Running inventory jobs. The page displays different options depending on what is selected from the **View** drop-down list. If you select **Physical Disks**, another drop-down list is displayed. The next drop-down list is called Filter and enables you to filter the physical disk options. To view the storage details:

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **Hosts**.
2. In the **Objects** tab, select the specific host for which you want to view Storage: Physical Disk details.
3. In the **Monitor** tab, select the **OMIVV Host Information** tab.

   On the **Storage** subtab, view the following:

**Table 17. Storage details for a single host (continued)**

| *Component* | Information |
|---|---|
| **Storage** | Displays the count of virtual drives, controllers, enclosures, and associated physical disks with the global hot spare and dedicated hot spare counts. When you select from the View drop-down list, the selected option is selected. |
| **View** | Displays the options that you want to view for this host:<br>● Virtual drives<br>● Physical Disks<br>● Controllers<br>● Enclosures<br>ⓘ **NOTE:**<br>When the hosts are managed by using chassis profile:<br>In the left pane, if you click **Storage**, and then select the following from the **View** drop-down menu: |

Table 17. Storage details for a single host

| *Component* | Information |
|---|---|
| | - **Enclosures**—The Controller ID of the storage enclosure is displayed as 0 instead of the correct Controller ID.<br>- **Physical Disks**—The media type for HDD is displayed as **Magnetic Drive** instead of **Hard Disk Drive**. |

**NOTE:** For an MX chassis in an MCM configuration, the storage data may not be displayed for an MX host managed using the chassis profile and for a host present in the member chassis. In such cases, it is recommended to manage the host using iDRAC.

## Viewing storage details for the view option

The storage options on the **Host Storage** page depend on what you select from the **View** drop-down list.

Select either of the mentioned options from the View drop-down list and view the following:

Table 18. Storage details for a single host

| Information | Description |
|---|---|
| Virtual drives | - **Name**—displays the name of the virtual drive<br>- **Device FQDD**—displays the FQDD<br>- **Physical Disk**—displays on which physical disk the virtual drive is located<br>- **Capacity**—displays the capacity of the virtual drive<br>- **Layout**—displays the layout type of the virtual storage, which means the type of RAID that was configured for this virtual drive<br>- **Media Type**—displays either SSD or HDD<br>- **Controller ID**—displays the controller ID<br>- **Device ID**—displays the device ID<br>- **Stripe Size**—displays the stripe size, which is the amount of space that each stripe consumes on a single disk<br>- **Bus Protocol**—displays the technology that the physical disks in the virtual drive are using. The possible values are:<br>○ SCSI<br>○ SAS<br>○ SATA<br>- **Default Read Policy**—displays the default read policy that is supported by the controller. The options include:<br>○ Read-Ahead<br>○ No-Read-Ahead<br>○ Adaptive Read-Ahead<br>○ Read Cache Enabled<br>○ Read Cache Disabled<br>- **Default Write Policy**—displays the default write policy that is supported by the controller. The options include:<br>○ Write-Back<br>○ Force Write Back<br>○ Write Back Enabled<br>○ Write-Through<br>○ Write Cache Enabled Protected<br>○ Write Cache Disabled<br>- **Cache Policy**—displays if cache policy is enabled |

## Table 18. Storage details for a single host (continued)

| Information | Description |
|---|---|
| Physical Disks—When you select this option, the **Filter** drop-down list is displayed.<br>You can filter physical disks based on the following options:<br>● All Physical Disks<br>● Global Hot Spares<br>● Dedicated Hot Spares<br>● The last option displays custom named virtual drives | ● **Name**—displays the name of the physical disk<br>● **Device FQDD**—displays the device FQDD<br>● **Capacity**—displays the physical disk capacity<br>● **Disk Status**—displays physical disk status. The options include:<br>○ ONLINE<br>○ READY<br>○ DEGRADED<br>○ FAILED<br>○ OFFLINE<br>○ REBUILDING<br>○ INCOMPATIBLE<br>○ REMOVED<br>○ CLEARED<br>○ SMART ALERT DETECTED<br>○ UNKNOWN<br>○ FOREIGN<br>○ UNSUPPORTED<br>● **Configured**—displays whether the disk is configured<br>● **Hot Spare Type**(Not applicable for PCIe)—shows the hot spare type. The options include:<br>○ No—there is no hot spare<br>○ Global—an unused backup disk that is part of the disk group<br>○ Dedicated—an unused backup disk that is assigned to a single virtual drive. When a physical disk in the virtual drive crashes, the hot spare is enabled to replace the failed physical disk without interrupting the system or requiring your intervention.<br>● **Virtual Disk**—displays the name of the virtual drive<br>● **Bus Protocol**—displays the bus protocol<br>● **Controller ID**—displays the controller ID<br>● **Media Type**—displays either SSD or HDD.<br>● **Remaining Rated Write Endurance**—displays the SSD remaining write endurance.<br>● **Connector ID**—displays the connector ID<br>● **Enclosure ID**—displays the enclosure ID<br>● **Device ID**—displays the device ID<br>● **Model**—displays the model number of the physical storage disk<br>● **Part Number**—displays the storage part number<br>● **Serial Number**—displays the storage serial number<br>● **Vendor**—displays the storage vendor name |
| Controllers | ● **Controller ID**—displays the controller ID<br>● **Name**—displays the name of the controller<br>● **Device FQDD**—displays the FQDD of the device<br>● **Firmware Version**—displays the firmware version<br>● **Minimum Required Firmware**—displays the minimum required firmware. This column is populated if the firmware is out of date and a newer version is available<br>● **Driver Version**—displays the driver version<br>● **Patrol Read State**—displays the Patrol Read State<br>● **Cache Size**—displays the cache size |
| Enclosures | ● **Controller ID**—displays the controller ID<br>● **Connector ID**—displays the connector ID<br>● **Enclosure ID**—displays the enclosure ID<br>● **Name**—displays the name of the enclosure |

Table 18. Storage details for a single host

| Information | Description |
|---|---|
| | - **Device FQDD**—displays the device FQDD<br>- **Service Tag**—displays the service tag |

# About system event logs in web client

System event log (SEL) provides status information for hardware that is discovered by OMIVV and displays information based on the following criteria:

**Status** There are several status icons: Informational (blue exclamation point), Warning (yellow triangle with exclamation point), Error (red X), and Unknown (a box with a ?).

**Time (Server Time)** Indicates the time and date when the event occurred.

**Search this page** Displays the specific message, server names, configuration settings, and so on.

**Clear Log** Click this option to clear all SEL.

ⓘ **NOTE:** Clear SEL feature is not supported on the host managed using chassis.

The severity levels are defined as:

**Info** OMIVV operation completed successfully.

**Warning** OMIVV operation that is partially failed, and was partially successful.

**Error** OMIVV operation failed.

You can save the log as an external .CSV file. See Displaying system event logs for an individual host.

# Displaying event logs for a single host

To display the events, perform the following steps:

1. To access the **Monitor** tab, and open the **System Event Log** subtab, perform either of the following steps:

| Option | Description |
|---|---|
| From OMIVV | Perform the following steps in this option:<br>a. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **Hosts**.<br>b. In the **Objects** tab, double-click a specific host for which you want to view SEL log. |
| From the **Home** page | In the **Home** page, click **Hosts and Clusters**. |

2. In the **Monitor** tab, select **OMIVV Host Information** > **System Event Log**.
   The recent system log entries provide the 10 most recent system event log entries.
3. To update the **System Event Log**, perform a global refresh.
4. To limit (filter) the number of event log entries, choose one of the following options:
   - In the search filter text box, to dynamically filter the log entries, enter a text string.
   - To clear the filter text box, click **X** and all the event log entries are displayed.
5. To clear all event log entries, click **Clear Log**.

   A message is displayed stating that all log entries are deleted after they are cleared and you can select one of the following options:

   - To agree to clear log entries, click **Clear Log**.
   - To cancel, click **Cancel**.
6. To export the event log to a .CSV file, click 📄.
7. To browse to the location and save the system event log, click **Save**.

# Viewing additional hardware details for a single host

You can view the firmware, power monitoring, warranty status details for a single host on the **OMIVV Host Information** tab. For information to appear on this page, run an inventory job. The hardware views directly report the data from OMSA and iDRAC. See Running chassis inventory job now.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **Hosts**.
2. In the **Objects** tab, select the specific host for which you want to view `<Component Name>` details.
3. In the **Monitor** tab, select the **OMIVV Host Information** tab.

   On the Hardware: `<Component Name>` tab, view the following information for each of the components:

**Table 19. Single host information**

| *Component* | Information |
|---|---|
| **Firmware**<br>The host page lets you use the search, filter, and export a .CSV file of firmware information. | ● **Name**—displays the name of all the firmware on this host<br>● **Type**—displays the type of firmware<br>● **Version**—displays the version of all the firmware on this host<br>● **Installation Date**—displays the installation date<br>ⓘ **NOTE:** When the hosts are managed using the Chassis Profile, the firmware inventory data will show few extra components such as Life Cycle Controller and Software RAID. |
| **Power Monitoring**<br>ⓘ **NOTE:** The host time, as used here, means the local time where the host is located.<br>ⓘ **NOTE:** Power monitoring information will not be available for hosts with cabled PSU or for modular servers. | ● **General Information**—displays the Power Budget and Current Profile name<br>● **Threshold**—displays the Warning and Failure thresholds in watts<br>● **Reserve Power Capacity**—displays the Instant and Peak reserve power capacity in watts<br>**Energy Statistics**<br>● **Type**—displays the energy statistics type<br>● **Measurement Start Time (Host Time)**—displays the date and time when the host began to consume power.<br>● **Measurement Finish Time (Host Time)**—displays the date and time when the host stopped to consume power.<br>● **Reading**—displays the average value of readings over a one-minute time period<br>● **Peak Time (Host Time)**—displays the date and time of the host peak amps<br>● **Peak Reading**—displays the System Peak Power statistic, which is the peak power that is consumed by the system (in watts) |
| **Warranty**<br>ⓘ **NOTE:** To view a warranty status, ensure that you run a warranty job. See Running a warranty retrieval job. The **Warranty Status** page enables you to monitor the warranty expiration date. The warranty settings control when server warranty information is retrieved from Dell online by enabling or disabling the warranty schedule, and then setting the Minimum Days Threshold alert. | ● **Provider**—displays the name of the provider for the warranty<br>● **Description**—displays a description<br>● **Start Date**—displays the start date of the warranty<br>● **End Date**—displays the end date of the warranty<br>● **Days Left**—displays the days left on the warranty<br>● **Last Updated**—the last time the warranty was updated |

# Monitoring hosts on clusters and data centers

The OpenManage Integration for VMware vCenter enables you to view detailed information for all hosts included in a data center or cluster. You can sort the data by clicking the data grid row header. The data center and cluster pages enable you to export information to a CSV file and offers filter or search functionality on the data grid.

## Viewing overview of data centers and clusters

View the host details for data centers or clusters on the Dell EMC Datacenter/Cluster Information tab. For information to appear on this page, run an inventory job. The data you view may vary depending on which view you are accessing the data. The hardware views directly reports data from OMSA and iDRAC. See Running inventory jobs.

ⓘ **NOTE:** Data center and cluster pages enable you to export information to a .CSV file and offers filter or search functionality on the data grid.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. In the **Objects** tab, select the specific data center or cluster for which you want to view host details.
4. In the **Monitor** tab, select the **Dell EMC Datacenter/Cluster Information** > **Overview** tab, and view the details.

   ⓘ **NOTE:** To display the full list of details, select a specific host from the data grid.

**Table 20. Overview of data centers and clusters**

| Information | Description |
|---|---|
| **Datacenter/Cluster Information** | Displays the following:<br>● Datacenter/cluster name<br>● Number of Dell's managed hosts<br>● Total energy consumption |
| **System Lockdown Mode** | Displays the status of the iDRAC Lockdown Mode. The iDRAC Lockdown Mode status of the total number of hosts are displayed as follows:<br>● Turned On<br>● Turned Off<br>● Not Applicable (Only for 14th generation servers) |
| **Hardware Resources** | Displays the following:<br>● Total Processors<br>● Total Memory<br>● Virtual Disk Capacity |
| **Warranty Summary** | Displays the warranty status for the selected host. The status options include:<br>● Expired warranty<br>● Active warranty<br>● Unknown warranty |
| **Host** | Displays the host name |
| **Service Tag** | Displays the host service tag |
| **Model** | Displays the PowerEdge model |
| **Asset Tag** | Displays the asset tag, if configured |
| **Chassis Service Tag** | Displays the chassis service tag, if applicable |
| **OS Version** | Displays the ESXi OS version |
| **Location** | Blades only: Displays the slot location. For other, displays "Not Applicable" |

Table 20. Overview of data centers and clusters

| Information | Description |
|---|---|
| **System Lockdown Mode** | Only for 14th generation PowerEdge servers: Displays the iDRAC Lockdown Mode of the host, which is turned on, turned off, or unknown.<br>For all PowerEdge servers earlier than 14th generation, the System Lockdown Mode displayed is, not applicable. |
| **iDRAC IP** | Displays the iDRAC IP address |
| **Service Console IP** | Displays the service console IP |
| **CMC or Management Module URL** | Displays the CMC or Management Module URL, which is the Chassis URL for Blade servers, or else, it displays, “Not Applicable” |
| **CPUs** | Displays the number of CPUs |
| **Memory** | Displays the host memory |
| **Power State** | Displays, if the host has power |
| **Last Inventory** | Displays the day, date, and time of the last inventory job |
| **Connection Profile** | Displays the name of the connection profile |
| **Remote Access Card Version** | Displays the remote access card version |
| **BIOS Firmware Version** | Displays the BIOS firmware version |

# Viewing hardware details for data centers and clusters

You can view hardware details for a single host on the **Dell EMC Datacenter/Cluster Information** tab. For information to appear on this page, run an inventory job. The data center and cluster pages enable you to export information to a CSV file and offer filter or search functionality on the data grid. The data you view might vary depending on which view you are accessing the data. The hardware views directly report data from OMSA and iDRAC. See Running inventory jobs.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. In the **Objects** tab, select the specific data center or cluster for which you want to view the component-specific details.
4. In the **Monitor** tab, select the **Dell EMC Datacenter/Cluster Information** tab.

   On the Hardware: `<Component Name>` subtab, view the following information for each of the components.

Table 21. Hardware information for data centers and clusters (continued)

| Hardware: *Component* | Information |
|---|---|
| **Hardware: FRU** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Part Name**—displays the FRU part name<br>● **Part Number**—displays the FRU part number<br>● **Manufacturer**—displays the manufacturer’s name<br>● **Serial Number**—displays the manufacturer’s serial number<br>● **Manufacture Date**—displays the manufacture date |
| **Hardware: Processor** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Socket**—displays the slot number<br>● **Speed**—displays the current speed<br>● **Brand**—displays the processor brand<br>● **Version**—displays the processor version |

Table 21. Hardware information for data centers and clusters (continued)

| Hardware: *Component* | Information |
|---|---|
| | ● **Cores**—displays the number of cores in this processor |
| **Hardware: Power Supply** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Type**—displays the type of power supply. The power supply types include:<br>○ UNKNOWN<br>○ LINEAR<br>○ SWITCHING<br>○ BATTERY<br>○ UPS<br>○ CONVERTER<br>○ REGULATOR<br>○ AC<br>○ DC<br>○ VRM<br>● **Location**—displays the location of the power supply, such as slot 1<br>● **Output (Watts)**—displays the power in watts<br>● **Status**—displays the status of the power supply. The status options include:<br>○ OTHER<br>○ UNKNOWN<br>○ OK<br>○ CRITICAL<br>○ NOT CRITICAL<br>○ RECOVERABLE<br>○ NOT RECOVERABLE<br>○ HIGH<br>○ LOW |
| **Hardware: Memory** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Slot**—displays the DIMM slot<br>● **Size**—displays the memory size<br>● **Type**—displays the memory type |
| **Hardware: NICs** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Name**—displays the NIC name<br>● **Manufacturer**—displays only the manufacturer name<br>● **MAC Address**—displays the NIC MAC address |
| **Hardware: PCI Slots** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Slot**—displays the slot<br>● **Manufacturer**—displays the manufacturer name of the PCI slot<br>● **Description**—displays the description of the PCI device<br>● **Type**—displays the PCI slot type<br>● **Width**—displays the data bus width, if available |
| **Hardware: Remote Access Card** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **IP Address**—display the IP address for the remote access card |

Table 21. Hardware information for data centers and clusters

| Hardware: *Component* | Information |
|---|---|
| | ● **MAC Address**—displays the MAC address for the remote access card<br>● **RAC Type**—displays the type of the remote access card<br>● **URL**—displays the live URL for the iDRAC associated with this host |

## Viewing storage details for data center and clusters

You can view the physical storage details for a data center or cluster on the **Datacenter/Cluster Information** tab. For information to appear on this page, run an inventory job. The data center and cluster pages enable you to export information to a CSV file and offers filter/search functionality on the data grid. The hardware views directly report data from OMSA and iDRAC. See Running inventory jobs.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. In the **Objects** tab, select the specific data center or cluster.
4. In the **Monitor** tab, select the **Dell EMC Datacenter/Cluster Information** tab and navigate to **Storage** > **Physical Disk/Virtual Disk**.

   To display the full list of details, select a specific host from the data grid.

Table 22. Storage details for a data center and cluster

| Storage: disks | Description |
|---|---|
| **Physical Disk** | ● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host<br>● **Capacity**—displays the physical disk capacity<br>● **Disk Status**—displays physical disk status. The options include:<br>○ ONLINE<br>○ READY<br>○ DEGRADED<br>○ FAILED<br>○ OFFLINE<br>○ REBUILDING<br>○ INCOMPATIBLE<br>○ REMOVED<br>○ CLEARED<br>○ SMART ALERT DETECTION<br>○ UNKNOWN<br>○ FOREIGN<br>○ UNSUPPORTED<br>ⓘ **NOTE:** For more information about the meaning of these alerts, see the Dell EMC OpenManage Server Administrator Storage Management User's Guide at `dell.com/support`<br>● **Model Number**—displays the model number of the physical storage disk<br>● **Last Inventory**—displays the day, month, and time of the last inventory that was run<br>● **Status**—displays the host status<br>● **Controller ID**—displays the controller ID<br>● **Connector ID**—displays the connector ID<br>● **Enclosure ID**—displays the enclosure ID<br>● **Device ID**—displays the device ID<br>● **Bus Protocol**—displays the bus protocol |

### Table 22. Storage details for a data center and cluster (continued)

| Storage: disks | Description |
|---|---|
| | ● **Remaining Rated Write Endurance**—displays the SSD remaining write endurance.<br>● **Hot Spare Type**(Not applicable for PCIe)—shows the hot spare type. The options include:<br>○ No—there is no hot spare<br>○ Global—unused backup disk that is part of the disk group<br>○ Dedicated—unused backup disk that is assigned to a single virtual disk. When a physical disk in the virtual disk fails, the hot spare is enabled to replace the failed physical disk without interrupting the system or requiring your intervention<br>● **Part Number**—displays the storage part number<br>● **Serial Number**—displays the storage serial number<br>● **Vendor Name**—displays the storage vendor name |
| **Virtual Disk** | ● **Host**—displays the name of the host<br>● **Service Tag**—displays the service tag of the host<br>● **Name**—displays the name of the virtual disk<br>● **Physical Disk**—displays on which physical disk the virtual disk is located<br>● **Capacity**—displays the capacity of the virtual disk<br>● **Layout**—displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual disk<br>● **Last Inventory**—displays the day, date and time the inventory was last run<br>● **Controller ID**—displays the controller ID<br>● **Device ID**—displays the device ID<br>● **Media Type**—displays either SSD or HDD<br>● **Bus Protocol**—displays the technology that the physical disks included in the virtual disk are using. The possible values are:<br>○ SCSI<br>○ SAS<br>○ SATA<br>○ PCIe<br>● **Stripe Size**—displays the stripe size, which provides the amount of space that each stripe consumes on a single disk<br>● Default Read Policy—displays the default read policy supported by the controller. The options include:<br>○ Read-Ahead<br>○ No-Read-Ahead<br>○ Adaptive Read-Ahead<br>○ Read Cache Enabled<br>○ Read Cache Disabled<br>● **Default Write Policy**—displays the default write policy supported by the controller. The options include:<br>○ Write-Back<br>○ Force Write Back<br>○ Write Back Enabled<br>○ Write-Through<br>○ Write Cache Enabled Protected<br>○ Write Cache Disabled<br>● **Disk Cache Policy**—displays the default cache policy supported by the controller. The options include:<br>○ Enabled—cache I/O<br>○ Disabled—direct I/O |

# Viewing additional hardware details for data center and clusters

You can view the firmware, power monitoring, warranty status details for a data center and cluster on the **Dell EMC Datacenter/Cluster Information** tab. For information to appear on this page, run an inventory job. The data center and cluster pages enable you to export information to a CSV file and offers filter/search functionality on the data grid. The hardware views directly report the data from OMSA and iDRAC. See Running an inventory job now.

1. In OpenManage Integration for VMware vCenter, in the Navigator pane, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. In the **Objects** tab, select the specific data center or cluster for which you want to view the host component details.
4. In the **Monitor** tab, select the **Dell EMC Datacenter/Cluster Information** tab.

   On the `<Component Name>` subtab, view the following information for each of the components:

**Table 23. Single host information (continued)**

| ***Component*** | **Information** |
|---|---|
| **Firmware** | ● **Host**—displays the name of the host<br>● **Service Tag**—displays the service tag of the host<br>● **Name**—displays the name of all the firmware on this host<br>● **Version**—displays the version of all the firmware on this host |
| **Power Monitoring**<br>ⓘ **NOTE:** To display the full list of details, select a specific host from the data grid. | ● **Host**—displays the name of the host<br>● **Service Tag**—displays the service tag of the host<br>● **Current Profile**—displays power profile to maximize your system's performance and conserve energy<br>● **Energy Consumption**—displays the energy consumption of the host<br>● **Peak Reserve Capacity**—displays the peak power reserve capacity<br>● **Power Budget**—displays the power cap for this host<br>● **Warning Threshold**—displays your system's configure maximum value for temperature probe warning threshold<br>● **Failure Threshold**—displays your system's configure maximum value for temperature probe failure threshold<br>● **Instant Reserve Capacity**—displays the host instantaneous headroom capacity<br>● **Energy Consumption Start Date**—displays the date and time when the host began to consume power<br>● **Energy Consumption End Date**—displays the date and time when the host stopped to consume power<br>● **System Peak Power**—displays the host peak power<br>● **System Peak Power Start Date**—displays the date and time when the host peak power started<br>● **System Peak Power End Date**—displays the date and time when the host peak power ended<br>● **System Peak Amps**—displays the hosts peak amps<br>● **System Peak Amps Start Date**—displays the starting date and time of the host peak amps<br>● **System Peak Amps End Date**—displays the end date and time of the host peak amps |
| **Warranty Summary**<br>ⓘ **NOTE:** To view a warranty status, ensure to run a warranty job. See Running a warranty retrieval job. The **Warranty Summary** page lets you monitor the warranty expiration date. The warranty settings control when server warranty information is retrieved from Dell online | ● **Warranty Summary**—the host warranty summary is displayed using icons to visually show the number of hosts in each status category<br>● **Host**—displays the host name<br>● **Service Tag**—displays the service tag of the host.<br>● **Description**—displays a description. |

Table 23. Single host information

| *Component* | Information |
|---|---|
| by enabling or disabling the warranty schedule, and then setting the Minimum Days Threshold alert. | - **Warranty Status**—displays the warranty status of the host. Status options include:<br>○ Active—the host is under warranty, and has not exceeded any threshold<br>○ Warning—the host is Active, but exceeded the warning threshold<br>○ Critical—same as warning, but for a critical threshold<br>○ Expired—the warranty has expired for this host<br>○ Unknown—OpenManage Integration for VMware vCenter does not get warranty status because the warranty job is not run, an error has occurred getting the data, or the system does not have a warranty<br>- **Days Left**—displays the number of days left for the warranty |

# Setting up physical server blink indicator light

To help in locating a physical server in a large data center environment, you can set the front indicator light to blink for a set time period.

1. In OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. In the **Object** tab, double-click the host you want.
3. In the **Summary** tab, scroll down to the Dell EMC Server Management portlet.
4. Under **Host Actions**, select **Blink Indicator Light**.
5. Choose one of the following:
   - To turn on the blink and set the time period, in the **Indicator Light** dialog box, click **Blink On**, and use the Timeout drop-down list to select the time-out increment, and then click **OK**.
   - To turn off the blink, in the **Indicator Light** dialog box, click **Blink Off**, and then click **OK**.

# Configuring System Lockdown Mode

The System Lockdown Mode setting is available in iDRAC for 14th generation of the PowerEdge servers. The setting when turned on locks the system configuration including firmware updates. This setting is intended to protect the system from unintentional changes. You can turn on or turn off the System Lockdown Mode for managed hosts using the OMIVV appliance or from the iDRAC console. From the OMIVV version 4.1 and later, you can configure and monitor the Lockdown Mode of iDRAC in servers. Also, iDRAC must have an enterprise license to enable Lockdown Mode.

**NOTE:** You cannot change the System Lockdown Mode for hosts that are managed by chassis profile.

You can configure the System Lockdown Mode by locking or unlocking a host or cluster at host or cluster level. When the System Lockdown Mode is turned on, the following functionality have limitations:

- All configuration tasks, such as firmware update, OS deployment, clear system event logs, reset iDRAC, and configuring iDRAC trap destination.

To configure System Lockdown Mode of a host or cluster at host or cluster level, perform the following steps:

1. To launch the Configure System Lockdown Mode wizard, perform either of the following substeps:
   a. In the **Navigator** pane, click **Hosts and Clusters**, select and right-click a host or cluster and click the **Actions** drop-down list, and then select **All OpenManage Integration Actions** > **Configure System Lockdown Mode**.
   b. In OpenManage Integration, click the **Hosts** or **Clusters** page, select and right-click a host or cluster or select a host or cluster and click the **Actions** drop-down list, and then select **All OpenManage Integration Actions** > **Configure System Lockdown Mode**.
   c. In the **Navigator** pane, select a host, and then click **Summary** > **OMIVV Host Information** > **Configure System Lockdown Mode**.
   d. In the **Navigator** pane, select a host or cluster, and then click **Monitor** > **OMIVV Host Information** > **Firmware** > **Configure System Lockdown Mode**.

2. To enable the System Lockdown Mode, select the **Turn On** option, or to disable the Lockdown Mode, select **Turn Off**.
3. Click **Apply**.

If you attempt to configure the System Lockdown Mode for 11th to 13th generation of PowerEdge servers, you are prompted with a message that this feature is not supported on this platform.

After the System Lockdown configuration is complete, you can view the updated status of Lockdown Mode in the **Job Queue** page. The job queue information for Lockdown Mode is valid only at a cluster level. To access the job queue page, in OpenManage Integration, select **Monitor** > **Job Queue** > **System Lockdown Mode Jobs**. See the iDRAC documentation for more information about System Lockdown mode.

10

# Events, alarms, and health monitoring

The goal of hardware management is to provide the system health status and up-to-date infrastructure information that an administrator needs to respond to critical hardware events without leaving the OMIVV plug-in or vCenter.

The data center and host system monitoring enables an administrator monitor infrastructure health by displaying hardware (server and storage) and virtualization-related events on the **Tasks** and **Events** tab in vCenter. Also, critical hardware alerts can trigger the OpenManage Integration for VMware vCenter alarms and few alarms defined for Dell virtualization-related events can move the managed host system to maintenance mode.

To receive events from servers, OMIVV is configured as a Trap destination on all monitored devices and the various destinations are as follows:

- SNMP Trap destination is set in iDRAC for 12th generation hosts and later.
- Trap destination is set in OMSA for hosts earlier than 12th generation.
- Trap destination is set in CMC or Management Module for chassis.

**NOTE:**

For an MX chassis in an MCM configuration, the trap destination is only configured on lead chassis. OMIVV will receive alerts from all lead and member chassis using the lead chassis.

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

To monitor, perform the following:

- Configure the **Event and Alarm** settings.
- Configure SNMP OMSA Trap destinations, if necessary.
- Use the **Tasks** and **Events** tab in vCenter to review event information.

### Topics:

- About events and alarms for hosts
- About events and alarms for chassis
- Virtualization-related events
- Proactive HA events
- Viewing alarms and events setting
- Viewing events
- Hardware component redundancy health—Proactive HA
- Launching management consoles

## About events and alarms for hosts

You can edit events and alarms from the OpenManage Integration for VMware vCenter within the **Manage** > **Settings** tab. From here, you can select the event posting level, enable alarms for the Dell EMC hosts, or restore default alarms. You can configure events and alarms for each vCenter or all at after for all registered vCenters.

The following are the four event posting levels:

**Table 24. Event posting level**

| Event | Description |
|---|---|
| Do not post any events | Do not allow the OpenManage Integration for VMware vCenter forward any events or alerts into related vCenters. |
| Post all events | Post all events, including informal events, that the OpenManage Integration for VMware vCenter receives from managed Dell EMC hosts into related vCenters. |

Table 24. Event posting level

| Event | Description |
|---|---|
| Post only critical and warning events | Posts only events with either a Critical or Warning criticality into related vCenters. |
| Post only virtualization-related critical, and warning events | Post virtualization-related events received from hosts into related vCenters. The virtualization-related events are events that Dell selects to be most critical to hosts that run virtual machines. |

When you configure the events and alarms, you can enable them. When enabled, the critical hardware alarms can trigger the OMIVV appliance to put the host system into a maintenance mode, and in certain cases, migrate the virtual machines to another host system. The OpenManage Integration for VMware vCenter forwards events received from managed the Dell EMC hosts, and creates alarms for those events. Use these alarms to trigger actions from vCenter, such as a reboot, maintenance mode, or migrate.

For example, when a dual power supply fails and an alarm is created, the resulting action puts the machine into maintenance mode, which results in workloads being migrated to a different host in the cluster.

All hosts outside of clusters, or in clusters without VMware Distributed Resource Scheduling (DRS) enabled, can see virtual machines being shut down due to a critical event. DRS continuously monitors usage across a resource pool and intelligently allocates available resources among virtual machines according to business needs. To ensure that virtual machines are automatically migrated on critical hardware events, use clusters with DRS configured Dell alarms. The details of the on-screen message list the clusters on this vCenter instance that might be impacted. Ensure that you confirm that the clusters are impacted before enabling events and alarms.

If you ever must restore the default alarm settings, you can do so with the **Reset Default Alarm** button. This button is a convenient option to restore the default alarm configuration without uninstalling and reinstalling the product. If any Dell EMC alarm configurations have been changed since installation, those changes are reverted using this button.

ⓘ **NOTE:** To receive the Dell events, ensure that you enable the events.

ⓘ **NOTE:** The OpenManage Integration for VMware vCenter preselects the virtualization-related events that are essential to hosts successfully running the virtual machines. By default, the Dell host alarms are disabled. If Dell alarms are enabled, the clusters should use DRS to ensure that the virtual machines that send critical events are automatically migrated.

# About events and alarms for chassis

The events and alarms corresponding to a chassis are shown only at the vCenter level. The events and alarms settings for hosts at every vCenter is also applicable at the chassis level. You can edit events and alarms settings from OpenManage Integration for VMware vCenter within the **Manage** > **Settings** tab. From here, you can select the event posting level, enable alarms for Dell EMC hosts and chassis, or restore default alarms. You can configure events and alarms for each vCenter or for all registered vCenters at once.

## Viewing chassis events

1. In the left pane, select vCenter, and click the vCenter servers.
2. Click a specific vCenter.
3. Click the **Monitor** > **Events** tab.
4. To view more event details, select a specific event.

    ⓘ **NOTE:** For an MX member chassis in an MCM configuration, the source of the event will be displayed as lead chassis, however, the message details will have the Service Tag of the member chassis for identification.

## Viewing chassis alarms

1. In the left pane, select vCenter, and click the vCenter servers.
2. Click a specific vCenter.
   The alarms are displayed. Only the first four alarms are displayed.

3. To view the complete list, click **Show All** to view the detailed list in the **Monitor** tab as **All Issues**.
4. In **Triggered Alarms**, click **Alarm** to view the alarm definition.

# Virtualization-related events

The following table contains the virtualization-related critical and warning events, and includes event name, description, severity level, and recommended action.

The vitalization-related events are displayed in the following format:

Dell-Message ID:<*ID number*>, Message:<*Message Description*>.

The chassis events are displayed in the following format:

Dell-Message:<*Message description*>, Chassis name:<*name of the chassis*>, Chassis Service Tag:<*chassis Service Tag* >, Chassis Location:<*chassis location*>

### Table 25. Virtualization events

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| Dell-Current sensor detected a warning value | A current sensor in the specified system exceeded its warning threshold | Warning | No action |
| Dell-Current sensor detected a failure value | A current sensor in the specified system exceeded its failure threshold | Error | Put the system into maintenance mode |
| Dell-Current sensor detected a non-recoverable value | A current sensor in the specified system detected an error from which it cannot recover | Error | No action |
| Dell-Redundancy regained | Sensor Returned to Normal Value | Info | No action |
| Dell-Redundancy degraded | A redundancy sensor in the specified system detected that one of the components of the redundancy unit has failed but the unit is still redundant | Warning | No action |
| Dell-Redundancy lost | A redundancy sensor in the specified system detected that one of the components in the redundant unit has been disconnected, has failed, or is not present | Error | Put the system into maintenance mode |
| Dell-Power supply returned to normal | Sensor returned to Normal Value | Info | No action |
| Dell-Power supply detected a warning | A power supply sensor reading in the specified system exceeded a user definable warning threshold | Warning | No action |
| Dell-Power supply detected a failure | A power supply has been disconnected or has failed | Error | Put the system into maintenance mode |
| Dell-Power supply sensor detected a non-recoverable value | A power supply sensor in the specified system detected an error from which it cannot recover | Error | No action |

Table 25. Virtualization events (continued)

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| Dell-Memory Device Status warning | A memory device correction rate exceeded an acceptable value | Warning | No action |
| Dell-Memory Device error | A memory device correction rate exceeded an acceptable value, a memory spare bank was activated, or a multibit ECC error occurred | Error | Put the system into maintenance mode |
| Dell-Fan enclosure inserted into system | Sensor returned to normal value | Info | No action |
| Dell-Fan enclosure removed from system | A fan enclosure has been removed from the specified system | Warning | No action |
| Dell-Fan enclosure removed from system for an extended amount of time | A fan enclosure has been removed from the specified system for a user-definable length of time | Error | No action |
| Dell-Fan enclosure sensor detected a non-recoverable value | A fan enclosure sensor in the specified system detected an error from which it cannot recover | Error | No action |
| Dell-AC power has been restored | Sensor Returned to Normal Value | Info | No action |
| Dell-AC power has been lost warning | An AC power cord has lost its power, but there is sufficient redundancy to classify this as a warning | Warning | No action |
| Dell-An AC power cord has lost its power | An AC power cord has lost its power, and lack of redundancy requires this to be classified as an error | Error | No action |
| Dell-Processor sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Processor sensor detected a warning value | A processor sensor in the specified system is in a throttled state | Warning | No action |
| Dell-Processor sensor detected a failure value | A processor sensor in the specified system is disabled, has a configuration error, or experienced a thermal trip | Error | No action |
| Dell-Processor sensor detected a non-recoverable value | A processor sensor in the specified system has failed. | Error | No action |
| Dell-Device configuration error | A configuration error was detected for a pluggable device in the specified system | Error | No action |
| Dell-Battery sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Battery sensor detected a warning value | A battery sensor in the specified system detected | Warning | No action |

Table 25. Virtualization events (continued)

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| | that a battery is in a predictive failure state | | |
| Dell-Battery sensor detected a failure value | A battery sensor in the specified system detected that a battery has failed | Error | No action |
| Dell-Battery sensor detected a nonrecoverable value | A battery sensor in the specified system detected that a battery has failed | Error | No Action |
| Dell-Thermal shutdown protection has been initiated | This message is generated when a system is configured for thermal shutdown due to an error event. If a temperature sensor reading exceeds the error threshold for which the system is configured, the operating system shuts down and the system powers off. This event may also be initiated on certain systems when a fan enclosure is removed from the system for an extended period of time | Error | No action |
| Dell-Temperature sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Temperature sensor detected a warning value | A temperature sensor on the backplane board, system board, CPU, or drive carrier in the specified system exceeded its warning threshold | Warning | No action |
| Dell-Temperature sensor detected a failure value | A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its failure threshold value | Error | Put the system into maintenance mode |
| Dell-Temperature sensor detected a non-recoverable value | A temperature sensor on the backplane board, system board, or drive carrier in the specified system detected an error from which it cannot recover | Error | No action |
| Dell-Fan sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Fan sensor detected a warning value | Fan Sensor reading in the host <x> exceeded a warning threshold value | Warning | No Action |
| Dell-Fan sensor detected a failure value | A fan sensor in the specified system detected the failure of one or more fans | Error | Put the system into maintenance mode |
| Dell-Fan sensor detected a nonrecoverable value | A fan sensor detected an error from which it cannot recover | Error | No action |

## Table 25. Virtualization events (continued)

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| Dell-Voltage sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Voltage sensor detected a warning value | A voltage sensor in the specified system exceeded its warning threshold | Warning | No action |
| Dell-Voltage sensor detected a failure value | A voltage sensor in the specified system exceeded its failure threshold | Error | Put the system into maintenance mode |
| Dell-Voltage sensor detected a nonrecoverable value | A voltage sensor in the specified system detected an error from which it cannot recover | Error | No action |
| Dell-Current sensor returned to a normal value | Sensor Returned to Normal Value | Info | No action |
| Dell-Storage: storage management error | Storage management has detected a device independent error condition | Error | Put the system into maintenance mode |
| Dell-Storage: Controller warning | A portion of the physical disk is damaged | Warning | No action |
| Dell-Storage: Controller failure | A portion of the physical disk is damaged | Error | Put the system into maintenance mode |
| Dell-Storage: Channel Failure | Channel failure | Error | Put the system into maintenance mode |
| Dell-Storage: Enclosure hardware information | Enclosure hardware information | Info | No action |
| Dell-Storage: Enclosure hardware warning | Enclosure hardware warning | Warning | No action |
| Dell-Storage: Enclosure hardware failure | Enclosure hardware error | Error | Put the system into maintenance mode |
| Dell-Storage: Array disk failure | Array disk failure | Error | Put the system into maintenance mode |
| Dell-Storage: EMM failure | EMM failure | Error | Put the system into maintenance mode |
| Dell-Storage: power supply failure | Power supply failure | Error | Put the system into maintenance mode |
| Dell-Storage: temperature probe warning | Physical disk temperature probe warning, too cold or too hot | Warning | No action |
| Dell-Storage: temperature probe failure | Physical disk temperature probe error, too cold or too hot. | Error | Put the system into maintenance mode |
| Dell-Storage: Fan failure | Fan failure | Error | Put the system into maintenance mode |
| Dell-Storage: Battery warning | Battery warning | Warning | No action |
| Dell-Storage: Virtual disk degraded warning | Virtual disk degraded warning | Warning | No action |
| Dell-Storage: Virtual disk degraded failure | Virtual disk degraded failure | Error | Put the system into maintenance mode |

Table 25. Virtualization events (continued)

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| Dell-Storage: Temperature probe information | Temperature probe information | Info | No action |
| Dell-Storage: Array disk warning | Array disk warning | Warning | No action |
| Dell-Storage: Array disk information | Array disk information | Info | No action |
| Dell-Storage: Power supply warning | Power supply warning | Warning | No action |
| Dell-Fluid Cache Disk failure | Fluid cache disk failure | Error | Put the system into maintenance mode |
| Dell-Cable failure or critical event | Cable failure or critical event | Error | Put the system into maintenance mode |
| Dell-Chassis Management Controller detected a warning | Chassis Management Controller detected a warning | Warning | No action |
| Dell-Chassis Management Controller detected an error | Chassis Management Controller detected an error | Error | Put the system into maintenance mode |
| Dell-IO Virtualization failure or critical event | IO virtualization failure or critical event | Error | Put the system into maintenance mode |
| Dell-Link status warning | Link status warning | Warning | No action |
| Dell-Link status failure or critical event | Link status failure or critical event | Error | Put the system into maintenance mode |
| Dell-Security warning | Security warning | Warning | No action |
| Dell-System: Software configuration warning | System: Software configuration warning | Warning | No action |
| Dell-System: Software configuration failure | System: Software configuration failure | Error | Put the system into maintenance mode |
| Dell-Storage Security warning | Storage security warning | Warning | No action |
| Dell-Storage Security failure or critical event | Storage security failure or critical event | Error | Put the system into maintenance mode |
| Dell-Software change update warning | Software change update warning | Warning | No action |
| Dell-Chassis Management Controller audit warning | Chassis Management Controller audit warning | Warning | No action |
| Dell-Chassis Management Controller audit failure or critical event | Chassis Management Controller audit failure or critical event | Error | Put the system into maintenance mode |
| Dell-PCI device audit warning | PCI device audit warning | Warning | No action |
| Dell Power Supply audit warning | Power supply audit warning | Warning | No action |
| Dell-Power Supply audit failure or critical event | Power supply audit failure or critical event | Error | Put the system into maintenance mode |
| Dell-Power usage audit warning | Power usage audit warning | Warning | No action |
| Dell-Power usage audit failure or critical event | Power usage audit failure or critical event | Error | Put the system into maintenance mode |

Table 25. Virtualization events (continued)

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| Dell-Security configuration warning | Security configuration warning | Warning | No action |
| Dell-Configuration: Software configuration warning | Configuration: Software configuration warning | Warning | No action |
| Dell-Configuration: Software configuration failure | Configuration: Software configuration failure | Error | Put the system into maintenance mode |
| Dell-Virtual Disk Partition failure | Virtual disk partition failure | Error | Put the system into maintenance mode |
| Dell-Virtual Disk Partition warning | Virtual disk partition warning | Warning | No action |
| **iDRAC events**<br>**NOTE:** For all Proactive HA enabled hosts that are part of a cluster, the following virtualization events are mapped to the Proactive HA events; except events, "The fans are not redundant" and "The power supplies are not redundant" are not mapped. | | | |
| The fans are redundant | None | Info | No action |
| Fan redundancy is lost | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Critical | Remove and reinstall failed fans or install additional fans |
| Fan redundancy is degraded | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans. | Warning | Remove and reinstall failed fans or install additional fans |
| The fans are not redundant | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Info | Remove and reinstall failed fans or install additional fans |
| The fans are not redundant. Insufficient resources to maintain normal operations | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Critical | Remove and reinstall failed fans or install additional fans |
| The power supplies are redundant | None | Info | No action |
| Power supply redundancy is lost | The current power operational mode is non-redundant because of a power supply exception, a power supply inventory change, or a system power inventory change. The system was previously operating in a power redundant mode | Critical | Check the event log for power supply failures. Review system configuration and power consumption |
| Power supply redundancy is degraded | The current power operational mode is non-redundant because of a power supply exception, a power supply inventory change, or a system power | Warning | Check the event log for power supply failures. Review system configuration and power consumption |

**Table 25. Virtualization events (continued)**

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| | inventory change. The system was previously operating in a power redundant mode | | |
| The power supplies are not redundant | The current power supply configuration does not meet the platform requirements to enable redundancy. If a power supply fails the system may shut down. | Info | If unintended, review system configuration and power consumption and install power supplies accordingly. Check power supply status for failures |
| The power supplies are not redundant. Insufficient resources to maintain normal operations | The system may power down or operate in a performance degraded state | Critical | Check the event log for power supply failures. Review system configuration and power consumption and upgrade or install power supplies accordingly |
| Internal Dual SD Module is redundant | None | Info | No action |
| Internal Dual SD Module redundancy is lost | Either one of the SD card or both the SD cards are not functioning properly | Critical | Replace the failed SD card |
| Internal Dual SD Module redundancy is degraded | Either one of the SD card or both the SD cards are not functioning properly | Warning | Replace the failed SD card |
| Internal Dual SD Module is not redundant | None | Info | Install additional SD card and configure for redundancy if redundancy is desired |
| **Chassis events** | | | |
| Power supply redundancy is lost | The current power operational mode is non-redundant because of a power supply exception, a power supply inventory change, or a system power inventory change. The system was previously operating in a power redundant mode | Critical | Check the event log for power supply failures. Review system configuration and power consumption |
| Power supply redundancy is degraded | The current power operational mode is non-redundant because of a power supply exception, a power supply inventory change, or a system power inventory change. The system was previously operating in a power redundant mode | Warning | Check the event log for power supply failures. Review system configuration and power consumption |
| The power supplies are redundant | None | Info | No action |
| The power supplies are not redundant | The current power supply configuration does not meet the platform requirements to enable redundancy. If a power supply fails the system may shut down. | Info | If unintended, review system configuration and power consumption and install power supplies accordingly. Check power supply status for failures |

**Table 25. Virtualization events**

| Event name | Description | Severity | Recommended action |
|---|---|---|---|
| The power supplies are not redundant. Insufficient resources to maintain normal operations | The system may power down or operate in a performance degraded state | Critical | Check the event log for power supply failures. Review system configuration and power consumption and upgrade or install power supplies accordingly |
| Fan redundancy is lost | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Critical | Remove and reinstall failed fans or install additional fans |
| Fan redundancy is degraded | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans. | Warning | Remove and reinstall failed fans or install additional fans |
| The fans are redundant | None | Info | No action |
| The fans are not redundant | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Info | Remove and reinstall failed fans or install additional fans |
| The fans are not redundant. Insufficient resources to maintain normal operations | One of more fans have failed or have been removed or a configuration change occurred, which requires additional fans | Critical | Remove and reinstall failed fans or install additional fans |

# Proactive HA events

Based on the components supported by VMware for Proactive HA, the following events are registered by the Dell Inc provider during its registration with vCenter:

**NOTE:** The Proactive HA health status of the supported components can be normal (green), or warning (yellow), or critical (red), or unknown (gray) state.

**Table 26. Dell Proactive HA events**

| Dell Inc provider event | Component type | Description |
|---|---|---|
| DellFanRedundancy | Fan | Fan redundancy event |
| DellPowerRedundancy | Power supply (PSU) | Power redundancy event |
| DellIDSDMRedundancy | Storage | IDSDM redundancy event<br>**NOTE:** When the hosts are managed using chassis are added to PHA enabled cluster and if IDSDM components are present, ensure that Internal SD Card Redundancy is configured in the iDRAC settings as "Mirror". |

For a Proactive HA enabled host, the following Traps are used by OMIVV as a trigger to determine the redundant health of components: Based on the redundant health information, a Proactive HA health update might be sent to the vCenter for that host. These Traps are not forwarded directly to a vCenter for a Proactive HA host.

Table 27. Proactive HA events

| Event name | Description | Severity |
|---|---|---|
| Fan Information | Fan information | Info |
| Fan Warning | Fan warning | Warning |
| Fan Failure | Fan failure | Critical |
| Power Supply Normal | The power supply returns to normal | Info |
| Power Supply Warning | The power supply detects a warning | Warning |
| Power Supply Failure | The power supply detects a failure | Critical |
| Power Supply Absent | The power supply is absent | Critical |
| Redundancy Information | Redundancy information | Info |
| Redundancy Degraded | Redundancy is degraded | Warning |
| Redundancy Lost | Redundancy is lost | Critical |
| Integrated Dual SD Module Information | Integrated Dual SD Module (IDSDM) information | Info |
| Integrated Dual SD Module Warning | Integrated Dual SD Module warning | Warning |
| Integrated Dual SD Module Failure | Integrated Dual SD Module failure | Critical |
| Integrated Dual SD Module Absent | Integrated Dual SD Module is absent | Critical |
| Integrated Dual SD Module Redundancy Information | Integrated Dual SD Module redundancy information | Info |
| Integrated Dual SD Module Redundancy Degraded | Integrated Dual SD Module redundancy is degraded | Warning |
| Integrated Dual SD Module Redundancy Lost | Integrated Dual SD Module redundancy is lost | Critical |
| **Chassis events** | | |
| Fan Information | Fan information | Info |
| Fan Warning | Fan warning | Warning |
| Fan Failure | Fan failure | Critical |
| Power Supply Normal | The power supply returns to normal | Info |
| Power Supply Warning | The power supply detects a warning | Warning |
| Power Supply Failure | The power supply detects a failure | Critical |
| Redundancy Information | Redundancy information | Info |
| Redundancy Degraded | Redundancy is degraded | Warning |
| Redundancy Lost | Redundancy is lost | Critical |

# Viewing alarms and events setting

Once you configure alarms and events, you can view if the vCenter alarms for hosts are enabled and which event posting level is selected on the settings tab.

1. In OpenManage Integration for VMware vCenter, in the **Manage** > **Settings** tab, under **vCenter Settings**, expand **Events and Alarms**.

   The following details are displayed:

   - vCenter alarms for Dell EMC hosts — Displays either **Enabled** or **Disabled**.
   - Event posting level

2. Configure events and alarms. See Configuring events and alarms.

To view the event posting levels, see About events and alarms.

# Viewing events

Ensure that you configure events before you can view them in the **Events** tab. See Configuring events and alarms.

View the events for a host, cluster, or data center in the events tab.

1. In the OpenManage Integration for VMware vCenter Navigator, click **Hosts**, **Datacenter** or **Clusters**.
2. In the **Objects** tab, select a specific host, data center, or cluster for which you want to view events.
3. In the **Monitor** tab, click **Events**.
4. To view the event details, select a specific event.

# Hardware component redundancy health—Proactive HA

ⓘ **NOTE:** The configured Proactive HA policies on the Proactive HA cluster might be affected when global alerts are configured through OMIVV.

ⓘ **NOTE:** Proactive HA is available only on the platforms that support redundancy on power, fan, and IDSDM.

ⓘ **NOTE:** Proactive HA feature is not supported for PSUs for which redundancy cannot be configured (for example, cabled PSUs).

Proactive HA is a vCenter (vCenter 6.5 and later) feature that works with OMIVV. When you enable Proactive HA, the feature safeguards your workloads by proactively taking measures based on degradation of redundancy health of supported components in a host.

ⓘ **NOTE:** All hosts from the PowerEdge 12th generation and later, and the ESXi versions v6.0 and later that are part of a connection profile and successfully inventoried are eligible for Proactive HA.

After assessing the redundancy health status of the supported host components, the OMIVV appliance updates the health status change to the vCenter server. The available states of redundancy health status for the supported components (power supply, fans, and IDSDM) are:

- Healthy (Information)—component operating normally.
- Warning (Moderately degraded)—component has a noncritical error.
- Critical (Severely degraded)—component has a critical failure.

ⓘ **NOTE:** The moderately degraded and severely degraded states are represented as *Warning* in the **Type** column on the **Events** page.

ⓘ **NOTE:** An *Unknown* health status denotes the unavailability of any Proactive HA health update from the Dell Inc provider. An unknown health status might occur when:

- All hosts that are added to a Proactive HA cluster may remain in the unknown state for a few minutes until OMIVV initializes them with their appropriate states.
- A vCenter server restart may put the hosts in a Proactive HA cluster into an unknown state until OMIVV initializes them with their appropriate states again.

When OMIVV detects a change in the redundancy health status of supported components (either through Traps or polling), the health update notification for the component is sent to the vCenter server. Polling runs every hour, and it is available as a fail-safe mechanism to cover the possibility of a Trap loss.

# Configuring Proactive HA for Rack and Tower servers

To configure for the Rack and Tower servers, perform the following steps:

Ensure that all hosts are properly configured for redundancy of all the three supported redundant components (power supply, fans, and IDSDM).

1. Create a connection profile and associate hosts with connection profile. See Creating a connection profile.
2. Verify that hosts inventory is completed successfully. See Viewing hosts inventory.
3. Verify that the SNMP Trap destination in iDRAC is set as the OMIVV appliance IP address.

   **NOTE:** Ensure that from the **OpenManage Integration** > **Monitor** > **Log** tab, the user action log confirms the availability of a host for a Proactive HA cluster.
4. Enable Proactive HA on a cluster. See Enabling Proactive HA on a cluster.

## Configuring Proactive HA for Modular servers

To configure for the Modular servers, perform the following steps:

Before configuring Proactive HA for the Modular servers, ensure that the following conditions are met:

- All hosts are properly configured for redundancy of all the three supported redundant components (power supply, fans, and IDSDM).
- Hosts and chassis inventory is completed successfully.

**NOTE:** It is recommended that all the modular hosts in a Proactive HA cluster should not be in the same chassis, as chassis failure affects all its blades.

1. Create a connection profile and associate hosts with connection profile. See Creating a connection profile.
2. Verify that hosts inventory is completed successfully. See Viewing hosts inventory.

   **NOTE:** Ensure that from the **OpenManage Integration** > **Monitor** > **Log** tab, the user action log confirms the availability of a host for a Proactive HA cluster.
3. Create a chassis profile for associated chassis. See Creating a chassis profile.
4. Verify that chassis inventory is completed successfully. See Viewing chassis inventory.
5. Launch CMC or Management Module and verify that the Trap destination for chassis is set as the OMIVV appliance IP address.
6. In **Chassis Management Controller**, go to **Setup** > **General**.
7. In the **General Chassis Settings** page, select **Enable Enhanced Chassis Logging and Events**.
8. Enable Proactive HA on a cluster. See Enabling Proactive HA on a cluster.

# Enabling Proactive HA on clusters

Before enabling Proactive HA on clusters, ensure that the following conditions are met:

- A cluster with DRS enabled is created and configured in the vCenter console. To enable DRS on a cluster, see the VMware Documentation.
- All hosts that are part of the cluster should be part of a connection profile and successfully inventoried, and the chassis should have a chassis profile when applicable.

1. In OpenManage Integration, click **Clusters**.
2. Under **Clusters**, click a cluster, select **Configure** > **vSphere Availability**, and then click **Edit**.
   The **Edit Cluster Settings** wizard is displayed.
3. Click **vSphere DRS** and select **Turn on vSphere DRS**, if not selected.
4. Click **vSphere Availability** and select **Turn on Proactive HA**, if not selected.
5. In the left pane, under **vSphere Availability**, click **Proactive HA Failures and Responses**.
   The **Proactive HA Failures and Responses** screen is displayed.
6. In the **Proactive HA Failure and Responses** screen, expand the **Automation Level**.
7. For the **Automation Level**, select **Manual** or **Automated**.
8. For the **Remediation**, select quarantine mode, maintenance mode, or a combination of both quarantine and maintenance mode based on severity status (Mixed mode). See the VMware Documentation for more information.
9. For the **Proactive HA provider**, use the check box to select the Dell provider for the cluster.

10. Click **edit** against the selected Dell provider.
    The **Edit Blocked Failure Conditions** dialog box for the Proactive HA provider is displayed.
11. To block a failure condition from posting events, use the check boxes to select events (generated through Traps or polling) from the **failure conditions** table.

    You can filter the content of the failure conditions data grid by using the **Filter** field, or drag and drop columns within the failure conditions data grid. The failure conditions can be applied at a cluster level or host level.
12. To apply on all current and future hosts in the cluster, select the **Cluster-level** check box.
13. To apply the changes, in the **Edit Blocked Failure Conditions**, click **OK**, or to cancel, click **Cancel**.
14. To save the changes, in the **Edit Cluster Settings** wizard, click **OK**, or to cancel, click **Cancel**.

After Proactive HA is enabled on a cluster, OMIVV scans through all hosts within the cluster and initializes the Proactive HA health status of all supported host server components. OMIVV can now send the health update notification of supported components to the vCenter server. Based on the health update notification from OMIVV, the vCenter server takes a manual or automatic action that you have selected for **Remediation**.

To override the existing severity, see Overriding severity of health update notification on page 91.

## Overriding severity of health update notification

You can configure to override the existing severity of the Dell Proactive HA events for the Dell EMC host and its components with customized severity, which is aligned to your environment.

The following are the severity levels that apply to each of the Proactive HA events:

- **Info**
- **Moderately Degraded**
- **Severely Degraded**

**NOTE:** You cannot customize the severity of the Proactive HA components with the **Info** severity level.

1. In OpenManage Integration for VMware vCenter, from the **Manage** tab, click **Proactive HA Configuration** > **Proactive HA Events**.
2. Click to view information about the list of supported events.
   The data grid displays all the supported Proactive HA events and includes columns; events id, event description, component type, default severity, and override severity column for customizing the severity of the host and its components.
3. To change severity of a host or its component, in the **Override Severity** column, select the desired status from the drop-down list.
   This policy applies to all the Proactive HA hosts across all vCenter servers that are registered with OMIVV.
4. Repeat step 3 for all the events that must be customized.
5. Perform any one of the following actions:
   a. To save the customization, click **Apply Changes**.
   b. To revert the overridden severity after selecting a severity level, click **Cancel**.
   c. To apply the default severity to the overridden severity, click **Reset To Default**.

# Launching management consoles

There are three management consoles that you can start from the Dell EMC Server Management portlet. They include:

- To access the iDRAC user interface, start the Remote Access Console. See Launching the Remote Access console (iDRAC).
- To access the OpenManage Server Administrator user interface, start the OMSA console. Before starting OMSA console, OMSA URL should be configured in the Open Management Integration for VMware vCenter. See Launching the OMSA console.
- To access the chassis user interface, click the Blade chassis console. See Launching the Chassis Management Controller or Management Module console.

  **NOTE:** If you are on a Blade system, start the CMC console to launch the Chassis Management Controller user interface. If you are not on a Blade system, the Chassis Management Controller user interface is not displayed.

# Launching Remote Access console

You can start the iDRAC user interface from the Dell EMC Server Management portlet.

1. In OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. On the **Object** tab, double-click the host you want.
3. On the **Summary** tab, scroll down to the Dell EMC Server Management portlet.
4. Click **Management Consoles** > **Remote Access Console (iDRAC)**.

# Launching OMSA console

Before you can start the OMSA console, ensure that you set up the OMSA URL and install and configure the OMSA web server. You can set up the OMSA URL from the **Settings** tab.

**NOTE:** Install OMSA to monitor and manage PowerEdge 11th generation servers by using OpenManage Integration for VMware vCenter.

1. In OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. In the **Object** tab, double-click the host you want.
3. In the **Summary** tab, scroll down to the **OMIVV Host Information**.
4. In the **OMIVV Host Information** section, click **OMSA Console**.

# Launching the Chassis Management Controller or Management Module console

You can start the chassis user interface from the Dell EMC Server Management portlet.

1. In OpenManage Integration for VMware vCenter, in the Navigator area, under Inventory Lists, click **Hosts**.
2. In the **Object** tab, double-click the blade server you want.
3. In the **Summary** tab, scroll down to the Dell EMC Server Management portlet.
4. Click **Management Consoles** > **Chassis Management Controller Console (CMC) or Management Module**.

# 11

# About firmware updates

The OMIVV appliance enables you to perform BIOS and firmware update jobs on the managed hosts. You can perform concurrent firmware update jobs across multiple clusters or nonclustered hosts. Running concurrent firmware update on two hosts of the same cluster is not allowed.

The following are the two methods by which you can perform firmware update:

- Single DUP—performs firmware update for iDRAC, BIOS, or LC by pointing directly to the DUP location (either CIFS or NFS share). The single DUP method can be used only at the host level.•

  Repository—performs BIOS and all supported firmware updates. The method can be used at both the non-vSAN host level and cluster level. The following are the two locations of repository:

  - Dell Default Online—the firmware updates default repository is set to Dell Online (`https://downloads.dell.com`). The OMIVV downloads selected firmware updates from the Dell repository and updates the managed hosts.

    **NOTE:** Based on the network settings, enable proxy settings, if the network needs proxy.
  - Dell Custom Online—the OMIVV downloads the selected firmware updates from the Dell Custom Online, and applies to the hosts as necessary.
  - 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:** 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.

For information about setting up firmware update repository, see Setting up firmware update repository on page 38.

The **Firmware Update Wizard** always checks for the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller, and attempts to update them to the required minimum versions. See *OpenManage Integration for VMware vCenter Compatibility Matrix* for more information about the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller. Once iDRAC, Lifecycle Controller, and BIOS firmware versions meet the minimum requirements, the firmware update process enables updates for all firmware versions including: iDRAC, Lifecycle Controller, RAID, NIC/LOM, power supply, BIOS, and so on.

**Topics:**

- Updating firmware for an MX server managed using chassis
- Running firmware update wizard for non-vSAN host
- Running firmware update wizard for vSAN host
- Running firmware update wizard for non-vSAN clusters
- Running firmware update wizard for vSAN clusters

## Updating firmware for an MX server managed using chassis

Ensure that following prerequisites are met before scheduling the update for an MX chassis:

- Chassis must be in the administrator role.
- Chassis must be present in the vCenter.

You can run the firmware update wizard for the following:

- For the non-vSAN host, for more information about running firmware update for the non-vSAN host, see Running firmware update wizard for non-vSAN host on page 94.
- For the vSAN host, for more information about running firmware update for the vSAN host, see Running firmware update wizard for non-vSAN host on page 94.
- For the vSAN cluster, for more information about running firmware update for the vSAN cluster, see Running firmware update wizard for vSAN clusters on page 99.

- For the non-vSAN cluster, for more information about running firmware update for the non-vSAN cluster, see Running firmware update wizard for non-vSAN clusters on page 97.

# Running firmware update wizard for non-vSAN host

> **NOTE:** During the firmware update process, ensure that you do not delete the following:
> - The host from vCenter for which the firmware update job is in progress.
> - The connection profile of the host for which the firmware update job is in progress.

To perform the firmware update for a non-vSAN host, perform the following steps:

1. To access the firmware update wizard, in OpenManage Integration, click **Hosts** and perform either of the following actions:
   - Right-click a host, select **All OpenManage Integration Actions** > **Firmware Update**.
   - On the **Hosts** page, click a host, and then select **All OpenManage Integration Actions** > **Firmware Update**.
   - In the **Navigator** pane, select a host, and then click **Summary** > **OMIVV Host Information** > **Run Firmware Wizard**.
   - In the **Navigator** pane, select a host, and then click **Monitor** > **OMIVV Host Information** > **Firmware** > **Run Firmware Wizard**.

   OMIVV checks compliance of the host and whether any other firmware update job is in progress in any host within the same cluster. After the verification, the **Firmware Update** wizard is displayed.

   > **NOTE:** If you upgrade from an earlier version of OMIVV to the available version and there is already a firmware update job scheduled, you can launch the firmware update wizard on the same host after you back up the OMIVV database and restore it to the available version.

2. On the **Welcome** page, read the instructions, click **Next**.
   The **Select Update Source** page is displayed.
3. On the **Select Update Source** page, select either of the following:
   a. The **Current repository location** is displayed and selects the firmware update bundle from the **Select an Update Bundle** drop-down list.

      > **NOTE:** 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.

      > **NOTE:** 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.

      > **NOTE:** OMIVV supports 32–bit and 64–bit bundles for firmware update. Apart from the mentioned bundles, OMIVV also creates a hybrid bundle when there are 32-bit and 64-bit bundles available in the catalog for a particular model with the same release ID.

   b. To load a single firmware update from a file, select **Single DUP**. If you select **Single DUP**, go to step 6.
      A single DUP can reside on a CIFS or NFS share that is accessible by the virtual appliance. Enter the **File Location** in one of the following formats:
      - NFS share — `<host>:/<share_path/FileName.exe`
      - CIFS share — `\\<host accessible share path>\<FileName>.exe`

        For CIFS share, OMIVV prompts you to enter the user name and password in a domain format that can access the share drive.

        > **NOTE:** OMIVV supports only Server Message Block(SMB) version 1.0 and SMB version 2.0 based CIFS shares. It is recommended to use SMB version 2.0 based CIFS shares.

4. Click **Next**.
   The **Select Components** page is displayed.
5. Use the check boxes to select at least one firmware component from the list, and then click **Next**.

   The components that are either in a downgrade or currently scheduled for update cannot be selected. You can select the components that are listed for downgrade by selecting the **Allow Downgrade** option.

   The **Schedule Firmware Update** page is displayed.

   To filter comma-separated values from the content of the various components of the data grid, use **Filter**.

   You can also drag columns within the component data grid. If you want to export from the wizard, click 📤.

> ⓘ **NOTE:** If you select components that require a reboot, ensure that the vCenter environment is configured in such a way that the workloads can be migrated.

6. On the **Schedule Firmware Update** page, do the following:
   1. Specify job name in the **Firmware Update Job Name** field and description in the **Firmware Update Description** field, which is optional.

      The firmware update job name is mandatory and ensures that you do not use a name that is already in use. If you purge the firmware update job, you can reuse the job name again.
   2. If you have issues while updating the firmware, click **Delete Job Queue and Reset iDRAC**. This may result in successful completion of the update process. This increases the overall update time required for job completion, cancels any pending jobs or activities scheduled on the iDRAC, and resets the iDRAC.
   3. Enter the Maintenance Mode timeout value (in minutes). If the wait time goes beyond the specified time, the update job fails and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is rebooted.

      > ⓘ **NOTE:** The minimum Maintenance Mode timeout value is 60 minutes.

      > ⓘ **NOTE:** The maximum Maintenance Mode timeout value is one day.
   4. Select either of the following options:
      - Select **Update Now** to start the firmware update job immediately.

        By default, *Exit maintenance mode after firmware update completes* option is selected.

        By default, the *Move powered off and suspended virtual machines to other hosts in the cluster* option is selected. Disabling this option disconnects the VM until the host device is online.
      - To run the firmware update job later, select **Schedule Update**. You can schedule the firmware update job 30 minutes from the current time.
        - In the Calendar box, select the month and day.
        - In the Time text box, type the time in HH: MM. The time is the OMIVV appliance time.
      - To avoid a service interruption, select **Apply updates on next reboot**.
      - To apply the update and reboot even if the host is not in maintenance mode, select **Apply Updates, and Force Reboot without entering maintenance mode**. It not recommended to use this method.
7. Click **Next**.
   The **Summary** page is displayed that provides details about all components for firmware update.
8. Click **Finish**.

The firmware update job takes several minutes to complete, and the time varies based on the number of components included for the firmware update job. You can view the status of the firmware update jobs on the **Job Queue** page. To access the job queue page, in OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**. After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode based on an option selected in the **Schedule Firmware Update** page.

# Running firmware update wizard for vSAN host

Ensure that the following prerequisites are met before scheduling the update:

- DRS is enabled.
- Host is not in maintenance mode.
- vSAN data objects are healthy.

  To skip the above checks, clear the **Check Pre-Requisite** check box on the **Schedule Firmware Update** page.
- The selected drivers and firmware versions are compliant as per the VMware vSAN guidelines. Selected drivers are installed before the firmware update.
- The cluster satisfies the vSAN requirements for the selected data migration option.
- Rerun the inventory after enabling vSAN.

> ⓘ **NOTE:** During the firmware update process, Dell EMC recommends not to delete the following:
> - The host from vCenter for which the firmware update job is in progress.
> - The connection profile of the host for which the firmware update job is in progress.

To perform the firmware update for a single host, perform the following steps:

1. To access the firmware update wizard, in OpenManage Integration, click **Hosts** and perform either of the following actions:
   - Right-click a host, select **All OpenManage Integration Actions** > **Firmware Update**.
   - On the **Hosts** page, click a host, and then select **All OpenManage Integration Actions** > **Firmware Update**.
   - In the **Navigator** pane, select a host, and then click **Summary** > **OMIVV Host Information** > **Run Firmware Wizard**.
   - In the **Navigator** pane, select a host, and then click **Monitor** > **OMIVV Host Information** > **Firmware** > **Run Firmware Wizard**.

   OMIVV checks compliance of the host and whether any other firmware update job is in progress in any host within the same cluster. After the verification, the **Firmware Update** wizard is displayed.

   **NOTE:** If you upgrade from an earlier version of OMIVV to the available version and there is already a firmware update job that is scheduled, you can launch the firmware update wizard on the same host after you back up the OMIVV database and restore it to the available version.

2. On the **Welcome** page, read the instructions, click **Next**.

   The **Select Update Source** page is displayed.

3. On the **Select Update Source** page, do the following:
   a. Select the driver repository profile and firmware repository profile from the drop-down.

      If Baseline repository is associated in Cluster profile, the associated Firmware and Driver repositories are automatically selected.

   b. From the **Select an Update Bundle** drop-down, select an appropriate update bundle for your systems. Click **Next**.
      The **Driver Selection** page is displayed. The page displays the details of driver component such as **hostname**, **Service Tag**, **Component Name**, **Vendor**, **Package Name**, **Current**, **Available**, **Update applicable**.

   c. To load a single firmware update from a file, select **Single DUP**. If you select **Single DUP**, go to step 4.
      A single DUP can reside on a CIFS or NFS share that is accessible by the virtual appliance. Enter the **File Location** in one of the following formats:
      - NFS share—`<host>:/<share_path/FileName.exe`
      - CIFS share—`\\<host accessible share path>\<FileName>.exe`

      For CIFS share, OMIVV prompts you to enter the username and password in a domain format that can access the share drive.

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

   d. On the **Driver Selection** page, select the driver components that require update, and click **Next**.

      When you select a driver component for update, all the components in the package are selected.

      The **Select Components** page is displayed. The page displays the details of components such as **hostname**, **Service Tag**, M**odel Name**, **Component**, **Current**, **Available**, **Criticality**.

   e. Use the check boxes to select at least one firmware component from the list, and then click **Next**.

      The components that are either in a downgrade or currently scheduled for update cannot be selected. You can select the components that are listed for downgrade by selecting the **Allow Downgrade** option.

      The **Schedule Firmware Update** page is displayed.

      To filter comma-separated values from the content of the various components of the data grid, use **Filter**.

      You can also drag columns within the component data grid. If you want to export from the wizard, click 📤.

4. On the **Schedule Firmware Update** page, do the following:
   a. Specify job name in the **Firmware Update Job Name** field and description in the **Firmware Update Description** field, which is optional.

      The firmware update job name is mandatory and ensures that you do not use a name that is already in use. If you purge the firmware update job name, you can reuse the job name again.

      **NOTE:** By default, the **Check Pre-Requisite** check box is selected. The firmware update job is stopped if:
      - DRS is not enabled.
      - Maintenance mode is enabled for some hosts in the cluster.
      - The vSAN objects health is not healthy.

   b. If you have issues while updating the firmware, click **Delete Job Queue and Reset iDRAC**. This may result in successful completion of the update process. This increases the overall update time that is required for job completion, cancels any pending jobs or activities that are scheduled on the iDRAC, and resets the iDRAC.

   c. Enter the Maintenance Mode timeout value (in minutes). If the wait time goes beyond the specified time, the update job fails and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is rebooted.

ⓘ **NOTE:** The minimum Maintenance Mode timeout value is 60 minutes.

ⓘ **NOTE:** The maximum Maintenance Mode timeout value is 1440 minutes.

d. Select either of the following options:
   - Select **Update Now** to start the firmware update job immediately.

     By default, *Exit maintenance mode after firmware update completes* option is selected.

     By default, *Move powered down and suspended virtual machines to other hosts in the cluster* option is selected. Disabling this option disconnects the VM until the host device is online.

   - To run the firmware update job later, select **Schedule Update**. You can schedule the firmware update job 30 minutes from the current time.
     - In the Calendar box, select the month and day.
     - In the Time text box, type the time in HH: MM. The time is the OMIVV appliance time.
   - To avoid a service interruption, select **Apply updates on next reboot**.
   - To apply the update and reboot even if the host is not in maintenance mode, select **Apply Updates, and Force Reboot without entering maintenance mode**. It not recommended to use this method.

5. Click **Next**.
   The **Summary** page is displayed that provides details about all components for firmware update.
6. Click **Finish**.

The firmware update job takes several minutes to complete, and the time varies based on the number of components that are included for the firmware update job. You can view the status of the firmware update jobs on the **Job Queue** page. To access the job queue page, in OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**. After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode based on an option that is selected in the **Schedule Firmware Update** page.

# Running firmware update wizard for non-vSAN clusters

OMIVV allows you to perform BIOS and firmware updates on all hosts of a cluster. The wizard only updates hosts that are part of a connection profile and compliant in terms of firmware, CSIOR status, hypervisor, and OMSA status (11th generation servers only). OMIVV performs a cluster aware firmware update if Distribute Resource Scheduling (DRS) is enabled on the cluster, by migrating the workload when a host enters or exits maintenance mode.

Ensure that the following conditions are met before running the firmware update wizard:
- The firmware update repository is already set. For information about setting up firmware update repository, see Setting up the firmware update repository.
- There are no active firmware update jobs for any hosts under the cluster that you are updating.
- The hosts in the cluster are added to a connection profile and inventory is run successfully.
- DRS is enabled.

ⓘ **NOTE:** VMware recommends clusters to be built with identical server hardware.

ⓘ **NOTE:** During the firmware update process, Dell EMC recommends not to delete the following:
- The host/hosts of a cluster from vCenter for which the firmware update job is in progress.
- The connection profile of the host/hosts of a cluster for which the firmware update job is in progress.

1. To launch the Firmware Update wizard, in OpenManage Integration, click **Clusters** and perform either of the following substeps:
   - Click a cluster, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
   - In the **Objects** tab, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
   - Click a cluster, select **Monitor** > **OMIVV Cluster Information** > **Firmware**. In the **Firmware** screen, click the **Run Firmware Wizard** link.
   - Right-click a cluster, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.

   OMIVV checks compliance of the host and whether any other firmware update job is in progress in any host within the same cluster. After the verification, the **Firmware Update** page is displayed.

2. On the **Welcome** page, read the instructions, and click **Next**.
   The **Select Servers** page is displayed.
3. On the **Select Servers** page, in the **Name** tree view, use the check boxes to select the hosts.
4. Click **Next**.

   The **Select Update Source** page is displayed where you can select the bundles. The repository location is also displayed.
5. On the **Select Update Source** page, from the **Select an Update Bundle** drop-down, select an appropriate update bundle for your systems. Click **Next**.

   > **NOTE:** OMIVV supports 32–bit and 64–bit bundles for firmware update. Apart from these bundles, OMIVV also creates a hybrid bundle when there are 32-bit and 64-bit bundles available in the catalog for a particular model with the same release ID.

   > **NOTE:** 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.

   > **NOTE:** 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.
6. Click **Next**.
   The **Select Components** page is displayed. The page displays the details of components such as **hostname**, **Service Tag**, **Model Name**, **Component**, **Current**, **Available**, **Criticality**.
7. On the **Select Components** page, select the firmware components that require update and click **Next** to proceed.

   The components that are either in a downgrade or currently scheduled for update cannot be selected. You can select the components that are listed for downgrade by selecting the **Allow Downgrade** option.

   To filter comma-separated values from the content of the various components of the data grid, use **Filter**.

   You can also drag columns within the component data grid. If you want to export from the wizard, click .
8. On the **FW Update Information** page, view all the firmware update details.
9. Click **Next**.

   The **Schedule Firmware Update** page is displayed.

   a. Enter the firmware update job name in the **Firmware Update Job Name** field.
      The firmware update job name is mandatory and does not use a name that is already in use. If you purge the firmware update job name, you can reuse it again.
   b. Enter the firmware update description in the **Firmware Update Description** field, which is optional.
   c. If you have issues while updating the firmware, click **Delete Job Queue and Reset iDRAC**. This may result in successful completion of the update process. This increases the overall update time required for job completion, cancels any pending jobs or activities scheduled on the iDRAC, and resets the iDRAC.
   d. Enter the Maintenance Mode timeout value (in minutes). If the wait time goes beyond the specified time, the update job fails and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is rebooted.

      > **NOTE:** The minimum Maintenance Mode timeout value is 60 minutes.

      > **NOTE:** The maximum Maintenance Mode timeout value is one day.
   e. Under **Schedule Firmware Updates**, select an option from the following:
      - To run the update job now, click **Update Now**.
      - To run the update job later, click **Schedule Update**, and then perform the following subtasks:
        i. In the **Calendar** box, select the month and day.
        ii. In the **Time** text box, type the time in HH:MM.
10. Click **Next**.
    The **Summary** page is displayed.
11. On the **Summary** page, click **Finish** and the **The firmware update job has been created successfully** message is displayed.

The firmware update job takes several minutes to complete, and time varies based on the number of hosts that are selected and the number of components in each host. You can view the status of the firmware update jobs in the **Job Queue** page. To access the job queue page, in OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**. After the firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode.

# Running firmware update wizard for vSAN clusters

Ensure that the following condition is met before running the firmware update wizard:

- DRS is enabled.
- Hosts are not in maintenance mode.
- vSAN data objects are healthy. If the vSAN objects health is not healthy for the first host, the firmware update job fails. For other hosts, it waits for 60 minutes for the vSAN object heath to become healthy again.
- Selected drivers and firmware are compliant as per the VMware vSAN guidelines. Selected drivers are installed before the firmware update.
- Cluster satisfies the vSAN requirements for the selected data migration option. It is highly recommended to select the baselined (Cluster Profile) Firmware or Driver repository.
- You must create driver repository profile and firmware repository profile before you begin with firmware update. For information about creating driver repository and firmware repository, see Creating repository profile on page 43.
- There are no active firmware update jobs for any hosts under the cluster that you are updating.
- The hosts in the cluster are added to a connection profile and inventory is run successfully.
- Rerun the inventory after enabling the vSAN.

**NOTE:** VMware recommends clusters to be built with identical server hardware.

**NOTE:** During the firmware update process, Dell EMC recommends not to delete the following:

- The host/hosts of a cluster from vCenter for which the firmware update job is in progress.
- The connection profile of the host/hosts of a cluster for which the firmware update job is in progress.
- The repositories located in CIFS or NFS.

1. To launch the Firmware Update wizard, in **OpenManage Integration**, click **Clusters** and perform either of the following substeps:
   - Click a cluster, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
   - In the **Objects** tab, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
   - Click a cluster, select **Monitor** > **OMIVV Cluster Information** > **Firmware**. In the **Firmware** screen, click the **Run Firmware Wizard** link.
   - Right-click a cluster, select **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.

   OMIVV checks compliance of the host and whether any other firmware update job is in progress in any host within the same cluster. After the verification, the **Firmware Update** page is displayed.
2. On the **Welcome** page, read the instructions, and click **Next**.
   The **Select Servers** page is displayed.
3. On the **Select Servers** page, in the **Name** tree view, use the check boxes to select the hosts.
4. Click **Next**.

   The **Select Update Source** page is displayed.
5. On the **Select Update Source** page, do the following:
   a. Select the driver repository profile and firmware repository profile from the drop-down.

      If Baseline repository is associated in Cluster profile, the associated Firmware and Driver repositories are automatically selected.

      By default, the model name of the host is selected in the **Select Bundles** area.

   b. Select an appropriate update bundle for your systems and click **Next**.

      The **Driver Selection** page is displayed. The page displays the details of driver component such as **hostname**, **Service Tag**, **Component Name**, **Vendor**, **Package Name**, **Current**, **Available**, **Update applicable**.

   **NOTE:** OMIVV supports 32–bit and 64–bit bundles for firmware update. Apart from these bundles, OMIVV also creates a hybrid bundle when there are multiple bundles available in the catalog with the same release ID.

   **NOTE:** 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.
6. On the **Driver Selection** page, select the driver components that require update, and click **Next**.
   The **Select Components** page is displayed. The page displays the details of components such as **Host name**, **Service Tag**, M**odel Name**, **Component**, **Current**, **Available**, **Criticality**ol>.
7. On the **Select Components** page, select the firmware components that require update, and click **Next**.

   The components that are either in a downgrade or currently scheduled for update cannot be selected. You can select the components that are listed for downgrade by selecting the **Allow Downgrade** option.

To filter comma-separated values from the content of the various components of the data grid, use **Filter**.

You can also drag columns within the component data grid. If you want to export from the wizard, click 📤.

8. On the **FW Update Information** page, view all the firmware update details, and click **Next**.
   The **Schedule Firmware Update** page is displayed.
9. On the **Schedule Firmware Update** page, do the following:
   a. Enter the firmware update job name in the **Firmware Update Job Name** field.

      > **NOTE:** The firmware update job name is mandatory and does not use a name that is already in use. If you purge the firmware update job name, you can reuse it again.

   b. Enter the firmware update description in the **Firmware Update Description** field, which is optional.
   c. If you have issues while updating the firmware, click **Delete Job Queue and Reset iDRAC**. This may result in successful completion of the update process. This increases the overall update time required for job completion, cancels any pending jobs or activities scheduled on the iDRAC, and resets the iDRAC.
   d. Enter the Maintenance Mode timeout value (in minutes). If the wait time goes beyond the specified time, the update job fails and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is rebooted.

      > **NOTE:** The minimum Maintenance Mode timeout value is 60 minutes.

      > **NOTE:** The maximum Maintenance Mode timeout value is 1440 minutes.

   e. To run the update job now, click **Update Now**.
   f. Select the appropriate options from the **Virtual vSAN data migration** drop-down list. By default, **Ensure accessibility** is selected.

      > **NOTE:** By default, *Move powered off and suspended virtual machines to other hosts in the cluster* option is selected. Disabling this option disconnects the VM until the host device is online.

   g. To run the update job later, click **Schedule Update**, and then perform the following tasks:
      i. In the **Calendar** box, select the month and day.
      ii. In the **Time** text box, type the time in HH:MM.
      iii. Select the appropriate options from the **Virtual vSAN data migration** drop-down list. By default, **Ensure accessibility** is selected.

      > **NOTE:** By default, *Move powered off and suspended virtual machines to other hosts in the cluster* option is selected. Disabling this option disconnects the VM until the host device is online.

10. Click **Next**.
    The **Summary** page is displayed.
11. On the **Summary** page, click **Finish** and the **The firmware update job has been created successfully** message is displayed.

The firmware update job takes several minutes to complete, and time varies based on the number of hosts that are selected and the number of components in each host. You can view the status of the firmware update jobs in the **Job Queue** page. To access the job queue page, in OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**. After the firmware update task is completed, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode.

12

# Chassis management

OMIVV allows you to view additional information for chassis associated with the Modular servers. In the chassis information tab, you can view the chassis overview details for an individual chassis, information about hardware inventory, firmware and management controller, health of the individual chassis components, and chassis warranty information. The following three tabs are displayed for each chassis and varies for some chassis based on the models:

- Summary tab
- Monitor tab
- Manage tab

**NOTE:** To view all information, ensure that the chassis are associated with a chassis profile and chassis inventory is completed successfully. See the About chassis profile for more information.

**Topics:**

- Managing MX7000X Chassis
- Viewing chassis summary details
- Viewing hardware inventory information for chassis
- Viewing additional hardware configuration for chassis
- Viewing associated host for chassis
- Viewing related chassis information

## Managing MX7000X Chassis

The way that you manage an MX7000X chassis is different from managing other Dell EMC chassis such as M1000e, VRTX, and FX2.

You can manage an MX chassis in a standalone mode having public IPs for Management Module and iDRAC IPs. Also, you can configure an MX chassis in the Multi-Chassis Management (MCM) mode having one lead and multiple members.

Dell EMC OpenManage Enterprise-Modular supports wired MCM groups. In the wired type, the chassis is daisy-chained or wired through a redundant port on the management module. The chassis that you select for creating the group must be daisy-chained to at least one chassis. For more information about creating the chassis group, see *Dell EMC OpenManage Enterprise-Modular Edition Version 1.00.00 for PowerEdge MX Chassis User's Guide* at dell.com/support.

You can manage the servers present in an MX chassis in two ways:

1. **Managing the servers using the Connection profile**: The standard and recommended way of managing the servers where all the functions are supported. In this case, the chassis is discovered only after MX host inventory is complete. For more information about creating a connection profile, see Creating connection profile on page 34.
2. **Managing the servers using the Chassis profile**: If you choose to manage your hosts using the chassis profile, OMIVV features such as, inventory, monitoring, firmware and driver updates are supported. For more information about managing chassis and host using the chassis profile, see Chassis and host management using the Unified Chassis Management IP on page 102.

**NOTE:** If the IPv4 address of the iDRAC is disabled, you can choose to manage the server using the chassis profile. If you are managing the server using the chassis profile, the following OMIVV functions are not supported:

- iDRAC Lockdown mode
- Ability to use this server as a reference server to capture System Profile and Hardware profile
- OS deployment
- Getting or updating CSIOR status
- Server configuration compliance

**NOTE:** The hosts with a public IPv4 iDRAC IP can also be managed using the chassis profile. However, it is not recommended as the above listed functions are not supported.

## Chassis and host management using the Unified Chassis Management IP

If an iDRAC IPv4 is disabled for a host that is managed using connection profile, the host inventory fails and chassis is not discovered. In such cases, the chassis must be added manually and should be associated to a chassis profile to manage the chassis and its associated hosts.

If you choose to manage your hosts using the Unified Chassis Management IP, OMIVV features such as, inventory, monitoring, firmware, and driver updates are supported. The following are the high-level description of the tasks to manage the hosts and chassis using the Unified Chassis Management IP:

1. Add an MX chassis.

   For information about adding an MX chassis, see Adding an MX Chassis on page 102.

2. Create a chassis profile and associate the hosts.

   For more information about creating a chassis profile, see Creating chassis profile on page 53.

3. View jobs for both chassis and host that are managed using the chassis profile.
4. View chassis and host inventory.

   For more information about host and chassis inventory, see Viewing host inventory on page 56 and Viewing chassis inventory on page 57.

5. Perform firmware update on hosts that are managed using chassis.

   For more information about firmware update, see Updating firmware for an MX server managed using chassis on page 93.

   ⓘ **NOTE:** Bare-metal workflow is not supported when the hosts are managed using chassis.

## Adding an MX Chassis

A host with valid IPv4 iDRAC IP can be added to connection profile and during the host inventory, the associated MX chassis gets discovered automatically and displayed on the **Dell EMC Chassis** page.

If an iDRAC IPv4 is disabled for a host, the host inventory fails and chassis is not discovered. In such cases, an MX chassis must be added manually and should be associated to a chassis profile to manage the chassis and its associated hosts.

To add an MX chassis manually, do the following:

1. On the **OpenManage Integration for VMware vCenter** page, click **Dell EMC Chassis**.
2. On the **Dell EMC Chassis** page, click **Add MX Chassis**.
3. Enter a management module IPv4 or FQDN or hostname, and click **OK**.

   When you enter an IP, it is validated if the IP is being managed by OMIVV.

   ⓘ **NOTE:** Before adding chassis using hostname or FQDN, ensure that valid forward and reverse lookup entries are created in the DNS.

   ⓘ **NOTE:** If you enter FQDN, the chassis URL is displayed with the FQDN.

   The chassis is added to the **Dell EMC chassis** page.

4. Associate the hosts with the chassis profile by creating a chassis profile. For more information about creating a chassis profile, see Creating chassis profile on page 53.

ⓘ **NOTE:** If you enter an IP other than MX chassis IP, the test connection fails and invalid entry remains on the **Dell EMC Chassis** page. Only successfully validated chassis is associated with a chassis profile.

ⓘ **NOTE:** The test connection fails, if the hosts are not present in the registered vCenters that are associated to the added MX chassis.

# Viewing chassis summary details

You can view the chassis summary details for an individual chassis on the **Chassis Summary** page.

1. In the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration**, click **Dell EMC Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Summary** tab.

   The following information about the selected chassis is displayed:

   - Name
   - Model
   - Firmware version
   - Service tag
   - IP Address/FQDN

   ⓘ **NOTE:** If you do not run the inventory job for the chassis, you can see only Service Tag and CMC or Management Module IP address.

5. View the health status of the devices associated with the selected chassis.
   The main pane displays the overall health of a chassis. The valid health indicators are **Healthy**, **Warning**, **Critical**, **Not Present**. In the **Chassis Health** grid view, the health of each component is displayed. The chassis health parameters are applicable for models VRTX version 1.0 and later, M1000e version 4.4 and later. For M1000e firmware versions less than 4.3, only two health indicators are displayed, such as Healthy and Warning or Critical (Inverted triangle with an exclamatory mark in orange color).

   ⓘ **NOTE:** The overall health indicates the health based on the chassis with the least health parameter. For example, if there are 5 healthy signs and 1 warning sign, the overall health is shown as warning

6. View **CMC Enterprise** or **Express** with the license type and expiry date for a chassis.

   The mentioned details are not applicable for M1000e and MX chassis.

7. Click the **Warranty** icon and view the number of remaining days and the days used for a host.
   If you have more than one warranty, the last day of the last warranty is considered to calculate the number of days left for warranty.
8. View the errors in the **Active Errors** table lists for a chassis, which are displayed in the **Chassis Health** page.

   ⓘ **NOTE:** For M1000e version 4.3 and earlier, the active errors are not displayed.

# Viewing hardware inventory information for chassis

You can view information about the hardware inventory within the selected chassis. To view the information in this page, ensure that you run an inventory job and export a .CSV file with the component information.

1. In the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration**, click **Dell EMC Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.

   To view the relevant component information, navigate through OMIVV:

**Table 28. Hardware inventory information**

| Hardware inventory: Component | Navigation through OMIVV | Information |
|---|---|---|
| Fans | Use either of the following methods:<br>● In the **Overview** tab, click **Fans**.<br>● In **Monitor** tab, expand the left pane, click **Hardware** | Information about fans:<br>● Name<br>● Present<br>● Identifier<br>● Power State<br>● Reading (RPM) |

### Table 28. Hardware inventory information

| Hardware inventory: Component | Navigation through OMIVV | Information |
|---|---|---|
| | **Inventory**, and then click **Fans**. | - Warning Threshold<br>- Critical Threshold<br>  ○ Minimum<br>  ○ Maximum<br>- Pulse Width Modulation (Only for MX chassis)<br>ⓘ **NOTE:** In an MX chassis, the presence of a fan is indicated as 'Yes' even when a fan is removed from the chassis. However, the fan health is displayed as **Critical** on the **Summary** page with active error. |
| Power supplies | Use either of the following methods:<br>- In the **Overview** tab, click **Power Supplies**.<br>- In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **Power Supplies**. | Information about power supplies:<br>- Name<br>- Capacity<br>- Present<br>- Power state<br>- Input Voltage (Only for MX chassis) |
| Temperature sensors | Use either of the following methods:<br>- In the **Overview** tab, click **Temperature Sensors**.<br>- In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **Temperature Sensors**. | Information about temperature sensors:<br>- Location<br>- Reading<br>- Warning threshold<br>  ○ Maximum<br>  ○ Minimum<br>- Critical threshold<br>  ○ Maximum<br>  ○ Minimum<br>ⓘ **NOTE:** For PowerEdge M1000e chassis, information about the temperature sensors is displayed only for chassis. For other chassis, information about the temperature sensors is displayed for chassis and associated modular servers. |
| I/O modules | Use either of the following methods:<br>- In **Overview** tab, click **I/O Modules**.<br>- In **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **I/O Modules**. | Information about I/O modules:<br>- Slot/Location<br>- Present<br>- Name<br>- Fabric<br>- Service Tag<br>- Power Status<br>To view additional information, select the corresponding I/O module and the following information is displayed:<br>- Role<br>- Firmware version<br>- Hardware version<br>- IP address<br>- Subnet mask<br>- Gateway<br>- MAC address<br>- DHCP enabled |

Table 28. Hardware inventory information (continued)

| Hardware inventory: Component | Navigation through OMIVV | Information |
|---|---|---|
| Fabric (Only for MX chassis) | Use either of the following methods:<br>● In the **Overview** tab, click **Fabric**.<br>● In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **Fabric**. | Information about Fabric components:<br>● Health<br>● Fabric<br>● Description<br>● Switch Count<br>● Compute Count<br>● Uplink Count<br>To view the switches that are associated with the fabric, select a fabric component and the following information is displayed in the lower grid:<br>● Switch<br>● Chassis<br>● Slot<br>● Chassis Role<br>● Switch Model |
| PCIe | Use either of the following methods:<br>● In the **Overview** tab, click **PCIe**.<br>● In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **PCIe**. | Information about PCIe:<br>● PCIe slot<br>○ Slot<br>○ Name<br>○ Power status<br>○ Fabric<br>● Server slot<br>○ Name<br>○ Number<br>To view additional information, select the corresponding PCIe and following information is displayed:<br>● Slot type<br>● Server mapping<br>● Assignment status<br>● Allocated slot power<br>● PCI ID<br>● Vendor ID<br>**NOTE:** PCIe information is not applicable for M1000e chassis. |
| iKVM | Use either of the following methods:<br>● In the **Overview** tab, click **iKVM**.<br>● In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **iKVM**. | Information about iKVM:<br>● iKVM Name<br>● Present<br>● Firmware version<br>● Front Panel USB/Video enabled<br>● Allow access to CMC CLI<br>**NOTE:** You can view information about the iKVM only for PowerEdge M1000e Chassis<br>**NOTE:** The iKVM tab is displayed only if the chassis contains iKVM module. |

# Viewing additional hardware configuration for chassis

You can view information about the warranty, storage, firmware, management controller details within the selected chassis. To view the information in this page, ensure that you run an inventory job and export a .CSV file with the component information.

To view warranty, storage, firmware, management controller details for chassis, perform the following steps:

1. In the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration**, click **Dell EMC Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.

   To see the information about warranty, storage, firmware, and management controller, navigate through OMIVV.

**Table 29. Firmware details**

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| Firmware | a. In the **Monitor** tab, click the double arrow mark and expand the left pane, and then click **Firmware**.<br>b. In the **Monitor** tab, If you click **Launch Chassis**, the **Chassis Management Controller** page is displayed. | Information about firmware:<br>● Component<br>● Current Version |

**Table 30. Management controller details**

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| Management controller | a. In the **Monitor** tab, click the double arrow mark and expand the left pane, and then click **Management Controller**.<br>b. In the **Management Controller** page, to view additional information, click the arrow mark and expand the left column. | Information about management controller:<br>● General<br>○ Name<br>○ Firmware Version<br>○ Last Update Time<br>○ Chassis Location<br>○ Hardware Version<br>● Common Network<br>○ DNS Domain Name<br>○ Use DHCP for DNS<br>○ MAC Address<br>○ Redundancy Mode<br>● IPv4 Information<br>○ IPv4 Enabled<br>○ DHCP Enabled<br>○ IP Address<br>○ Subnet Mask<br>○ Gateway<br>○ Preferred DNS Server<br>○ Alternate DNS Server<br>● IPv6 Information<br>○ IPv6 Enabled<br>○ DHCP Enabled<br>○ IP Address<br>○ Link Local Address<br>○ Gateway<br>○ Preferred DNS Server<br>○ Alternate DNS Server |

Table 30. Management controller details

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| | | ● Local Access Configuration<br>○ Quick Sync Hardware Present<br>○ LCD Present<br>○ LED Present<br>○ KVM Enabled<br>**NOTE:** Few attributes of network related information of a member chassis which is part of the MCM configuration is not displayed in the **Management Controller** section. |

Table 31. Storage information

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| Storage | In the **Monitor** tab, click **Storage**. | Information about storage:<br>● Virtual Disks<br>● Controllers<br>● Enclosures<br>● Physical Disks<br>● Hot Spares<br>For MX chassis, the following information is displayed:<br>● Slot Number<br>● Slot Name<br>● Model<br>● Service Tag<br>● Firmware version<br>● Asset Tag<br>● Power State<br>● Assignment Mode<br>For MX chassis, if you want to view information about drives, click storage sled. The following drive information is displayed in the lower pane:<br>● Health<br>● State<br>● Slot<br>● Slot Assignment<br>● Disk Name<br>● Capacity<br>● Bus protocol<br>● Media<br>For M1000e chassis, if you have a storage module, the following storage details are displayed in a grid view without any additional information:<br>● Name<br>● Model<br>● Service Tag<br>● IP Address (Link to storage)<br>● Fabric<br>● Group Name<br>● Group IP Address (link to storage group)<br>**NOTE:** When you click a highlighted link under storage, the **View** table displays the details for each highlighted item. In the view table, if you click each line item, |

**Table 31. Storage information**

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| | | additional information is displayed for each highlighted item. |

**Table 32. Warranty information**

| Hardware configuration | Navigation through OMIVV | Information |
|---|---|---|
| Warranty | In the **Monitor** tab, click **Warranty**. | Information about warranty:<br>● Provider<br>● Description<br>● Status<br>● Start Date<br>● End Date<br>● Days Left<br>● Last Updated<br>**NOTE:** To view warranty status, ensure that you run a warranty job. See Running a warranty retrieval job. |

# Viewing associated host for chassis

You can view information about the associated host for the selected chassis on the **Manage** tab.

1. In the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration**, click **Dell EMC Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Manage** tab.

   The following information about the associated host is displayed:

   - Hostname (If you click the selected host IP, the details about the host is displayed.)
   - Service Tag
   - IP
   - Chassis URL
   - Model
   - iDRAC IP
   - Location
   - Last Inventory
   - Role (Only for MX chassis)

     **NOTE:** When you export the chassis information from the **Dell EMC Chassis** page, the group ID, enumeration value, and role value are all listed in the **Role** column of the .csv file.

# Viewing related chassis information

The **Related Chassis** page shows the relationship between chassis in an MX chassis that is deployed in the MCM mode. In the **Related Chassis** tab, you can view all the associated chassis information for lead and member chassis.

**NOTE:** Related chassis information is applicable only for an MX chassis that is configured in an MCM group.

1. On the **OpenManage Integration for VMware vCenter** page, in the left pane, click **Dell EMC Chassis**.
   The **Dell EMC Chassis** page is displayed.
2. On the **Dell EMC Chassis** page, click **Manage**.
3. In the left pane, select a chassis (lead or member) and click **Related Chassis**.

The following information is displayed:

- Name
- IP
- Service Tag
- Chassis URL
- Model
- Location
- Last Inventory
- Available Slots
- Profile Name
- Role

**NOTE:** Related Chassis information is not applicable for standalone chassis.

13

# Deploying hypervisor

OMIVV enables you to configure the following components in the supported bare-metal servers along with deploying the hypervisor and adding it to the specified data center and cluster in a vCenter:

- Boot order setting
- RAID configuration
- BIOS configuration
- iDRAC configuration

You can create hardware profiles, System profiles, and hypervisor profiles on the bare-metal servers using VMware vCenter without using PXE.

**NOTE:** Dell EMC recommends using system profile for 14th Gen and later servers when deploying hypervisor.

To provision hardware and perform deployment, ensure that the physical servers are displayed in the Deployment Wizard. Ensure that all physical servers are as per the following requirements:

- Meet specific hardware support information that is available in the *OpenManage Integration for VMware vCenter Compatibility Matrix*.
- Meet minimum supported versions of the iDRAC firmware, Lifecycle Controller, and BIOS. See the *OpenManage Integration for VMware vCenter Compatibility Matrix* for specific firmware support information.
- Configure NICs in PCI slots manually after the deployment. If you are using add-on NICs, the system must have the host LAN on Motherboard (LOMs) or Network Daughter Card (NDC) enabled and connected to network.
- Meet the storage specifications of IDSDM. To know about the storage specifications of IDSDM, see the VMware Documentation. Ensure that you enable the IDSDM from BIOS before you deploy the hypervisor with OMIVV. OMIVV enables deployment on IDSDM or local hard drives.
- Ensure that there is a route between the vCenter and the iDRAC networks if vCenter and iDRAC are connected to different networks.
- Ensure that Collect System Inventory on Reboot (CSIOR) is enabled. Also, before initiating auto/manual discovery, ensure that retrieved data is current by completely powering down the system and then turn-on the system—hard reboot.
- Click to order the Dell EMC servers with auto discovery and handshake options that are preconfigured by the factory. If a server is not preconfigured with these options, manually enter the OMIVV IP address or configure your local network to provide this information.
- Ensure that the following conditions are met before initiating hypervisor deployment if OMIVV is not used for hardware configuration:
  - Enable the Virtualization Technology (VT) flag in BIOS.
  - Set the system's boot order to either a bootable virtual drive or IDSDM for operating system installation.
- Verify that the BIOS setting for VT is automatically enabled even if the BIOS configuration is not part of the hardware profile, if OMIVV is used for hardware configuration. The Express/Clone RAID configuration is required if a virtual drive is not already present on the target system.
- Ensure that the custom ESXi images that contain all the Dell drivers are available for deployment. You can find the correct images from `Support.dell.com` by going to to the **Dell Drivers & Downloads** page, and saving the custom images to a CIFS or NFS share location that OMIVV can access during the deployment process. For up-to-date list of supported ESXi versions for this release, see *OpenManage Integration for VMware vCenter Compatibility Matrix*. To use the correct images, see the Downloading custom Dell ISO images.
- Ensure that you have BIOS mode that is selected in the reference hardware profile before applying the hypervisor profile as OMIVV only supports BIOS mode to autodeploy hypervisor on the target server. If there is no hardware profile that is selected, ensure that you manually configure the boot mode as BIOS and reboot the server before applying the hypervisor profile.

If servers are from versions earlier than PowerEdge 12th Gen servers, the deployment process performs the following tasks:

- Installs the OMSA package on the target system.
- Automatically configures the SNMP trap destination in OMSA to hover over OMIVV.

**Topics:**

- Device discovery
- Provisioning

- System profiles
- Managing System profiles
- Configuring hardware profile
- Creating hypervisor profile
- Creating deployment templates
- About deployment wizard
- Deployment job timing
- Downloading custom Dell EMC ISO images

# Device discovery

Discovery is the process of adding supported bare-metal server. After a server is discovered, you can use it for hypervisor and hardware deployment. See *OpenManage Integration for VMware vCenter Compatibility Matrix* for the list of the servers required for deployment. The network connectivity from the bare-metal server's iDRAC to the OMIVV virtual machine is required.

> **NOTE:** The hosts with existing hypervisors should not be discovered into OMIVV, instead they should be added to the vCenter. Add them to a connection profile, and then reconcile with the OpenManage Integration for VMware vCenter using the host compliance wizard.

> **NOTE:** If bare-metal servers were discovered earlier than OMIVV 4.0, ensure that you remove the machines from the bare-metal server list and rediscover them.

> **NOTE:** To perform OS deployment on SD card for 12th generation bare-metal PowerEdge servers, ensure that iDRAC 2.30.30.30 and later is installed.

## Manual discovery

You can manually add a bare-metal server that is not added by the discovery process. Once added, the server is displayed in the list of servers in the Deployment Wizard.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, click the ✚ icon.
   The **Add Server** dialog box is displayed.
2. In the **Add Server** dialog box, do the following:
   a. In the **iDRAC IP Address** text box, enter the iDRAC IP Address.
   b. In the **User Name** text box, enter the user name.
   c. In the **Password** text box, enter the password
3. Click **Add Server**.
   The task of adding the server might take few minutes to complete.

# Auto discovery in OpenManage Integration for VMware vCenter

Auto discovery is the process of adding bare-metal server. Once a server is discovered, use it for hypervisor and hardware deployment. Auto discovery is an iDRAC feature that removes the need of manually discovering a bare-metal server from OMIVV.

## Auto discovery prerequisites

Before attempting to discover the PowerEdge bare-metal servers, ensure that OMIVV has been already installed. The PowerEdge servers with iDRAC Express or iDRAC Enterprise can be discovered into a pool of bare-metal servers. Ensure that there is network connectivity from the Dell EMC bare-metal server's iDRAC to the OMIVV appliance.

> **NOTE:** The hosts with existing hypervisors should not be discovered in to OMIVV, instead add the hypervisor to a connection profile, and then reconcile with OMIVV by using the Host Compliance Wizard.

For auto discovery to occur, the following conditions must be met:

- Power—ensure that you connect the server to the power outlet. The server need not be powered on.

- Network connectivity—ensure that the server's iDRAC has network connectivity and communicates with the provisioning server over port 4433. You can obtain the IP address by using a DHCP server or manually specify it in the iDRAC configuration utility.
- Additional network settings—ensure that you enable Get DNS server address from DHCP setting, if using DHCP, so that DNS name resolution can occur.
- Provisioning service location—ensure that iDRAC knows the IP address or host name of the provisioning service server. See Provisioning service location.
- Account access disabled—ensure that you enable the administrative account access to iDRAC and if there are any iDRAC accounts with administrator privileges, first disable them from within the iDRAC web console. Once auto discovery completes successfully, the administrative iDRAC account is re-enabled.
- Auto discovery enabled—ensure that the server's iDRAC has auto discovery enabled so that the auto discovery process can begin.

### Provisioning service location

Use the following options to obtain the provisioning service location by iDRAC during auto discovery:

- Manually specified in the iDRAC—manually specify the location in the iDRAC configuration utility under LAN User Configuration, Provisioning Server.
- DHCP scope option—specify the location using a DHCP scope option.
- DNS service record—specify the location using a DNS service record.
- DNS known name—DNS server specifies the IP address for a server with the known name DCIMCredentialServer.

If the provisioning service value is not manually specified in the iDRAC console, iDRAC attempts to use the DHCP scope option value. If the DHCP scope option is not present, iDRAC attempts to use the service record value from DNS.

For detailed information about how to configure the DHCP scope option and DNS service record, see Dell Auto-Discovery Network Setup Specification at https://www.dell.com/support.

## Enabling or disabling administrative accounts on iDRAC

Before you set up auto discovery, disable all administrative accounts other than root. The root account should be disabled during the auto discovery procedure. Once you have successfully set up auto discovery, return to iDRAC GUI and re-enable the administrative accounts that were turned off, other than root.

> **NOTE:** To guard against a failed auto discovery, you can enable a nonadmin account on iDRAC. The nonadmin account allows remote access when auto discovery fails.

1. In a browser, type the **iDRAC IP address**.
2. Log in to the **Integrated Dell Remote Access Controller GUI**.
3. Do one of the following:
   - For iDRAC6: In the left pane, select the **iDRAC Settings** > **Network/Security** > **Users** tab.
   - For iDRAC7: In the left pane, select the **iDRAC Settings** > **User Authentication** > **Users** tab.
   - For iDRAC8: In the left pane, select the **iDRAC Settings** > **User Authentication** > **Users** tab.
4. In the **Users** tab, locate any administrative accounts other than root.
5. To disable the account, under User ID, select the **ID**.
6. Click **Next**.
7. In the **User Configuration** page, under **General**, clear the **Enable User** check box.
8. Click **Apply**.
9. To re-enable each administrative account, repeat steps 1 through 8 after you have successfully set up auto discovery, but select the **Enable User** check box now, and click **Apply**.

## Manually configuring PowerEdge 11th generation servers for auto discovery

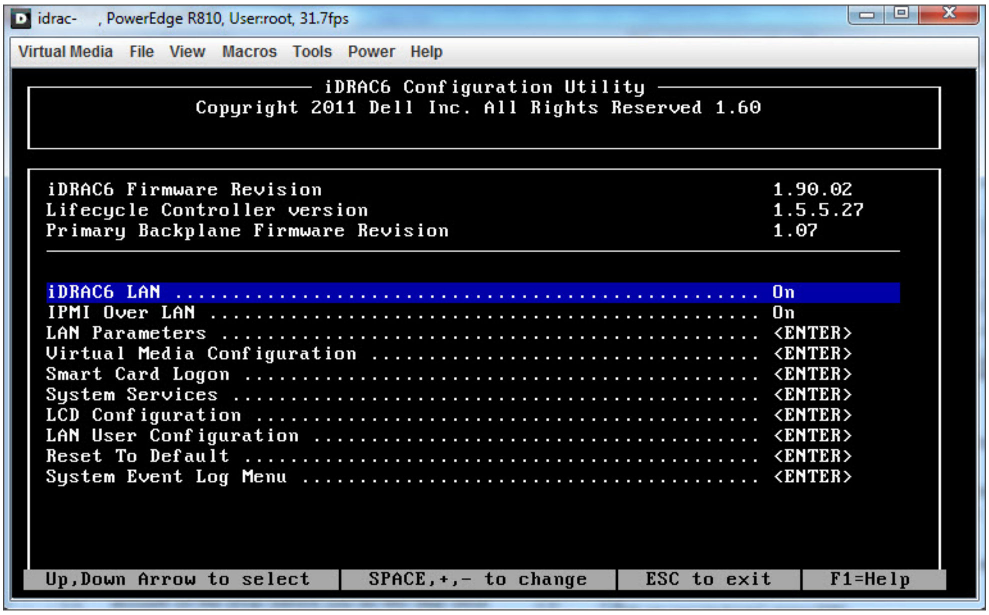
Ensure that you have the iDRAC and host IP addresses.

If you have not ordered your bare-metal appliance to use auto discovery from the factory, you can set it up manually.

On successful auto discovery of bare-metal servers, a new administrator account is created or an existing account is enabled with the credentials returned by the handshake service. All the other administrative accounts that were disabled prior to auto discovery are not enabled. Ensure that you re-enable the administrator accounts after a successful auto discovery. See Enabling or disabling administrative accounts on iDRAC.

> **NOTE:** If for some reason, the auto discovery did not complete successfully, there is no way to connect to iDRAC remotely. A remote connection requires you to enable a non-admin account on the iDRAC. If there is no non-admin enabled account present on the iDRAC, the only way to access the iDRAC is to log in to the box locally and enable the account on the iDRAC.

1. Enter the **iDRAC IP** address into a browser.
2. Log in to the **iDRAC Enterprise GUI**.
3. In the **Integrated Dell Remote Access Controller 6 — Enterprise** > **System Summary** tab, in the Virtual Console Preview, click **Launch**.
4. In the **Warning — Security** dialog box, click **Yes**.
5. In the iDRAC Utility Console, press **F12** once or twice.
   The **Authentication Required** dialog box is displayed.
6. In the **Authentication Required** dialog box, view the name that is displayed, and press **Enter**.
7. Enter `Password`.
8. Press **Enter**.
9. When the **Shutdown/Restart** dialog box is displayed, press **F11**.
10. The host restarts and the screen displays information about loading memory, then RAID, then when it shows iDRAC and prompts you to press CTRL + E, immediately press **CTRL + E**.
    If you view the following dialog box, the action is successful, else, go to the Power menu, Power Off and Power On again, and repeat this step.


idrac- , PowerEdge R810, User:root, 31.7fps
Virtual Media File View Macros Tools Power Help

```
iDRAC6 Configuration Utility
Copyright 2011 Dell Inc. All Rights Reserved 1.60

iDRAC6 Firmware Revision                                    1.90.02
Lifecycle Controller version                                1.5.5.27
Primary Backplane Firmware Revision                         1.07

iDRAC6 LAN ................................................ On
IPMI Over LAN ............................................. On
LAN Parameters ............................................ <ENTER>
Virtual Media Configuration ............................... <ENTER>
Smart Card Logon .......................................... <ENTER>
System Services ........................................... <ENTER>
LCD Configuration ......................................... <ENTER>
LAN User Configuration .................................... <ENTER>
Reset To Default .......................................... <ENTER>
System Event Log Menu ..................................... <ENTER>

Up,Down Arrow to select | SPACE,+,- to change | ESC to exit | F1=Help
```

**Figure 1. iDRAC configuration utility**

11. In the iDRAC6 Configuration Utility, use the arrow keys to select **LAN Parameters**.
12. Press **Enter**.
13. If this host is a blade, to configure NIC, use the space bar to toggle the options to **Enabled**.
14. If you are using DHCP, use the arrow keys to select **Domain Name from DHCP**.
15. Use the space bar to toggle the option to **On**.
16. If you are using DHCP, use the arrow keys to navigate to the IPv4 settings and select **DNS Servers from DHCP**.
17. Use the spacebar to toggle the option to **On**.
18. To Exit, on your keyboard, press **ESC**.
19. Use the arrow keys to select **LAN User Configuration**.
20. Use the arrow Keys to select **Provisioning Server**.
21. Press **Enter**.
22. Enter the IP address of the host.
23. Press **ESC**.

24. Use arrow keys to select **Account Access**.
25. Use the space bar to toggle the option to **Disable**.
26. Use the arrow keys to select **Auto-Discovery**.
27. Use the space bar to toggle the option to **Enabled**.
28. From your keyboard, press **ESC**.
29. Press **ESC** again.

## Manually configuring PowerEdge 12th and later generation servers for auto discovery

Ensure that you have an iDRAC address.

When you order servers from Dell EMC, you can ask for the auto discovery feature to be enabled on the servers after you provide the provisioning server IP address. The provisioning server IP address should be the IP address of OMIVV. Therefore, after you receive the servers from Dell EMC, when you power on the servers after mounting and connecting the iDRAC cable, the servers get auto discovered and listed in the first page of the Deployment Wizard.

> **NOTE:** For auto discovered servers, the credentials that are provided under **Manage** > **Settings** > **Deployment Credentials** is set as admin credentials and is used for further communication with the server, until the OS deployment is completed. After a successful OS deployment, the iDRAC credentials that are provided in the associated connection profile are set.

To enable auto discovery manually on the target machine, perform the following steps for 12th and later generation servers:

1. To go to system setup, boot/reboot the target system and press F2 during the initial boot.
2. Go to **iDRAC Settings** > **User Configuration** and disable the root user. Ensure that there are no other users with active administrator privileges on the iDRAC address when you are disabling the root user.
3. Click **Back**, and click **Remote Enablement**.
4. Set **Enable Auto-Discovery** as **Enabled** and **Provisioning Server** as the IP address of the OMIVV.
5. Save the settings.
   The server is auto discovered upon next server boot. After successful auto discovery, the root user gets enabled, and the **Enable Auto-Discovery** flag is disabled automatically.

## Removing bare-metal server

You can manually remove a server that has been auto discovered or manually added.

1. In OpenManage Integration for VMware vCenter, click the **Manage** > **Deployment** tab.
2. In the **Bare Metal Servers** page, select the servers and click ✖.

# Provisioning

All auto/manually discovered complaint bare-metal systems are available to OMIVV for hardware provisioning and hypervisor deployment. To prepare for provisioning and deployment, do the following:

### Table 33. Preparing for deployment (continued)

| Steps | Description |
|---|---|
| Create a system profile | Contains the system configuration settings gathered from a 14th generation reference server that is used to configure the new servers. |
| Create a hardware profile | Contains the hardware settings gathered from a reference server that is used to deploy new servers. See Creating or customizing hardware profile on page 118. |
| Create a hypervisor profile | Contains the hypervisor installation information needed for the ESXi deployment. See Creating hypervisor profile on page 121. |
| Create a deployment template | A deployment template contains a system profile, hardware profile, hypervisor profile, a combination of system profile and hypervisor profile, or a combination of the hardware profile |

**Table 33. Preparing for deployment**

| Steps | Description |
|---|---|
| | and hypervisor profile. You can save and reuse these profiles as required for all available data center servers. |

After the deployment template is created, use the deployment wizard to gather the information necessary to create a scheduled job that provisions server hardware and deploys new hosts in vCenter. For information about running the deployment wizard, see Running Deployment Wizard on page 124. Lastly, view the job status through job queue and change the pending deployment jobs.

# System profiles

The System profiles feature is available in iDRAC for PowerEdge servers that provide support for configuring CNA, FCoE apart from configuration support for the Boot order, RAID, BIOS, and iDRAC. OMIVV supports System profiles of iDRAC 14th generation as "System Profile". By supporting Server Configuration Profile, OMIVV allows you to export the entire configuration of a 14th generation Dell EMC server and import to target servers.

While applying a System profile of a modular server installed in an FX2 chassis to another similar server installed on another FX2 chassis, the slot numbers of both the servers must be the same.

For example, System profile taken from an FC640 server in slot 1 of a FX2s chassis can only be applied on another FC640 server residing in the slot 1 of another FX2s chassis.

**NOTE:** System profile does not support enabling and disabling of boot options.

**NOTE:** While using the system profile, exporting a system profile with enterprise license and importing the same system profile on servers with express license fails, and conversely.

**NOTE:** You cannot import system profile by using the Express license of iDRAC9 firmware 3.00.00.00. You must have an Enterprise license.

**NOTE:** The System profiles searches for exact instance (FQDD) while applying the profile, which works successfully on rack servers (identical), but may have few restrictions in modular servers. For example, in FC640, the System profiles created from one modular server cannot be applied on other modular servers in the same FX chassis because of NIC level restrictions. In this case, it is recommended to have a reference System profile from each slot of the chassis and apply these System profiles across the chassis for the corresponding slots only.

The typical tasks of using a system profile include:

- Creating or capturing the system profile information from a reference server. See Creating system profile on page 116.
- Applying the profile on selected servers by using the deployment template. See Creating deployment templates on page 122.

**NOTE:** It is recommended to use system profile for 14th generation and later servers.

To launch the system profile page, perform the following steps:

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **System Profiles**.
    a. In the **System Profiles** page, view the list of System profiles that you have created.

       A table is displayed that lists the System profiles along with profile name, description, server model, and reference server information.

    b. To view further details of a system profile host, select a system profile.

       Review the system profile information that displays details such as profile name, iDRAC IP, iDRAC type, Service Tag, Host Name, Server Model, created date, modified date, and modified by whom.

    c. To swap the columns within the data grid, drag and drop columns within the data grid.
    d. To filter or search the content of the data grid, click the **Filter** field.
    e. To export the system profile information to a .CSV file, select a system profile, and then in the right-hand corner of the data grid, click the  icon.

# Creating system profile

Ensure that the following conditions are met before creating a system profile:

- The reference server is configured as per the requirement, outside of OMIVV. Modifying any values of any of the attributes is not supported in the current version, except for the iDRAC user passwords.
- Collect System Inventory On Restart (CSIOR) is enabled on a reference server, and the reference server is rebooted, so that the data returned from iDRAC is up-to-date.
- OpenManage Integration had performed a successful inventory on each of the vCenter managed hosts.
- Bare-metal servers have the minimum BIOS and firmware versions already installed. See *OpenManage Integration for VMware vCenter Compatibility Matrix* for more information about the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller.

You can create a system profile by using only a 14th generation reference server.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **System Profiles**.
2. Click ➕.
3. On the **Welcome** page, read the instructions, and click **Next**.
   - In the **Profile Name** text box, enter the profile name.
   - In the **Profile Description** text box, type a description. The description value is optional.
4. Click **Next**.
   The **Reference Server** dialog box is displayed. You can either select 14th generation reference servers from the dialog box directly or through the browse button in the profile source page.
5. Select a 14th generation reference server by performing either of the following substeps:

   > **NOTE:** All hosts from 11th to 14th generations are displayed in the dialog box and the select link is enabled only for 14th generation complaint bare metal servers and hosts, whereas only 14th generation bare-metal servers are displayed and the select link is enabled only for complaint bare-metal servers.

   > **NOTE:** Select a 14G reference server which is compliant managed host or bare-metal server. However, you cannot select a host as a reference server which is managed through Chassis profile.

   a. In the **Reference Server** dialog box, click the right 14th generation reference server, and click the **Select** link against the reference server.

   > **NOTE:** The **Select** link is enabled only for complaint servers.

   b. In the **Reference Server** page, click **Browse** to select a compliant 14th generation host reference server that is managed and successfully inventoried by OMIVV, or a compliant 14th generation bare-metal server.

   The **Extract Confirmation** dialog box that states extracting the settings is displayed. To extract the hardware configuration from reference server, in the **Extract Confirmation** dialog box, click **Yes**, and the extracting is completed in few minutes.

   The selected Server name, Reference Server Type, the iDRAC IP address, Model, and Service Tag are displayed in the **Profile Source** page.

   > **NOTE:** If **Reference Server Type** is a bare-metal server, only iDRAC IP is displayed whereas if **Reference Server Type** is a host, both iDRAC IP and host IP/FQDN is displayed.

6. Click **Next**.
7. On the **Profile Settings** page, expand iDRAC to view the system profile attributes. You can sort the data grid columns in ascending or descending order. Click the data filter icon to filter the data.

   a. To quickly view the Set Password link in the **Value** column, click ▽, type 'password' in the **Value Contains**, and enter the password for enabled user.

   > **NOTE:** Dell EMC recommends you to provide the credentials same as the credentials used during addition of bare metal server. If you change the password in the deployment template, the changes are not displayed to the root user. During OS deployment, if Hypervisor Profile is associated with the deployment template, deployment takes connection profile (iDRAC and ESXi) password.

   > **NOTE:** The **Set Password** option is available only for the iDRAC enabled user with valid user name.

   Also, you can view the profile settings for the components based on the configuration of the Dell Reference Server such as iDRAC, BIOS, RAID, NIC, CNA, FCoE, and EvenFilters.

b. Expand each of the components to display the setting options such as **Instance**, **Attribute Name**, **Value**, **Destructive**, **Dependency**, and **Group**.

When you hover over the attributes, more information about the attribute is displayed.

By default, few attributes such as **Read Only**, **System Specific**, and **Destructive** attributes are disabled for selection.

If the dependency text is not available, dependency text is empty.

> **NOTE:** When performing RPM upgrade, or backup and restore, following are applicable for all the migrated profiles:
> - When you hover over the attributes, attribute names are displayed.
> - Only non system-specific attributes are selected.
> - Dependency text is not displayed.
> - Enabled attributes display the total number of selected attributes.

8. Click **Next**.
The **Summary** page is displayed that provides information about the profile details and the attribute statistics of the system configurations.

   The total number of attributes, total number of enabled attributes, total number of platform-specific attributes, and total number of destructive attributes are displayed under attribute statistics.
9. In the **Summary** page, click **Finish**.
The profile is automatically saved, and is displayed in the **System Profiles** window.

All system-specific attributes are not supported in the current release. For more information about system-specific attributes, see System specific attributes on page 161.

Few attributes of System Profile are overridden for the OMIVV to be functional. For more information about customized attributes, see Customization attributes on page 165. For more information about the System Profile configuration template, attributes, and workflows, see Additional information on page 166.

# Managing System profiles

The System profiles define system configuration of a server by using a reference server. From OpenManage Integration for VMware vCenter, there are several management actions that you can perform on existing System profiles, including:

- Viewing system profile
- Deleting system profile

> **NOTE:** Modifying System Profile from OMIVV is not supported in the current release. You must configure your machine outside of OMIVV, and then use it as reference server for System Profile.

# Configuring hardware profile

To configure server hardware settings, create a hardware profile. A hardware profile is a configuration template that you can apply to newly discovered infrastructure components and it requires the following information:

**Table 34. Requirements for creating hardware profile**

| Requirements | Description |
|---|---|
| Boot order | The boot order is the boot device sequence and hard drive sequence that you can edit only if the boot mode is set to BIOS. |
| BIOS settings | The BIOS settings include memory, processor, SATA, integrated devices, serial communications, embedded server management, power management, system security, and miscellaneous settings.<br>**NOTE:** The OpenManage Integration for VMware vCenter enables certain BIOS settings under the Processor group in the BIOS on all deployed servers, regardless of the settings on the reference server. Before using a reference server to create a hardware profile, the reference server must have the CSIOR setting enabled and rebooted to provide accurate inventory and configuration information. |
| iDRAC settings | The iDRAC settings include network, user list, and user configuration. |

**Table 34. Requirements for creating hardware profile**

| Requirements | Description |
|---|---|
| RAID configuration | The RAID configuration displays the current RAID topology on the reference server at the time the hardware profile was extracted.<br>ⓘ **NOTE:** There are 2 RAID configuration options configured in the hardware profile:<br>1. Apply RAID1 + create a dedicated hot spare, as applicable—use this option if you want to apply default RAID configuration settings to the target server.<br>2. Clone RAID configuration from the reference server—use this option if you want to clone the reference server setting. See Customizing reference server for creating hardware profile. |

The tasks for creating hardware profiles include:

- Enabling CSIOR on a reference server
- Customizing reference server to create a hardware profile
- Cloning a hardware profile

## Enabling CSIOR on reference server

Before creating a hardware profile by using a reference server, enable the Collect System Inventory On Reboot (CSIOR) setting, and reboot the server to provide accurate inventory and configuration information.

There are two methods for enabling CSIOR:

**Table 35. Methods for enabling CSIOR**

| Method | Description |
|---|---|
| Locally | Uses an individual host by using the Dell Lifecycle Controller United Server Configurator (USC) user interface. |
| Remotely | Uses a WS-Man script. For more information on scripting this functionality, see *Dell TechCenter* and *DCIM Lifecycle Controller Management Profile*. |

To enable CSIOR locally on a reference server:

1. Power on the system, and during POST, press **F2** to start USC.
2. Select **Hardware Configuration** > **Part Replacement Configuration**.
3. Enable the **Collect System Inventory on Reboot** setting, and exit USC.

## Creating or customizing hardware profile

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hardware Profiles**.
2. Click the ✚ icon.
3. In the **Hardware Profile Wizard**, click **Next** on the **Welcome** page and do the following:
   - In the **Profile Name** text box, enter the profile name.
   - In the **Description** text box, type a description. The description is optional.
4. Click **Next**.
   The **Reference Server** dialog box is displayed. You can either select reference servers from the dialog box directly or through the browse button in the reference server window.
5. Select a reference server by performing either of the following substeps:
   - In the **Reference Server** dialog box, choose the right reference server, and click the **Select** link against the reference server.

     The **Extract Confirmation** dialog box that states extracting the settings is displayed. To extract the hardware configuration from reference server, in the **Extract Confirmation** dialog box, click **Yes**, and the extracting is completed in few minutes.
   - In the **Reference Server** page, click **Browse** to select a compliant reference server that is managed and successfully inventoried by OMIVV, or a compliant bare-metal server.

To extract the hardware configuration from reference server, in the **Extract Confirmation** dialog box, click **Yes**.

The selected Server name, the iDRAC IP address, model, and Service Tag are displayed in the **Reference Server** page.

6. In the **Reference Server** page, to customize the reference server settings, click **Customize Reference Server Settings**, and choose the following settings that can be optionally included and customized:
   - **RAID Settings**
   - **BIOS Settings**
   - **Boot Order**
   - **iDRAC Settings**
     - **Network Settings**
     - **User List**
7. In the **RAID Configuration** window, select one of the following, and click **Next**:
   - **Apply RAID1 + create a dedicated hot spare, if applicable**—use this option, if you want to apply default RAID configuration settings to the target server. The RAID configuration task defaults to RAID1 on the first two drives of the integrated controller that are RAID1 capable. Also, a dedicated hot-spare for the RAID1 array is created, if a candidate drive that meets the RAID criteria exists.
   - **Clone RAID configuration from the reference server as shown below**—use this option, if you want to clone the reference server setting.
8. In the **BIOS Settings** page, to include BIOS setting information in the profile, expand a category to display the setting options, and click **Edit** to update one of the following:
   - **System Information**
   - **Memory Settings**
   - **Processor Settings**
   - **SATA Settings**
   - **Boot Settings**
   - **One-Time Boot**
   - **Integrated Devices**
   - **Slot Disablement**
   - **Serial Communication**
   - **System Profile Settings**
   - **System Security**
   - **Miscellaneous Settings**

   After all updates are made for a category, to save the changes, click **Next**, or to cancel the changes, click **Cancel**.

   **NOTE:** For detailed BIOS information, including setting options and explanations, see the *Hardware Owner's Manual* for the selected server.
9. In the **Boot Order** page, do the following and click **Next**:
   a. To display boot order options, expand **Boot Order**, and then click **Edit** to make the following updates:
      i. In the **Boot Mode** list, select `BIOS` or `UEFI`.
      ii. In the **View** list, under **Boot Device Sequence**, to change the displayed boot device sequence, select the device, and click either **Move Up** or **Move Down**.
      iii. Select **Enable Boot Sequence Retry** so that the server automatically retries the boot sequence.
      iv. To apply the changes, click **OK**, or to cancel the changes, click **Cancel**.
   b. To display the hard drive sequence options, Expand **Hard Drive Sequence**, and click **Edit**. Update the following:
      i. To change the displayed hard drive sequence, select the device and click either **Move Up** or **Move Down**.
      ii. To apply the changes, click **OK**, or to cancel the changes, click **Cancel**.

   **NOTE:** For servers earlier than 13th generation, both UEFI and BIOS modes are displayed; whereas for 13th or later generation servers, either BIOS, or UEFI mode is displayed.
10. In the **iDRAC Settings** page, do the following:
    a. Expand a category to display the setting options, and click **Edit**:

       Update one of the following:
       - **Network Settings**
       - **Network**
       - **Virtual Media**

b. Under iDRAC local **User List**, do one of the following:
    - **Add User**—manually enter an iDRAC user and the required information. When finished, to apply the changes, click **Apply**, or to cancel, click **Cancel**
    - **Delete User**—delete the selected user. To select a user, use the mouse, and click **Delete**. To confirm the deletion, click **Yes**.
    - **Edit User**—manually edit an iDRAC user's information. When complete, to apply the settings, click **Apply**, or to cancel, click **Cancel**.

After all updates are made for a category, to save the changes, click **Next**, or to cancel the changes, click **Cancel**.

> **NOTE:** For detailed iDRAC information, including setting options and explanations, see the *iDRAC User's Guide* for the selected server.

11. Click **Next**.
12. In the **Summary** page, click **Finish**.

The profile is automatically saved, and is displayed in the **Hardware Profiles** window.

# Creating or cloning hardware profile

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hardware Profiles**.
2. Click ➕.
3. In the **Hardware Profile Wizard**, click **Next** on the **Welcome** page and perform the following actions:
    - In the **Profile Name** text box, enter the profile name.
    - In the **Description** text box, enter `Description`. The description is optional.
4. Click **Next**.
5. To select a reference server that is compliant, managed by vCenter, and successfully inventoried by the Dell EMC OpenManage plugin, in the **Reference Server** page, click **Browse**.

    > **NOTE:** You can select the reference server whose inventory is successfully generated by OpenManage Integration or the compliant bare-metal servers. However, you cannot select a host as a reference server which is managed through Chassis profile.

6. To extract all hardware settings from the reference server, click the **Clone Reference Server Settings** option.
7. Click **Next**.
    Extracting the settings takes several minutes to complete.
8. Click **Next**.
    The settings are populated, and the selected server's name, the iDRAC IP address, and service tag are displayed in the reference server window.

The profile is saved and displayed in the **Hardware Profiles** window under **Available Profiles**.

# Managing hardware profiles

The hardware profiles define hardware configuration of a server by using a reference server. From OpenManage Integration for VMware vCenter, there are several management actions that you can perform on existing hardware profiles, including:

- Viewing or editing hardware profile
- Deleting hardware profile

## Viewing or editing hardware profile

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hardware Profiles**.
    The hardware profiles are displayed.
2. To edit a profile, select a profile, and click ✏.
3. In the **Hardware Profile** wizard, to configure with different values, click **Edit**.

4. To apply changes, click **Save**, or to cancel changes, click **Cancel**.

## Deleting hardware profile

ⓘ **NOTE:** Deleting a hardware profile that is part of a running deployment task might cause the deletion task to fail.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates Hardware Profiles**.
2. Select a profile, and click ✖.
3. To remove the profile, in the confirmation dialog box, click **Yes**, or to cancel, click **No**.

# Creating hypervisor profile

To deploy and configure ESXi to a server, create a hypervisor profile. A hypervisor profile requires the following information:

- A Dell customized ISO software media location on an NFS or CIFS share
- A vCenter instance that manages the deployed hosts, and an optional host profile
- The destination cluster or data center where the plug-in deploys servers in vCenter

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hypervisor Profiles**.
2. In the **Hypervisor Profiles** page, click ➕.
3. In the **Hypervisor Profile** dialog box, do the following subtasks:
   - In the **Profile Name** text box, enter the profile name.
   - In the **Description** text box, enter description, which is an optional entry.
4. Under **Choose the Reference ISO Path and Version**, in the **Installation Source (ISO)** text box, type the path to the hypervisor share location.

   A copy of the hypervisor image is modified to permit a scripted installation. The reference ISO location can be in one of the following formats:

   - `NFS format: host:/share/hypervisor.iso`
   - `CIFS format: \\host\share\hypervisor.iso`

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

   If using a CIFS share, enter the **User Name**, **Password**, and **Verify Password**. Ensure that the passwords match.
5. In the **Select a version** list, select an ESXi version.
   All servers deployed using this hypervisor profile has this image, and if the servers are from versions earlier than 12th generation, the latest recommended version of OMSA is also installed.
6. To verify the path and authentication, click **Begin Test** under **Test Settings**.
7. Click **Apply**.

# Managing hypervisor profiles

There are several management actions that you can perform on existing hypervisor profiles, including:

- Viewing or editing hypervisor profiles
- Deleting hypervisor profiles

## Viewing or editing hypervisor profiles

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hypervisor Profiles**.
   The hypervisor profiles are displayed.
2. Select a profile, and click ✏.
3. In the **Hypervisor Profile** dialog box, provide updated values.

4. To apply changes, click **Save**, or to cancel changes, click **Cancel**.

## Deleting hypervisor profile

**NOTE:** Deleting a hypervisor profile that is part of a running deployment task can cause the task to fail.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates** > **Hypervisor Profiles**.
2. Select a profile, and click ✖.
3. In the confirmation dialog box, to remove the profile, click **Delete**, or to cancel, click **Cancel**.

# Creating deployment templates

A deployment template contains a system profile, hardware profile, hypervisor profile, a combination of system profile and hypervisor profile, or a combination of the hardware profile and hypervisor profile. The **Deployment Wizard** uses this template to provision server hardware and deploy hosts within vCenter.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates**.
2. Click ➕.
3. In the **Deployment Template** dialog box, enter a name for the template.
4. Enter **Description** for the deployment template, which is optional.
5. Click **System Profile** or **Hardware Profile** and select the appropriate profile from the drop-down menu.

   **NOTE:** It is recommended to use system profile for 14th generation servers and hardware profile for 14th generation and earlier servers.

6. Select a **Hypervisor Profile** from the drop-down menu.
7. To apply profile selections and save changes, click **Save**. To cancel, click **Cancel**.

## Managing deployment templates

From the OpenManage Integration, there are several management actions you can perform on existing deployment templates, including:

- Viewing or editing deployment templates
- Deleting deployment templates

## Viewing or editing deployment templates

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates**. The deployment template profiles are displayed.
2. In the **Deployment Template** dialog box, type the new name of the template and description.

   Ensure that the template has a unique name.
3. Change the **Hardware Profile** or **System Profile** from the drop-down menu.
4. Change the **Hypervisor Profile** from the drop-down menu and click **Save**.

## Deleting deployment templates

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Deployment** tab, select **Deployment Templates**.
2. In the **Deployment Template** page, select a template, and click ✖.
3. To confirm the template deletion, click **Delete** on the message box, or to cancel, click **Cancel**.

# About deployment wizard

The deployment wizard describes the deployment process, which is as follows:

- Selecting compliant bare-metal servers.

  ⓘ **NOTE:** If you select the 14th generation servers for deployment, the deployment template list includes a hardware profile or system profile or hypervisor profile or combination of hardware and hypervisor or combination of system and hypervisor profiles.

  ⓘ **NOTE:** If you select non-14th generation servers or a combination of 14th generation and non-14th generation servers, the deployment template list includes a hardware profile or hypervisor profile, or a combination of hardware profile and hypervisor profiles.
- Selecting a deployment template, which consists of hardware and hypervisor profiles.
- Selecting the installation target (hard disk, BOSS, or iDSDM).

  When you deploy hypervisor, you can deploy to an Internal Dual SD Module. The Internal Dual SD Module should be enabled from BIOS, before you deploy a hypervisor with OMIVV.
- Selecting the connection profile to be associated with the host.
- Assigning the network details for each host.
- Selecting the vCenter, destination data center or cluster, and an optional host profile.
- Scheduling the server deployment jobs to run.

ⓘ **NOTE:** If you are deploying a hardware profile only, then the Server Identification, Connection Profile, network detail options of the deployment wizard are skipped and you directly go to the **Schedule Deployment** page.

ⓘ **NOTE:** For trial/evaluation license, you can use deployment wizard as long as the license does not expire.

# VLAN support

OMIVV supports hypervisor deployment to a routable VLAN and you can configure VLAN support in the Deployment Wizard. In this portion of the Deployment Wizard, there is an option to specify use of VLANs and to specify a VLAN ID. When a VLAN ID is provided, it is applied to the hypervisor's management interface during deployment and tags all traffic with the VLAN ID.

Ensure that the VLAN provided during deployment communicates with both the virtual appliance and the vCenter server. The deployment of a hypervisor to a VLAN that cannot communicate to one or both of these destinations causes the deployment to fail.

If you have selected multiple bare-metal servers in a single deployment job and want to apply the same VLAN ID to all servers, in the server identification portion of the Deployment Wizard, use **Apply settings to all selected servers**. This option enables you to apply the same VLAN ID along with the other network settings to all the servers in that deployment job.

ⓘ **NOTE:** OMIVV does not support a multihomed configuration. Adding a second network interface to the appliance for communication with a second network causes problems for the workflow involving hypervisor deployment, server compliance, and firmware updates.

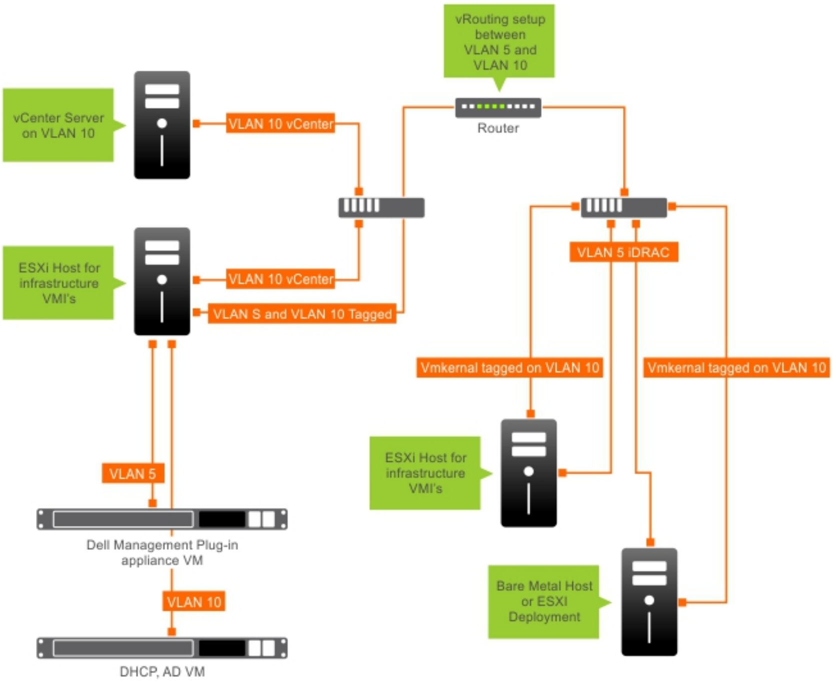

vRouting setup between VLAN 5 and VLAN 10
Router
vCenter Server on VLAN 10
VLAN 10 vCenter
ESXi Host for infrastructure VMI's
VLAN 10 vCenter
VLAN S and VLAN 10 Tagged
VLAN 5 iDRAC
Vmkernal tagged on VLAN 10
Vmkernal tagged on VLAN 10
ESXi Host for infrastructure VMI's
VLAN 5
Dell Management Plug-in appliance VM
VLAN 10
DHCP, AD VM
Bare Metal Host or ESXI Deployment

**Figure 2. VLAN network.**

In this example network, the OMIVV appliance is on VLAN 5, while the vCenter and the VMkernal of the ESXi hosts being deployed are on VLAN 10. Since OMIVV does not support multi-VLAN homing, VLAN 5 must route to VLAN 10 for all systems to communicate to each other correctly. If routing is not enabled between these VLANs, the deployment fails.

# Running Deployment Wizard

Ensure that you create a deployment template with hardware profile, system profile, and hypervisor profile, and connection profile for the vCenter before running the deployment wizard.

To run the deployment wizard:

1. In the OpenManage Integration for VMware vCenter, select the **Manage** > **Deployment** tab.
2. In the **Bare Metal Servers** window, click the **Run Deployment Wizard** link.
   The deployment wizard **Welcome** page is displayed.
3. In the **Welcome** page, view the information and click **Next**.
4. In the **Select the servers for deployment** page, to assign compliant bare-metal servers to a deployment job, click the check boxes next to the list of servers.
5. Click **Next**.
6. In the **Select Template/Profile** page, perform the following substeps:
   a. Under **Deployment Template**, to assign a deployment template to the selected servers, select an existing deployment template from **Select Deployment Template**.

      **NOTE:** System profile-based template is displayed only if you select the 14th Gen servers on the **Select the servers for deployment** page.

      You can select one of the following deployment templates from the drop-down list:

      - If you select a hardware profile only or system profile only deployment template that only configures server hardware, go to step 10.
      - If you select hypervisor profile deployment template that deploys a hypervisor, continue from step 6 (b) onwards.

        **NOTE:** If you select hardware profile or system profile only deployment, you are automatically prompted to include information for the **Schedule Deployment** page.

   b. Under **Hypervisor Installation**, select either of the following options:

      - **First boot disk**—deploys a hypervisor on the Hard Disk (HDD), Solid State Drive (SSD), virtual drive created by RAID controllers.

- **BOSS**—deploys a hypervisor on the BOSS card.

  ⓘ **NOTE:** If you are using OMIVV to deploy a hypervisor on the BOSS controller, ensure that system profile or hardware profile is captured from the reference server along with the BOSS VD configuration and target server must have a BOSS with similar configuration. For more information about creating VD, see *Dell EMC Boot Optimized Server Storage-S1 User's Guide* at dell.com/support.

  ⓘ **NOTE:** If BOSS is available on at least one of the selected servers, the **BOSS** option is enabled. If not, only the **Hard Disk** option is available.
- **Internal Dual SD Module**—deploys a hypervisor on the IDSDM.

  ⓘ **NOTE:** If an IDSDM is available on at least one of the selected servers, the **Internal Dual SD Module** option is enabled. If not, only the **Hard Disk** option is available.

  If any of the selected servers do not support an IDSDM, or an IDSDM is not present during deployment, perform one of the following actions:

  ⓘ **NOTE:** The **First boot disk** installation target is not equivalent to the first entry in the **BIOS Hard-Disk Drive Sequence** or **UEFI Boot sequence**. This option deploys the hypervisor on to the first disk identified by the ESXi pre-OS environment. Therefore, ensure that the **Hard-Disk FailOver** or **Boot sequence retry** option is enabled when the First Boot Disk option is selected

  - Select **Deploy the hypervisor to the first boot disk for servers that do not have an available Internal Dual SD Module** check box, if you want to deploy a hypervisor on the first boot disk of the servers.

    ⚠ **CAUTION: If you select this option and deploy the hypervisor on the first boot disk drive of the servers, all the data on the disk drives are erased.**
  - To skip the deployment on the selected servers and go to hypervisor deployment on the next server, clear **Deploy the hypervisor to the first boot disk for servers that do not have an available Internal Dual SD Module**.

c. Under **Credential Profile**, perform either of the following actions:

- Select the **Use this Credential Profile for all Servers** option button, and to assign all servers to the same existing profile, select the connection profile from the drop-down list.
- Click the **Select a Connection Profile for each Server** option button, and then select an individual connection profile for each server from the drop-down list.

7. Click **Next**.
   The **Server Identification** page is displayed.

   The server identification can be provided in two ways:

   - Enter networking information (IP address, subnet mask, and gateway)—a fully qualified domain name for the hostname is mandatory. The use of *localhost* for the FQDN is not supported. The FQDN is used when adding the host to vCenter.
   - Use Dynamic Host Configuration Protocol (DHCP) to configure IP addresses, subnet mask, gateway IP, hostname, and preferred/alternate DNS servers—the DHCP assigned IP address is used when adding the host to vCenter. When using DHCP, Dell EMC recommends that an IP reservation for selected NIC MAC addresses is used.

   ⓘ **NOTE:** Use a Fully Qualified Domain Name (FQDN) for host name instead of localhost. Starting with ESXi 5.1, a value of localhost impairs the OMIVV plug-in from processing events that are sent from the host. Create a DNS record that resolves the IP address with the FQDN. For SNMP alerts from ESXi 5.1 to be identified correctly, configure the DNS server to support reverse lookup requests. The DHCP reservations and DNS host names must be in place and verified before the deployment job is scheduled to run.
8. In the **Server Identification** page, do the following:

   The page provides the option to specify a VLAN ID. When a VLAN ID is provided, it is applied to the management interface of hypervisor during deployment and tags all traffic with the VLAN ID. Server Identification assigns new names and network identification to deployed servers. See VLAN support.

   a. To expand and view individual server information, under **Selected Servers**, click ☰.
   b. Under **Host Name and NIC**, enter a **Fully Qualified Host Name** for the server.
   c. In the **NIC for Management Tasks** drop-down list, select the NIC for managing the server.
   d. Enter IP addresses, subnet mask, default gateway, and DNS details, or select the **Obtain using DHCP** check box.
   e. If deploying to a network that requires a VLAN ID, select the **VLAN** check box and then enter the `VLAN ID`.

      For the VLAN ID, use the numbers 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.
   f. Repeat steps a through h for all servers to be deployed, or select the **Apply settings to all selected servers** check box.

      If you select the **Apply settings to all selected servers**, enter FQDN name and IP address for the other servers.

**NOTE:** While specifying FQDN name for servers, ensure to provide unique host names for each server.

9. Click **Next**.
10. In the **Schedule Deployment** page, perform the following actions:
    a. Enter a **Job Name** and **Job Description**.
    b. For **vCenter Settings**, enter the following:
        i. In **vCenter Instance**, select the server instance that manages a host after deployment.
        ii. In **vCenter Destination Container**, click **Browse** to search for vCenter destinations.
        iii. In **vCenter Host Profile**, select a profile that encapsulates host configuration and helps to manage host configuration, which is optional.
    c. Determine when to run a deployment job by selecting a job schedule:
        i. Select **Schedule Deployment Job**
            - Use the calendar control to select the date.
            - Enter the time.
        ii. To start the job immediately, select **Run Deployment Job Now**.

    To go to the job queue after the deployment job starts, select **Go to the Job Queue after the job is submitted**.
11. Click **Finish**.

After the deployment wizard tasks are complete, you can manage deployment jobs using **Job Queue**. .

## Managing deployment jobs using Job Queue

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Deployment Jobs**.

   The following details about deployment jobs are displayed in the upper grid:
   - Name
   - Description
   - Scheduled Time
   - Status
   - Collection Size
   - Progress Summary
2. To update **Deployment Jobs Details**, click the **Refresh** icon.
3. To display deployment job details, which contains detailed information about the servers included in the deployment job, select a deployment job in the upper grid.

   The following details are displayed in the lower grid:
   - Service tag
   - iDRAC IP address
   - Job status
   - Warnings
   - Deployment job details (more information available on mouse hover).
   - Start and End time
   - More Details

   You can view entire information about a deployment job as a pop-up text by selecting the job and hovering your cursor on the **Details** column of the deployment job.

   For more details about the system profile based jobs failure, click **More Details**. The **More Details** page displays the following information:
   - FQDD of the component
   - Value of the attribute
   - Old value
   - New value
   - Message and message ID about the failure (not displayed for few types of errors)

   For few attributes displayed under **Attribute Name** of **Apply System Profile-Failure Details** window is not same as **Attribute Name** of the system profile when you click **More Details**.

   To export the details to a .CSV file, in the right corner of the data grid, click .

4. To abort the deployment job, click the ✋ icon.
5. When the message is displayed, click **Abort Job** to abort, or to cancel, click **Do Not Abort Job**.
6. To display the **Purge Deployment Job Queue** window, click 🧹. Select the **Older than date and job Status**, and click **Apply**.
   The selected jobs are then cleared from the queue.

## System Lockdown Mode jobs

1. On the **OpenManage Integration for VMware vCenter** page, click the **Monitor** > **Job Queue** tab, and then click **System Lockdown Mode Jobs**.
   The following information about the System Lockdowm Mode jobs is displayed in the upper grid:
   - Name
   - Description
   - Scheduled Time
   - vCenter
   - Status
   - Collection Size
   - Progress Summary
2. To update **System Lockdown Mode Jobs Details**, click the **Refresh** icon.
3. To display the System Lockdown Mode job details, which contain detailed information about the servers included in the System Lockdown Mode job, select a System Lockdown Mode job in the upper grid.
   The following details are displayed in the lower grid:
   - Service Tag
   - iDRAC IP
   - Host Name
   - Status
   - Details

     > **NOTE:** If the **Status** column displays **Successful**, the **Details** column is empty.
     >
     > If the **Status** column displays **Failed**, the reason for failure is displayed in the **Details** column.
   - Start Date and Time
   - End Date and Time

   You can view entire information about a System Lockdown mode job as a pop-up text by selecting the job and hovering your cursor on the **Details** column of the System Lockdown Mode job.
4. To purge the System Lockdown Mode Jobs, click 🧹. Select the **Older than date and job Status**, and click **Apply**.
   The selected jobs are then cleared from the job queue.

## Drift Detection Jobs

A drift detection job is run to find the comparison between the validated baseline and the server configuration which includes hardware configuration, firmware, and driver versions.

1. On the **OpenManage Integration for VMware vCenter** page, click the **Monitor** > **Job Queue** tab, and then click **Drift Detection Jobs**.

   The following information about the Drift Detection jobs is displayed in the upper grid:
   - Name
   - Last Run
   - Next Run
   - Status
   - Collection Size
   - Progress Summary
2. To view the updated **Drift Detection Job Details**, click **Refresh**.
3. To display the Drift Detection job details, which contain detailed information about the servers included in the Drift Detection job, select a Drift Detection job in the upper grid.

The following details are displayed in the lower grid:

- Service Tag
- iDRAC IP
- Host Name
- Cluster
- vCenter
- Status
- Start Date and Time
- End Date and Time

4. To run the **Drift Detection** job on-demand, click ▶.

   > **NOTE:** In a baselined cluster, after adding a host device to the connection profile or chassis profile, the drift detection job is automatically run on a newly added host device.

## Managing firmware update jobs

To view information in this page, run a firmware update job for a cluster. See Running the firmware update wizard for clusters.

The page displays all the firmware update jobs. In this page you can view, refresh, purge, or abort your firmware update jobs.

1. From the OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**.
2. To display the most recent information, click the **Refresh** icon.
3. View the status in the datagrid.

   The grid offers the following information about firmware update jobs:

   - Status
   - Scheduled Time
   - Name
   - Description
   - vCenter
   - Collection Size (number of servers on the firmware job)
   - Progress Summary (progress details of the firmware update)

4. To view more details about a particular job, in the data grid for a particular job, select a job.

   Here you can find the following details:

   - Host Name
   - Status
   - Start Time
   - End Time

5. If you want to abort a scheduled firmware update that is not running, select the job you want to abort, and click ✋.

   > **NOTE:** If you abort a firmware update job that is already submitted to iDRAC, the firmware might still get updated on the host, but OMIVV reports the job as canceled.

6. If you want to purge earlier firmware update jobs or scheduled firmware updates, click 🧹.
   The **Purge Firmware Update Jobs** dialog box is displayed. You can only purge jobs that are canceled, successful, or failed and cannot purge scheduled or active jobs.
7. In the **Purge Firmware Update Jobs** dialog box, select **Older than**, and click **Apply**.
   The selected jobs are then cleared from the queue.

# Deployment job timing

The provisioning and deploying of bare-metal servers can take between 30 minutes to several hours to complete, depending on several factors. When starting a deployment job, Dell EMC recommends that you plan your deployment time according to the guidelines provided. The amount of time it takes to complete provisioning and deployment varies with deployment type, complexity, and number of deployment jobs running simultaneously. The following table provides the approximate time a deployment job can take: The deployment jobs are run in batches of up to five concurrent servers to improve time for the overall deployment job. The exact number of concurrent jobs depends on available resources.

ⓘ **NOTE:** The following table displays the average value, and may vary based on factors like configuration of the server, Gen of the server, and number of bare metal servers scheduled for deployment.

Table 36. Approximate deployment time

| Deployment type | Approximate time per deployment |
|---|---|
| Hypervisor only | Between 30–130 30 minutes to 130 minutes |
| Hypervisor and hardware profiles | 1–4 hours |
| System profile only | 5–6 minutes |
| System profile and hypervisor profile | 30–40 minutes |

## Server states within deployment sequence

When an inventory job is run, the auto or manually discovered bare-metal systems are classified in different states to help determine if the server is new to the data center or has a pending deployment job scheduled. The administrators can use these states to determine if a server should be in a deployment job. The following are the states:

Table 37. Server states in the deployment sequence

| Server state | Description |
|---|---|
| Unconfigured | The server has contacted OMIVV and is waiting to be configured. |
| Configured | The server is configured with all hardware information that is required for a successful hypervisor deployment. |

# Downloading custom Dell EMC ISO images

The custom ESXi images that contain all Dell drivers are required for deployment.

1. Open a browser and navigate to `support.dell.com`.
2. Click **Browse all products** > **Servers** > **PowerEdge**.
3. Click a PowerEdge server model.
4. Click **Drivers & Downloads** page of the server model.
5. From the **Operating System** drop-down, select the ESXi version.
6. From the **Category** drop-down menu, select **Enterprise Solutions**.
7. In the **Enterprise Solutions** list, select the required version of ISO, and then click **Download**.

14

# About host, bare-metal, and iDRAC compliance

To manage hosts and bare-metal servers with OMIVV, each must meet certain minimum criteria. If not compliant, they are not managed properly by OMIVV. OMIVV displays details about the noncompliance on a bare-metal or a host, and allows you to fix the noncompliance, where applicable.

In each case, you can view and fix the compliance issues by running one of the following:

- To view and fix vSphere host compliance issues, see Running the fix noncompliant vSphere hosts wizard.
- To view and fix bare-metal servers that have compliance issues, see Running the fix noncompliant bare-metal server wizard.

ⓘ **NOTE:** If the OEM hosts are not displayed on the **vSphere Hosts** page, add the OEM hosts by using the **Add OEM Hosts** wizard. For more information about adding OEM hosts, see Adding OEM Hosts.

**Topics:**

- Reporting and fixing compliance for vSphere hosts
- Support for OEM servers
- Adding OEM hosts
- Viewing baseline compliance
- Using OMSA with 11th generation servers
- Reporting and fixing compliance for bare-metal servers

## Reporting and fixing compliance for vSphere hosts

A host is noncompliant when:

- The host is not assigned to a connection profile.
- The Collect System Inventory on Reboot (CSIOR) is disabled or has not been run, which requires a manual reboot.

  ⓘ **NOTE:** The CSIOR status is not determined when hosts are managed using a chassis.
- The OMSA agent is not installed, is out of date, or not configured properly. An ESXi host reboot is required, if OMSA is installed or updated for 11th generation servers.
- The SNMP trap destination of the host is not configured to the OMIVV appliance IP address. The failure in SNMP trap destination setting might be when iDRAC or host credentials provided in connection profile is invalid, or there are no free slots in iDRAC, or iDRAC Lockdown Mode is turned on—only in 14th generation hosts.
- OMIVV fails to enable the WBEM service on hosts running ESXi 6.5.

△ **CAUTION: Hosts in Lockdown Mode do not appear in compliance checks, even if they are noncompliant. They do not display because their compliance status cannot be determined. Ensure to check the compliance of these systems manually. In such a scenario, a warning message is displayed.**

You can run the fix noncompliant vSphere hosts wizard to fix noncompliant hosts. Some noncompliant ESXi hosts require reboots. An ESXi host reboot is required, if OMSA must be installed or updated. In addition, a reboot is required on any host that has never run CSIOR. If you select to automatically reboot an ESXi host, the following actions take place:

- For a CSIOR status fix:

  If CSIOR has never run on the host, CSIOR is set to **ON** on the host, and then the host is set into maintenance mode and rebooted.

- For hosts that does not have OMSA installed, or is running an unsupported version of OMSA:
  - OMSA is installed on the host.
  - The host is set to maintenance mode and rebooted.
  - After reboot is complete, OMSA is configured for the changes to take effect.
  - The host comes out of maintenance mode.
  - The inventory is run to refresh data.

- For an OMSA status fix where supported version of OMSA is installed, but musts be configured:
  - OMSA is configured on the host.
  - The inventory is run to refresh data.

To view and fix the noncompliant hosts:

1. In OpenManage Integration for VMware vCenter, from the **Manage** tab, click **Compliance** > **vSphere Hosts**.
   a. In the **vSphere Hosts** page, view the list of noncompliant hosts.

      A table is displayed that lists the noncompliant hosts along with the host IP or host name, model, connection profile, the CSIOR status, OMSA status, WBEM status, SNMP trap status, hypervisor, and the iDRAC license status.

   b. To view further details of a noncompliant host, select a noncompliant host.
   c. To swap the columns within the table, drag and drop columns within the data grid.
2. To fix noncomplaint hosts, click **Fix non-compliant vSphere Hosts**.

   The **Fix Non-compliant vSphere Hosts** wizard is launched. This is a dynamic wizard and only those pages are displayed that are related to the selected noncompliant hosts.

   If all the selected noncompliant hosts are CSIOR-compliant, you can view the **Turn On CSIOR** page in the wizard.
3. In the **Fix Non-compliant vSphere Hosts** wizard, click **Next** in the **Welcome** page.
4. In the **Select vSphere Hosts to the Fix Compliance wizard** page, select the check boxes for the hosts you want to fix.

   **NOTE:** The hosts present in an MX chassis with an iDRAC IPv4 disabled has to be managed using chassis profile. To associate these hosts to chassis profile, you have to add the chassis using **Add MX Chassis** in the **Chassis Summary** page and associate the chassis to a chassis profile.
5. Click **Next**.
   A warning message is displayed, if there are selected hosts that are not assigned to a connection profile and prompts you to either continue with the compliance wizard or cancel the fix compliance wizard. To fix the connection profile noncompliance, do any one of the following:
   - To exclude the hosts without the connection profile assigned to it from the compliance wizard, click **Continue Compliance Wizard**.
   - To exit the wizard and fix the systems from the **Connection Profile** page, click **Cancel**. See Creating connection profile on page 34. After connection profile is created, you can return to the wizard.
6. If you click **Continue Compliance Wizard** for the warning message, in the **Turn On CSIOR** window, select the check boxes to turn on **CSIOR** for the selected hosts.
7. Click **Next**.
8. In the **Fix OMSA** window, select the check boxes to fix **OMSA** for the selected hosts.
9. Click **Next**.
10. In the **Reboot Hosts** window, view the ESXi hosts that must be rebooted.

    An ESXi host reboot is required, if OMSA is installed or updated. In addition, a reboot is required on any host that has never run CSIOR. Do one of the following:
    - If you want to automatically put hosts in maintenance mode and reboot when required, select the **Automatically put hosts in maintenance mode and reboot whenever required** check box.
    - If you want to reboot manually, reboot the host after installing OMSA, configure OMSA manually or through the compliance wizard after the host is running and if OMSA is not configured, and run the inventory again. See Running Inventory Jobs.
11. Click **Next**.
12. In the **Summary** window, review the actions that take place on the noncompliant hosts.
    Manual reboots are required for actions in the summary page to take effect.
13. Click **Finish**.

The wizard configures the SNMP trap destination status to **Configured** after you fix the iDRAC or host credentials by providing valid information in connection profile, or make any one of the first four slots available in the iDRAC trap destination, or disable System Lockdown Mode in iDRAC.

**NOTE:** System Lockdown Mode is applicable only for 14th generation servers.

If hosts with WBEM noncomplaince exist, ensure to manually fix the conditions for those hosts that caused the WBEM service enablement to fail. You can fix the error conditions by viewing them in the user logs, and then allowing OMIVV to enables the WBEM service for those hosts during inventory.

## Fixing iDRAC license compliance for vSphere hosts

The vSphere hosts listed in the vSphere host compliance pages are noncompliant because they do not have a compatible iDRAC license. The table displays the status of the iDRAC license. You can click a noncomplaint host to view more details such as, how many days are remaining for the iDRAC license, and then you can update it, as required. The **Run inventory job** link is active if the iDRAC compliance status is "non-compliant" or "Unknown" for any one of the host associated to a connection profile.

1. In OpenManage Integration for VMware vCenter, from the **Manage** tab, click **Compliance** > **vSphere Hosts**.
2. Select a host where **iDRAC License Status** is **Non-compliant**.
3. If license is out of date, click the **Purchase/Renew iDRAC License** link.
4. Log in to the **Dell License Management** page and update or purchase a new iDRAC license.
   Use the information in this page to identify and update your iDRAC.
5. After you install an iDRAC license, run an inventory job for the vSphere host and return to this page after the inventory job is successfully complete for the host to be compliant.

# Support for OEM servers

OEM servers are supplied by Dell EMC partners, who offer features or portfolios similar to PowerEdge servers.

- From OMIVV 4.3 onwards, OEM Rack and Tower servers are supported.
- Onboard OEM servers by using the **Add OEM Hosts** wizard. For more information about adding OEM hosts, see Adding OEM hosts on page 132.

  **NOTE:** If the WBEM service is already enabled on the OEM hosts and is added to vCenter, by default, OMIVV adds those OEM servers to the OMIVV–managed list. Associate the hosts to the connection profile to manage these servers. For more information about creating a connection profile, see Creating connection profile on page 48.
- After onboarding, all the host management processes will be similar to how Dell EMC PowerEdge servers are managed.
- Bare-metal and hypervisor flows are also supported on OEM servers by using iDRAC.

# Adding OEM hosts

Along with Dell EMC PowerEdge servers, OMIVV also supports rebranded and debranded servers. For more information about OEM, see https://www.dellemc.com.

**NOTE:** If the WBEM service is already enabled, OMIVV determines the iDRAC connectivity of the host. If the connection is available, OMIVV adds the host to the managed list. If OMIVV is unable to determine, you must manually select the host on the **Add OEM Hosts** wizard so that the host is added to the OMIVV-managed list.

**NOTE:** If the WBEM service is disabled or iDRAC is not reachable, use **Add OEM Hosts** wizard so that the host is added to the OMIVV-managed list.

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Compliance** > **vSphere Hosts** > **Add OEM Hosts**.
2. In the **Add OEM Hosts** window, from the **vCenter Instance** drop-down list, select a vCenter.
3. From the **Connection Profile** drop-down list, select the connection profile.
4. To add or remove the associated host, click ➕.
   The **Select Hosts** window is displayed.
5. In the **Select Hosts** window, select the hosts and click **YES**.

   **NOTE:** Only the hosts that are not managed by OMIVV are displayed in the **Select Hosts** window.

   OMIVV tests the connection automatically, and the hosts are displayed in the **Add OEM Hosts** window.

   The **Credentials to Test** column displays the test connection result for **iDRAC Credentials** and **Host Credentials**.

   - ✅—Indicates that the test connection is successful.
   - ❌—Indicates that the test connection is failed.

To stop all the test connections, click ✋.

6. Click **Finish**.
   The selected hosts are added to the selected connection profile and inventory will be triggered.

# Viewing baseline compliance

The **Baseline Compliance** page displays the baseline compliance status based on the drift detection for all OMIVV-managed vSAN hosts associated with the Cluster profile.

- Configuration Compliance—Displays the drift in attributes between the System profile used in the Cluster profile and the associated vSAN hosts.
- Firmware and Driver Compliance—Displays the firmware and driver version drift between the Firmware and/or Driver Repository Profiles used in the Cluster profile and the associated vSAN hosts.

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Compliance** > **Baseline Compliance**.
   A table is displayed that lists the non-compliant hosts that are associated with the baseline along with the host IP or FQDN, vCenter IP or FQDN, cluster name, cluster profile name, configuration compliance status, firmware compliance status, and driver compliance status.

   **NOTE:** Only non-compliant hosts are displayed on the **Baseline Compliance** page.

   The compliance categories are:

   - **Compliant**—Indicates that the components in the host comply with the associated profiles in baseline.
   - **Non-compliant**—Indicates that the components in the host do not comply with the associated profiles in baseline.
   - **Not Applicable**—Indicates that firmware, or driver, or System profiles are not associated to the cluster profile.

   a. To view further details of a host, select a desired host.

      You can view the **HostName** and **Last Drift Detection Time** in the bottom pane.

   b. To swap the columns within the table, drag columns within the data grid.

   c. To filter the content of the data grid, use **Filter**.

   **NOTE:** You can view the following information about the **Baseline Compliance** page:

   - Total number of non-compliant hosts
   - Total number of non-compliant clusters
   - Total number of hosts and clusters that are associated with the baseline
   - Total number of non-compliant hosts distributions of drift type

2. After a successful drift detection job, the hosts that are associated with the baseline are listed in the table. To view the drift details, select a desired host, and click **Show Drift Details**.
   The **Drift Details** dialog box is displayed.
3. In the **Drift Details** dialog box, you can view the following:
   - If the compliance drift detection job fails, the compliance status is displayed as "non-compliant" along with the reason for failure. Use the reason indicated to resolve the issue.
   - If the drift detection job is successful, the compliance status is displayed as "non-compliant" and the following details are displayed on the **Drift Details** page:

     For Hardware:

     - Instance—Indicates the hardware component name.
     - Group—Indicates the group name of the attributes.
     - Attribute Name—Indicates the attribute name.
     - Current Value—Indicates the host value.
     - Baseline Value—Indicates the baseline value.
     - Drift Type—Indicates the reason for non-compliance. For more information about the drift type, see Component vs. baseline version comparison matrix on page 167.

     For Firmware and Driver:

     - Component Name—Indicates the name of the component.
     - Current Value—Indicates the host value.
     - Baseline Value—Indicates the baseline value.
     - Drift Type—Indicates the reason for non-compliance. For more information about the drift type, see Component vs. baseline version comparison matrix on page 167.

    - Criticality(for firmware)—Indicates the importance level of updating the version of an identified component.
    - Recommendation(for driver)—Indicates the importance level of updating the version of an identified component.
    - Reboot required—Indicates whether the appliance reboot is required or not.

    **NOTE:** If more than one version of firmware is available, the latest firmware version is always used for compliance comparison.

4. Click **Finish**.

# Using OMSA with 11th generation servers

To manage the PowerEdge 11th generation servers, OMIVV requires OMSA to be running on them. For an 11th generation host that is deployed though OMIVV, OMSA is installed automatically. For 11th generation hosts that you deploy manually, you can choose either of the following:

- Install and configure OMSA using OMIVV. See Setting up OMSA trap destination on page 134.
- Install and configure OMSA manually. See Deploying OMSA agent on the ESXi system on page 134.

**NOTE:** When deploying the OMSA agent using OMIVV, OMIVV starts the HttpClient service and enables port 8080 and releases after ESXi 5.0 to download OMSA VIB and install it. Once the OMSA installation is completed, the service automatically stops and the port is closed.

**NOTE:** Apart from the preceding options, you can use the web client host compliance, which installs and configures the OMSA agent.

## Deploying OMSA agent on the ESXi system

Install the OMSA VIB on an ESXi system to gather inventory and alert information from the systems.

**NOTE:** OpenManage agents are required on Dell hosts that are earlier than Dell PowerEdge 12th generation servers. Install OMSA using OpenManage Integration for VMware vCenter or install OMSA manually to hosts before installing OpenManage Integration for VMware vCenter.

1. If OMSA is not installed, install the vSphere command line tool (vSphere CLI) from **www.vmware.com**.
2. Enter the following command:

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

    **NOTE:** It might take a few minutes for OMSA to install. This command requires you to reboot the host after it completes.

    **NOTE:** SNMP community string can be configured from **Manage** > **Settings** > **Appliance Settings** > **OMSA SNMP Trap Community String**.

## Setting up OMSA trap destination

All 11th generation of hosts must have OMSA configured.

**NOTE:** OMSA is only required for the Dell EMC servers earlier than 12th generation PowerEdge servers.

To set up an OMSA trap destination:

1. Navigate to the OMSA agent from a web browser by providing the `https://<HostIP>:1311/` as its URL.
2. Log in to the interface, and select the **Alert Management** tab.
3. Select **Alert Actions** and ensure that any events to be monitored have the **Broadcast Message** option set, so that the events are posted.
4. Select the **Platform Events** option at the top of the tab.
5. Click the grey the **Configure Destinations** button, and click the **Destination** link.
6. Select the **Enable Destination** check box.
7. Enter the OMIVV appliance IP address in the **Destination IP Address** field.

8. Click **Apply Changes**.
9. Repeat step 1 to step 8 to configure extra events.

   **NOTE:** SNMP community string can be configured from **Manage** > **Settings** > **Appliance Settings** > **OMSA SNMP Trap Community String**. For more information about SNMP trap community string, see the Configuring SNMP trap community string.

# Reporting and fixing compliance for bare-metal servers

A bare-metal server is noncompliant when:

- It is not a supported server.
- It does not have a supported iDRAC license (iDRAC Express is the minimum requirement).
- It does not have supported versions of iDRAC, BIOS, or LC.
- LOM or rNDC is not present.
- System Lockdown Mode is turned on.

To view and fix the list of noncompliant bare-metal servers:

1. In OpenManage Integration for VMware vCenter, select the **Manage** > **Deployment** tab.
   a. In the **Bare Metal Servers** page, view the list of noncompliant servers.

      A table is displayed that lists the noncompliant servers along with the Service Tag, model, iDRAC IP, server status, System Lockdown Mode, compliance status, and the iDRAC license status.

   b. To view further details of a server, select a noncompliant server.

   c. To export the noncomplaint information of a server to a .CSV file, in the right-hand corner of the table, click 📤.

   d. To filter the content of the data grid, click the **Filter** field.

   e. To swap the columns within the table, drag and drop columns within the data grid.
2. To fix noncomplaint servers, click **Fix non-compliant servers**.

   **NOTE:** The **Fix non-compliant servers** link is only enabled for 11th generation noncompliant servers.

3. In the **Fix bare metal Compliance** wizard, click **Next** in the **Welcome** page.
4. In the **Fix Compliance** page, select the check boxes for the servers you want to fix.

   The noncomplaint servers are listed and the firmware component for which it is noncompliant is displayed. The listed noncompliant servers require updating at least one of the following firmware components:

   - **iDRAC IP**

     **NOTE:** From OMIVV, you cannot fix bare-metal servers where the iDRAC licenses are noncompliant. Ensure that you upload supported iDRAC license to those servers outside OMIVV, and then click **Refresh Baremetal Servers**. SeeRefreshing bare-metal servers on page 136.

   - **BIOS**
   - **LC**
   - **System Lockdown Mode**

     **NOTE:** To view latest details of the noncomplaint bare-metal servers from the corresponding iDRAC, click**Refresh Bare Metal details**. If System Lockdown Mode is turned on, the server is noncomplaint, and conversely.

5. To view compliance issue details, click **Compliance Issues**.

   **NOTE:** If a bare-metal server is noncomplaint due to System Lockdown Mode being turned on, ensure that you manually configure the System Lockdown Mode of the server from the iDRAC console.

6. Click **Next**.
7. In the **Summary** window, review the actions that take place on the firmware components of noncompliant bare-metal servers.
8. Click **Finish**.

## Fixing iDRAC license compliance for bare-metal servers

The bare-metal servers listed in the **Bare Metal Servers** page are noncompliant because they do not have a compatible iDRAC license. A table displays the status of the iDRAC license. You can click a noncomplaint bare-metal server to view more details such as, how many days are remaining for the iDRAC license, and then you can update it, as required. If the **Refresh Baremetal Servers** link is enabled in the **Bare Metal Servers** page, there are bare-metal servers that are noncompliant due to the iDRAC license.

1. In OpenManage Integration for VMware vCenter, select the **Manage** > **Deployment** tab.
   In the **Bare Metal Servers** page, view the list of noncompliant servers that is displayed in a table.
2. Select a bare-metal server where **iDRAC License Status** is **Non-compliant** or **Unknown**.
3. If license is out of date, click the **Purchase/Renew iDRAC License** link.
4. Log in to the **Dell License Management** page and update or purchase a new iDRAC license.
   Use the information in this page to identify and update your iDRAC.
5. After you install an iDRAC license, click **Refresh Baremetal Servers**.

## Refreshing bare-metal servers

1. On the **OpenManage Integration for VMware vCenter** page, click **Manage** > **Deployment** > **Bare Metal Servers**, and then click **Refresh Baremetal Servers**.
2. In the **Refresh Baremetal Servers** window, select the servers that you want to refresh the data, and then click **Refresh Selected Servers**.

Refreshing bare-metal servers data may take few minutes.

All the selected bare-metal servers data is refreshed on the **Bare Metal Servers** page.

15

# Security roles and permissions

The OpenManage Integration for VMware vCenter stores user credentials in an encrypted format. It does not provide any passwords to client applications to avoid any improper requests. The backup database is fully encrypted by using custom security phrases, and hence data cannot be misused.

By default, users in the Administrators group have all the privileges. The Administrators can use all the functions of the OpenManage Integration for VMware vCenter within VMware vSphere web client. If you want a user with necessary privileges to manage the product, do the following:

1. Create a role with necessary privileges.
2. Register a vCenter server by using the user.
3. Include both the Dell roles, Dell operational role and Dell infrastructure deployment role.

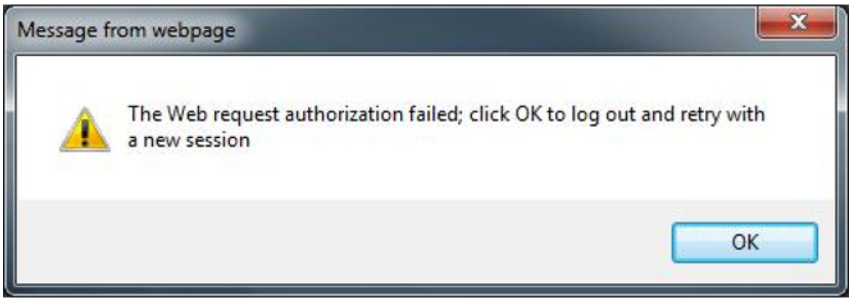
**Topics:**

- Data integrity
- Access control authentication, authorization, and roles
- Dell Operational role
- Dell Infrastructure Deployment role
- About privileges

## Data integrity

The communication between the OpenManage Integration for VMware vCenter, Administration Console, and vCenter is accomplished by using SSL/HTTPS. The OpenManage Integration for VMware vCenter generates an SSL certificate that is used for trusted communication between vCenter and the appliance. It also verifies and trusts the vCenter server's certificate before communication and the OpenManage Integration for VMware vCenter registration. The console tab of OpenManage Integration for VMware vCenter uses security procedures to avoid improper requests while the keys are transferred back and forth from the Administration Console and back-end services. This type of security causes cross-sites request forgeries to fail.

A secure Administration Console session has a 5-minutes idle time-out, and the session is only valid in the current browser window and/or tab. If you try to open the session in a new window or tab, a security error is prompted that asks for a valid session. This action also prevents the user from clicking any malicious URL that can attack the Administration Console session.



The Web request authorization failed; click OK to log out and retry with a new session

**Figure 3. Security error message**

## Access control authentication, authorization, and roles

To perform vCenter operations, OpenManage Integration for VMware vCenter uses the current user session of web client and the stored administration credentials for the OpenManage Integration. The OpenManage Integration for VMware vCenter uses the vCenter server's built-in roles and privileges model to authorize user actions with the OpenManage Integration and the vCenter managed objects (hosts and clusters).

# Dell Operational role

The role contains the privileges/groups to accomplish appliance and vCenter server tasks including firmware updates, hardware inventory, restarting a host, placing a host in maintenance mode, or creating a vCenter server task.

This role contains the following privilege groups:

**Table 38. Privilege groups**

| Group name | Description |
|---|---|
| Privilege group — Dell.Configuration | Perform Host-related tasks, Perform vCenter-related tasks, Configure SelLog, Configure ConnectionProfile, Configure ClearLed, Firmware Update |
| Privilege group — Dell.Inventory | Configure inventory, Configure warranty retrieval, Configure readonly |
| Privilege group — Dell.Monitoring | Configure monitoring, monitor |
| Privilege group — Dell.Reporting (Not used) | Create a report, Run a report |

# Dell Infrastructure Deployment role

The role contains the privileges related to the hypervisor deployment features.

The privileges this role provides are Create Template, Configure HW Configuration Profile, Configure Hypervisor Deployment Profile, Configure Connection Profile, Assign Identity, and Deploy.

**Privilege Group — Dell.Deploy-Provisioning**

Create Template, Configure HW Configuration Profile, Configure Hypervisor Deployment Profile, Configure Connection Profile, Assign Identity, Deploy

# About privileges

Every action performed by the OpenManage Integration for VMware vCenter is associated with a privilege. The following sections list the available actions and the associated privileges:

- Dell.Configuration.Perform vCenter-related tasks
  - Exit and enter maintenance mode
  - Get the vCenter user group to query the permissions
  - Register and configure alerts, for example enable/disable alerts on the event settings page
  - Post events/alerts to vCenter
  - Configure event settings on the event settings page
  - Restore default alerts on the event settings page
  - Check DRS status on clusters while configuring alerts/events settings
  - Reboot host after performing update or any other configuration action
  - Monitor vCenter tasks status/progress
  - Create vCenter tasks, for example firmware update task, host configuration task, and inventory task
  - Update vCenter task status/progress
  - Get host profiles
  - Add host to data center
  - Add host to cluster
  - Apply profile to host
  - Get CIM credentials
  - Configure hosts for compliance
  - Get the compliance tasks status
- Dell.Inventory.Configure ReadOnly
  - Get all vCenter hosts to construct the vCenter tree while configuring connection profiles
  - Check if the host is a Dell server when the tab is selected

  - Get the vCenter's Address/IP
  - Get host IP/Address
  - Get the current vCenter session user based on the vSphere client session ID
  - Get the vCenter inventory tree to display the vCenter inventory in a tree structure.
- Dell.Monitoring.Monitor
  - Get host name for posting the event
  - Perform the event log operations, for example get the event count, or change the event log settings
  - Register, unregister, and configure events/alerts — Receive SNMP traps and post events
- Dell.Configuration.Firmware Update
  - Perform firmware update
  - Load firmware repository and DUP file information on the firmware update wizard page
  - Query firmware inventory
  - Configure firmware repository settings
  - Configure staging folder and perform update by using the staging feature
  - Test the network and repository connections
- Dell.Deploy-Provisioning.Create Template
  - Configure HW Configuration Profile
  - Configure Hypervisor Deployment Profile
  - Configure Connection Profile
  - Assign identity
  - Deploy
- Dell.Configuration.Perform host-related tasks
  - Blink LED, Clear LED, Configure OMSA URL from the Dell Server Management tab
  - Launch OMSA Console
  - Launch iDRAC Console
  - Display and clear SEL log
- Dell.Inventory.Configure Inventory
  - Display system inventory in the Dell Server Management tab
  - Get storage details
  - Get power monitoring details
  - Create, display, edit, delete, and test connection profiles on the connection profiles page
  - Schedule, update, and delete inventory schedule
  - Run inventory on hosts

16

# Frequently Asked Questions-FAQ

Use this section to find answers to troubleshooting questions. This section includes:

- Frequently asked questions (FAQ)
- Bare-metal deployment issues on page 158

**Topics:**

- Frequently Asked Questions-FAQ
- Bare-metal deployment issues

## Frequently Asked Questions-FAQ

This section contains some common questions and solutions.

### Export All button fails to export to .CSV file in Google chrome

After registering a vCenter server, if you add a host and create a connection profile, and then view the inventory details of the host, the **Export All** button returns a failure. The **Export All** button does not export the information to a .CSV file.

> **NOTE:**
>
> In all versions of the Google chrome browser, the **Export All** button does not export the information to a .CSV file in **Incognito mode**.

Resolution: To export information to a .CSV file by using the **Export All** button in the Google chrome, disable the **Incognito mode** in chrome browser.

Version affected: 4.0

### iDRAC license type and description are displayed incorrectly for non-compliant vSphere hosts

If a host is noncomplaint when CSIOR is disabled or has not been run, iDRAC license information is displayed incorrectly although valid iDRAC license is available. Hence, you can view the host in vSphere hosts list, but when you click the host for details, the information in **iDRAC License Type** is displayed as empty and **iDRAC License Description** is displayed as ”Your license needs to be upgraded".

Resolution: To fix this issue, enable CSIOR on a reference server.

Version affected: 4.0

### Dell provider is not displayed as health update provider

When you register a vCenter server with OMIVV and then upgrade the vCenter server version, such as from vCenter 6.0 to vCenter 6.5, the Dell provider is not displayed in the **Proactive HA provider** list.

Resolution: You can upgrade a registered vCenter for non-administrator users or administrator users. To upgrade to the latest version of the vCenter server, see the VMware Documentation and then perform either of the following options, as applicable:

- For non-administrator users:
  1. Assign extra privileges to non-administrator users, if necessary. See Required privileges for non-administrator users on page 13.
  2. Reboot the registered OMIVV appliance.

3. Log out from web client and then log in again.

- For administrator users:
  1. Reboot the registered OMIVV appliance.
  2. Log out from web client and then log in again.

The Dell provider is now listed in the **Proactive HA provider** list.

Version affected: 4.0

# Inventory failing when performing firmware update task on ESXi 5.x host

After registering a vCenter server, if you perform firmware update task on an ESXi 5.x host and select iDRAC as the component from the **Select Component** screen, the ESXi in the host might not be synchronized with the new iDRAC IP, thereby resulting in an invalid iDRAC IP provided to OMIVV. Hence, you cannot run inventory successfully on that host.

Resolution: To resolve this issue, restart the sfcdb daemon on the ESXi host. See https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2077693 for more information.

Version affected: 4.0

# Host inventory or test connection fails due to invalid or unknown iDRAC IP.

The host inventory or test connection fails due to invalid or unknown iDRAC IP and you receive messages such as "network latencies or unreachable host", "connection refused", "operation has timed out", "WSMAN", "no route to host", and "IP address: null".

1. Open the iDRAC virtual console.
2. Press F2 and navigate to **Troubleshooting Options**.
3. In **Troubleshooting Options**, navigate to **Restart Management Agents**.
4. To restart the management agents, press F11.

A valid iDRAC IP is now available.

**NOTE:** Host inventory can also fail when OMIVV fails to enable WBEM services on hosts running ESXi 6.5. See Creating connection profile on page 48 for more information about WBEM service.

# On running fix noncompliant vSphere hosts wizard, the status of a specific host is displayed as Unknown

When you run the fix noncompliant vSphere hosts wizard to fix noncompliant hosts, the status of a specific host is displayed as "Unknown". The unknown status is displayed when iDRAC is not reachable.

Resolution: Verify the iDRAC connectivity of the host and ensure that inventory is run successfully.

Version affected: 4.0

# Dell privileges that are assigned while registering the OMIVV appliance are not removed after unregistering OMIVV

After registering vCenter with an OMIVV appliance, several Dell privileges are added to the vCenter privilege list. Once you unregister vCenter from the OMIVV appliance, the Dell privileges are not removed.

**NOTE:** Although the Dell privileges are not removed, there is no impact to any OMIVV operations.

Version Affected: 3.1

# OMIVV does not display all the relevant logs when trying to filter a severity category

When you select a severity category to filter the log data by choosing **All Categories** from the drop-down, all the logs belonging to specific category are displayed accurately. However, if you filter by choosing **Info** from the drop-down, the Firmware update logs are not displayed and only the task initiation logs are displayed.

Resolution: To view all the logs in OMIVV, select **All Categories** from the Filter drop-down.

Version Affected: 3.1

# How do I resolve error code 2000000 caused by VMware Certificate Authority-VMCA

When you run the vSphere certificate manager and replace the vCenter server or Platform Controller Service (PSC) certificate with a new CA certificate and key for vCenter 6.0, OMIVV displays error code 2000000 and throws an exception.

Resolution: To resolve the exception, you should update the ssl Anchors for the services. The ssl Anchors can be updated by running the `ls_update_certs.py` scripts on PSC. The script takes the old certificate thumbprint as the input argument and the new certificate is installed. The old certificate is the certificate before the replacement and the new certificate is the certificate after the replacement. Visit https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 and https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689 for more information.

## Updating the ssl Anchors in Windows vSphere 6.0

1. Download the lstoolutil.py.zip file from https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701.
2. Copy the lstoolutil.py file to the `%VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\` folder.

   **NOTE:** Do not replace the lstoolutil.py file if you are using vSphere 6.0 Update 1.

You can use the following relevant procedures to update the ssl Anchors:

- Updating the ssl Anchors for vCenter installed on Windows operation system: Replace the certificates on vCenter Windows installation by using vSphere Certificate Manager utility. See Replacing the certificates on vCenter Windows installation on page 142.
- Updating the ssl Anchors for the vCenter server appliance: Replace the certificates on vCenter server appliance by using vSphere Certificate Manager utility. See Replacing the certificates on the vCenter server appliance on page 143.

The output obtained from the mentioned procedures should display `Updated 24 service (s)` and `Updated 26 service (s)` respectively. If the output displayed is `Updated 0 service (s)`, the old certificate thumbprint is incorrect. You can perform the following steps to retrieve the old certificate thumbprint. Also, use the following procedure to retrieve the old certificate thumbprint, if **vCenter Certificate Manager** is not used to replace the certificates:

**NOTE:** Run the `ls_update_certs.py` with the old thumbprint obtained.

1. Retrieve the old certificate from the Managed Object Browser (MOB). See Retrieving the old certificate from Managed Object Browser-MOB on page 144.
2. Extract the thumbprint from the old certificate. See Extracting thumbprint from the old certificate on page 145.

Version Affected: 3.0 and later, vCenter 6.0 and later

# Replacing the certificates on vCenter Windows installation

Perform the following steps if vSphere Certificate Manager utility is used to replace the certificates on vCenter Windows installation:

1. Connect to External Platform Services Controller through remote desktop connection.
2. Open command prompt in administrative mode.
3. Create the `c:\certificates` folder by using the following command: `mkdir c:\certificates`

4. Retrieve the old certificate by using the following command: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt`
5. Retrieve the old certificate thumbprint by using the following command: `"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

   **NOTE:** The retrieved certificate thumbprint is in the following format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   The thumbprint is a sequence of numbers and alphabets which appears as follows:`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

6. Retrieve the new certificate by using the following command: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
7. Perform the following steps:
   a. Run `ls_update_certs.py` by using the following command. `"%VMWARE _PYTHON_BIN%" ls_update_certs.py --url`
   b. Replace psc.vmware.com by Lookup_Service_FQDN_of_Platform_Services_Controller and the 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 thumbprint with the thumbprint obtained in step 5 by using the following command: `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`

      **NOTE:** Ensure to provide valid credentials.

8. Log out and log in to the vCenter Web client after all the services are updated successfully.

OMIVV now launches successfully.

## Replacing the certificates on the vCenter server appliance

Perform the following steps if vSphere Certificate Manager utility is used to replace the certificates on the vCenter server appliance:

1. Log in to the External Platform Services Controller appliance through console or a secure shell (SSH) session.
2. Run the following command to enable accessing the Bash shell: `shell.set --enabled true`
3. Type **`shell`** and press **Enter**.
4. Create folders or certificates by using the following command: `mkdir /certificates`
5. Retrieve the old certificate by using the following command: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt`
6. Retrieve the old certificate thumbprint by using the following command: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

   **NOTE:** The retrieved certificate thumbprint is in the following format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   The thumbprint is a sequence of numbers and alphabets which appears as follows:`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

7. Retrieve the new certificate by using the following command:`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`
8. Run the following command to change the directory: `cd /usr/lib/vmidentity/tools/scripts/`
9. Perform the following steps:
   a. Run `ls_update_certs.py` by using the following command. `python ls_update_certs.py --url`
   b. Replace psc.vmware.com by Lookup_Service_FQDN_of_Platform_Services_Controller and the 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 thumbprint with the thumbprint obtained in step 6 by using the following command: `https://psc.vmware.com/lookupservice/sdk --fingerprint`

```
13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/
new_machine.crt --user Administrator@vsphere.local --password "Password"
```

**NOTE:** Ensure to provide valid credentials.

10. Log out and log in to the vCenter Web client after all the services are updated successfully.

OMIVV now launches successfully.

## Retrieving the old certificate from Managed Object Browser-MOB

You can retrieve the old certificate for the vCenter server system by connecting to Platform Service Controller (PSC) by using the Managed Object Browser (MOB).

To retrieve the old certificate, you should find the sslTrust field of the ArrayOfLookupServiceRegistrationInfo managed object by performing the following steps:

**NOTE:** In this guide, the `C:\certificates\` folder location is used to store all certificates.

1. Create the `C:\certificates\` folder on PSC by using the following command: `mkdir C:\certificates\`.
2. Open the following link in a browser: `https://<vCenter FQDN|IP address>/lookupservice/mob?moid=ServiceRegistration&method=List`
3. Log in with the `administrator@vsphere.local` user name and provide the password when prompted.

   **NOTE:** If you are using a custom name for vCenter Single Sign-On (SSO) domain, use that user name and password.

4. In **filterCriteria**, modify the value field to show only the tags **<filtercriteria></filtercriteria>** and click **Invoke Method**.
5. Search for the following hostnames depending on the certificates that you are replacing:

### Table 39. Search criteria information

| Trust anchors | Search criteria |
|---|---|
| vCenter server | Use Ctrl+F to search, vc_hostname_or_IP.example.com on the page |
| Platform Services Controller | Use Ctrl+F to search, psc_hostname_or_IP.example.com on the page |

6. Locate the value of the corresponding sslTrust field. The value of the sslTrust field is Base64 encoded string of the old certificate.
7. Use the following examples when updating the Platform Services Controller or vCenter Server trust anchors.

   **NOTE:** The actual string is shortened significantly to improve legibility.

   - For vCenter server

### Table 40. vCenter server example

| Name | Type | Value |
|---|---|---|
| url | anyURI | https://vcenter.vmware.local:443/sdk |

   - For Platform Services Controller

### Table 41. Platform Services Controller example

| Name | Type | Value |
|---|---|---|
| url | anyURI | https://psc.vmware.local/sts/STSService/vsphere.local |

8. Copy the content of the sslTrust field into a text document and save the document as `old_machine.txt`.
9. Open the `old_machine.txt` in a text editor.
10. Append the following at the starting and end of the `old_machine.txt` file respectively:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

11. Save `old_machine.txt` now as `old_machine.crt`.

You can now extract the thumbprint from this certificate.

# Extracting thumbprint from the old certificate

You can extract the thumbprint from the old certificate and upload it to the Platform Services by using the following options:

- Extract the thumbprint by using a Certificate Viewer Tool. See Extracting the certificate thumbprint by using a Certificate Viewer tool on page 145.
- Extract the thumbprint by using a command line on the appliance. See Extracting Thumbprint by using the command line on page 145.

## Extracting the certificate thumbprint by using a Certificate Viewer tool

Perform the following steps to extract the certificate thumbprint:

1. In Windows, double-click the `old_machine.txt` file to open it in Windows Certificate Viewer.
2. In Windows Certificate Viewer, select the **SHA1 Thumbprint** field.
3. Copy the thumbprint string into a plain text editor and replace the spaces with colons or remove the spaces from the string. For example, the thumbprint string can appear as either of the following:
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

## Extracting Thumbprint by using the command line

You can see the following sections for extracting thumbprint by using the command line on the appliance and Windows installation.

### Extracting thumbprint by using the Command Line on the vCenter server appliance

Perform the following steps:

1. Move or upload the old_machine.crt certificate to PSC in the `C:\certificates\old_machine.crt` location that is created in step 1 of retrieving the old certificate procedure. You can use Windows Secure Copy (WinSCP) or another SCP client to move or upload the certificate.
2. Log in to the External Platform Services Controller appliance through Secure Shell (SSH).
3. Run the following command to enable accessing the Bash shell: `shell.set --enabled true`.
4. Type `shell` and press **Enter**.
5. Run the following command to extract the thumbprint: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

**NOTE:** The thumbprint appears as a sequence of numbers and letters after the equal sign, which is as follows: `SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`

### Extracting thumbprint by using the Command Line on Windows installation

Perform the following steps:

1. Move or upload the old_machine.crt certificate to PSC in the `C:\certificates\old_machine.crt` location that is created in step 1 of retrieving the old certificate procedure. You can use Windows Secure Copy (WinSCP) or another SCP client to move or upload the certificate.
2. Connect to External Platform Services Controller through remote desktop connection.
3. Open command prompt in administrative mode.
4. Run the following command to extract the thumbprint: `"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

**NOTE:** The thumbprint appears as a sequence of numbers and letters after the equal sign, which is as follows: `SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`

Run the ls_update_certs.py with the old thumbprint. Log out and log in to the vCenter Web client after the services are updated successfully. The Dell plug-in launches successfully.

## In Administration Console, Update Repository Path is not set to default path after I reset appliance to factory settings

After you reset the appliance, go to the **Administration Console**, and then click **APPLIANCE MANAGEMENT** in the left pane. In the **Appliance Settings** page, the **Update Repository Path** is not changed to the default path.

**Resolution:** In **Administration Console**, manually copy the path in the **Default Update Repository** field to the **Update Repository Path** field.

## Warranty and inventory schedule for all vCenters is not applying when selected from the job queue page

Navigate to **Dell Home** > **Monitor** > **Job Queue** > **Warranty/Inventory History** > **Schedule**. Select a vCenter and select the modify schedule button. When a dialog is displayed, you can view a check box with the **Apply to All Registered vCenters** message. When you select the check box and press **Apply**, the setting is applied to a particular vCenter that you had initially selected and not all vCenters. The **Apply to All Registered vCenters** is not applicable when warranty or inventory schedule is modified from the **Job Queue** page.

Resolution: Use the modify warranty or inventory schedule from the job queue only to modify the selected vCenter.

Versions Affected: 2.2 and later

## What should I do when a web communication error in the vCenter web client appears after changing the DNS settings in OMIVV

If you see any kind of web communication error in the vCenter web client while doing any OMIVV-related tasks after changing the DNS settings, do either of the following:

- Clear the browser cache.
- Log out and then log in from web client.

## The settings page fail to load, if I navigate away and again go back to the settings page

For vSphere v5.5, in web client, if you navigate away and go back to the **Settings** page, the page might fail to load and the spinner continues to spin. The failure to load is a refresh issue and the page is not refreshing correctly.

Resolution: Click the global refresh and the screen refreshes correctly.

Versions Affected: 2.2 and 3.0

## Task cannot be scheduled for the time in the past- error in inventory schedule and warranty schedule page of Initial Configuration Wizard appear

In web client, the error “Task cannot be scheduled for the time in the past” appears:

- if you select ‘All registered vCenters’ in the Initial Configuration wizard, and there are some vCenters with no hosts.
- when vCenters where some have inventory or warranty tasks already scheduled.
- when some vCenters with no inventory or warranty schedule set yet.

Resolution: Run the setting of inventory and warranty schedule separately again from the **Settings** page for the vCenters.

Versions Affected: 2.2 and later

## Installation date appears as 12-31-1969 for some of the firmware on the firmware page

In web client, the installation date appears as 12/31/1969 for some firmware items on the firmware page for a host. If the firmware installation date is not available, the old date is displayed.

Resolution: If you see this old date for any firmware component, consider that the installation date is not available for it.

Versions Affected: 2.2 and later

## Successive global refresh cause exception to be thrown in the recent task window.

If you try to press the refresh button repeatedly, the VMware UI might throw an exception.

Resolution:  You can dismiss this error and can continue.

Version Affected: 2.2 and later

## Why is web client UI distorted for few Dell screens in IE 10

Sometimes when a popup dialog is displayed, the data in the background might become white and is distorted.

Resolution: Close the dialog box; the screen returns back to normal.

Version Affected: 2.2 and later

## I am not seeing OpenManage Integration icon in web client even if registration of plug-in to vCenter was successful

OpenManage Integration icon is not displayed in the web client unless the vCenter web client services are restarted. When you register the OpenManage Integration for VMware vCenter appliance, the appliance is registered with the web client. If you unregister the appliance and then either re-register the same version or register a new version of the appliance, it successfully registers, but the OMIVV icon may not appear in the web client. This is due to a caching issue from VMware. To clear the issue, ensure that you restart the web client service on the vCenter Server. Then the plug-in is displayed in the UI.

Resolution: Restart the web client service on the vCenter server.

Version Affected: 2.2 and later

## Even if repository has bundles for selected 11G system, firmware update displaying that there are no bundles for firmware update

When the host is added to the connection profile in lockdown mode, the inventory kicks off but fails stating that “No Remote Access Controller was found or Inventory is not supported on this host.” Inventory is supposed to work for a host in lockdown mode.

If you put the host in lockdown mode or remove a host from lockdown mode, ensure that you wait for 30 minutes before performing the next operation. If you use a 11G host for firmware update, the firmware update wizard does not display any bundles even if the repository has bundles for that system. This occurs because the 11G host might have not been configured for OMSA to send traps to OpenManage Integration.

Resolution: Ensure that the host is compliant by using the host compliance wizard of the OpenManage Integration web client. If it is not compliant, use the Fix Host Compliance to get it compliant.

Version Affected: 2.2 and later

## Why is DNS configuration settings restored to original settings after appliance reboot if appliance IP and DNS settings are overwritten with DHCP values

There is a known defect where statically assigned DNS settings are replaced by values from DHCP. This can happen when DHCP is used to obtain IP settings, and DNS values are assigned statically. When the DHCP lease is renewed or the appliance is restarted, the statically assigned DNS settings are removed.

Resolution: Statically assign IP settings when the DNS server settings are different from DHCP.

Version Affected: All

## Using OMIVV to update the Intel network card with firmware version of 13.5.2 is not supported

There is a known issue with the Dell PowerEdge 12th generation servers and some Intel network cards with the firmware version of 13.5.2. Updating some models of Intel network cards at this version of firmware fails when the firmware update is applied by using the Lifecycle Controller. Customers with this version of firmware must update the network driver software by using an operating system. If the Intel network card has a version of firmware other than 13.5.2, you can update using OMIVV. For more information, see http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx

ⓘ **NOTE:** Note: When using one-to-many firmware update, avoid selecting Intel network adapters that are at version 13.5.2, as the update fails and stops the update task from updating remaining servers.

## Using OMIVV to update Intel network card from 14.5 or 15.0 to 16.x fails due to staging requirement from DUP

This is a known issue with NIC 14.5 and 15.0. Ensure that you use the custom catalog to update the firmware to 15.5.0 before updating the firmware to 16.x.

Version Affected: All

## Why trying firmware update with invalid DUP, hardware update job status on vCenter console neither fails nor times-out for hours, although job status in LC prompts as FAILED

When the invalid DUP is picked for firmware update, the status of the task in the vCenter console window remains 'In Progress' but the message is changed to the reason of failure. This is a known VMware defect and will be fixed in the future releases of VMware vCenter.

Resolution: The task must be canceled manually.

Version Affected: All

## Why does Administration Portal display unreachable update repository location

If you provide an unreachable Update Repository path, the "Failed: Error while connecting to the URL…. " error message is displayed on the top of the Appliance Update view. However, the Update Repository Path is not cleared to the value before update.

Resolution: Move out of this page to another page and ensure that the page is refreshed.

Version Affected: All

## Why did system not enter maintenance mode when I performed one-to-many firmware update

Some firmware updates do not require rebooting the host. In that case, the firmware update is performed without putting the host into maintenance mode.

## Chassis global health still healthy when some of power supply status has changed to critical

The global health of the chassis about the power supply is based on the redundancy policies and whether the chassis power needs are satisfied by the PSU that are still online and functional. So even if some of the PSU is out of power, the overall power requirement of the chassis are met. So the global health of the chassis is Healthy. For more details on the Power Supply and Power Management look in the user’s Guide for Dell PowerEdge M1000e Chassis Management Controller Firmware document.

## Processor version is displayed as “Not Applicable” in processor view in system overview page

In PowerEdge 12th Generation Dell servers and higher generations, the processor version is in the Brand column. In lower generation servers, processor version is shown in the Version column.

## Does OMIVV support vCenter in linked mode

Yes, OMIVV supports up to 10 vCenter servers either in a linked mode or not in a linked mode. For more information about how OMIVV works in linked mode, see the white paper, *OpenManage Integration for VMware vCenter: Working in Linked Mode* at www.dell.com.

## What are required port settings for OMIVV

**NOTE:** When deploying the OMSA agent by using the **Fix non-compliant vSphere hosts** link available from the **Compliance** window in OMIVV, OMIVV starts the http client service and enables port 8080 on releases after ESXI 5.5 to download the OMSA VIB and install it. After the OMSA VIB installation is complete, the service automatically stops and the port is closed.

Use the following port settings for OMIVV:

**Table 42. Virtual appliance**

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|---|---|---|---|---|---|---|---|
| 53 | DNS | TCP | None | Out | OMIVV appliance to DNS server | DNS client | Connectivity to the DNS server or resolving the host names. |
| 69 | TFTP | UDP | None | Out | OMIVV appliance to TFTP server | TFTP Client | Used for firmware update on 11G servers with old firmware. |
| 80 | HTTP | TCP | None | Out | OMIVV appliance to internet | Dell Online Data Access | Connectivity to the online (internet) warranty, firmware and latest RPM information. |
| 80 | HTTP | TCP | None | In | ESXi server to OMIVV appliance | HTTP server | Used in OS deployment flow for post installation scripts to communicate with the OMIVV appliance. |

Table 42. Virtual appliance

| Port Number | Protocols | Port Type | Maximum Encryption Level | Direction | Destination | Usage | Description |
|---|---|---|---|---|---|---|---|
| 162 | SNMP Agent | UDP | None | In | iDRAC/ESXi to OMIVV appliance | SNMP Agent (server) | To receive SNMP traps from managed nodes. |
| 443 | HTTPS | TCP | 128-bit | In | OMIVV UI to OMIVV appliance | HTTPS server | Web services offered by OMIVV. These Web services are consumed by vCenter Web Client and Dell Admin portal. |
| 443 | WSMAN | TCP | 128-bit | In/Out | OMIVV appliance to/ from iDRAC/ OMSA | iDRAC/OMSA communication | iDRAC, OMSA, and CMC communication, used to manage and monitor the managed nodes. |
| 445 | SMB | TCP | 128-bit | Out | OMIVV appliance to CIFS | CIFS communication | To communicate with windows share. |
| 4433 | HTTPS | TCP | 128-bit | In | iDRAC to OMIVV appliance | Auto Discovery | Provisioning server used for auto discovering managed nodes. |
| 2049 | NFS | UDP/ TCP | None | In/Out | OMIVV appliance to NFS | Public Share | NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update and OS deployment flows. |
| 4001 to<br>4004 | NFS | UDP/ TCP | None | In/Out | OMIVV appliance to NFS | Public Share | NFS public share that is exposed by OMIVV appliance to the managed nodes and used in Firmware update and OS deployment flows. |
| 11620 | SNMP Agent | UDP | None | In | iDRAC to OMIVV appliance | SNMP Agent (server) | iDRAC, OMSA, and CMC communication, used to manage and monitor the managed nodes. |
| User defined | Any | UDP/ TCP | None | Out | OMIVV appliance to proxy server | Proxy | To communicate with the proxy server |

Table 43. Managed nodes (ESXi)

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

Table 44. Managed nodes (iDRAC/CMC)

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

**NOTE:** For 14th generation PowerEdge servers, iDRAC mounts the NFS through TCP on port 2049.

# Password is not changed for user used for bare-metal discovery after successfully applying hardware profile or system profile that has same user with new changed credentials in iDRAC user list

The password of the user used from discovery is not changed to the new credential if only hardware profile or system profile template is selected for deployment. This is done intentionally so that the plug-in is able to communicate with the iDRAC for future use in deployment needs.

# Unable to view new iDRAC version details listed on vCenter hosts and clusters page

Resolution: After successful completion of a firmware update task in the vSphere web client, refresh the **Firmware Update** page and verify the firmware versions. If the page displays the old versions, go to the **Host Compliance** page in OpenManage Integration for VMware vCenter, and check the CSIOR status of that host. If CSIOR is not enabled, enable CSIOR and reboot host. If CSIOR is already enabled, log in to the iDRAC console, reset iDRAC, wait for few minutes, and then refresh the **Firmware Update** page.

# How can I test event settings by using OMSA to simulate temperature hardware Fault

To ensure that events are functioning correctly, perform the following steps:

1. In the OMSA user interface, navigate to **Alert Management** > **Platform Events**.
2. Select the **Enable Platform Event Filter Alerts** check box.
3. Scroll down to the bottom, and click **Apply Changes**.
4. To ensure that a specific event is enabled, such as temperature warning, from the tree on the left, select **Main System Chassis**.
5. Under **Main System Chassis**, select **Temperatures**.
6. Select the **Alert Management** tab, and select **Temperature Probe Warning**.
7. Select the **Broadcast a Message** check box, and select **Apply Changes**.
8. To cause the temperature warning event, from the tree view on the left, select **Main System Chassis**.
9. Select **Temperatures** under **Main System Chassis**.
10. Select the **System Board Ambient Temp** link, and select the **Set to Values** option button.
11. Set the **Maximum Warning Threshold** to a value preceding the current listed reading.
    For example, if the current reading is 27, set the threshold to **25**.
12. Select **Apply Changes**, and the temperature warning event is generated.

    To cause another event, restore the original settings by using the same **Set to Values** option. Events are generated as warnings, and then to a normal state. If everything is working properly, navigate to the **vCenter Tasks & Events** view; a temperature probe warning event should be displayed.

    > **NOTE:** There is a filter for duplicate events; if you try to trigger the same event too many times in a row, you only receive one event. To see all events, allow at least 30 seconds between events.

## Although OMSA agent is installed on OMIVV host system, I still get error message that OMSA is not installed.

To resolve this issue on an 11th generation server:

1. Install **OMSA** with the **Remote Enablement** component on the host system.
2. If you are using the command line to install OMSA, ensure that you specify the**-c option**. If OMSA is already installed, reinstall it with the -c option and restart the service:

    ```
    srvadmin-install.sh -c
    srvadmin-services.sh restart
    ```

    For an ESXi host, ensure that you install **OMSA VIB** by using the **VMware Remote CLI tool**, and reboot the system.

## Can OMIVV support ESXi with lockdown mode enabled

Yes, lockdown mode is supported in this Release on hosts ESXi 5.0 and later.

## When I tried to use lockdown mode, it fails

When I added a host to the connection profile in lockdown mode, the inventory started, but failed stating that “No Remote Access Controller was found or Inventory is not supported on this host.”

If you put the host in lockdown mode or remove a host from lockdown mode, ensure that you wait for 30–minutes before performing the next operation in OMIVV.

## Creation of hardware profile fails if I am using reference server

Check to ensure that minimum recommended versions of the iDRAC firmware, the Lifecycle Controller firmware, and BIOS are installed.

To ensure that the data retrieved from the reference server is current, enable **Collect System Inventory On Restart (CSIOR)**, and restart the reference server prior to extraction of data.

# Attempting to deploy ESXi on server fails

1. Ensure that the **ISO location (NFS path)** and staging **folder paths** are accurate.
2. Ensure that the **NIC** selected during assignment of server identity is on the same network as the virtual appliance.
3. If using **static IP address**, ensure that the network information provided (including subnet mask and Default Gateway) is accurate. Also, ensure that the IP address is not already assigned on the network.
4. Ensure that at least one **Virtual Disk** is seen by the system.

   ESXi also installs to an internal SD card.

# Hypervisor deployments failing on Dell PowerEdge R210 II machines

A timeout issue on the Dell PowerEdge R210 II systems produces a hypervisor deployment failure error due to the failure of the BIOS to boot from the attached ISO.

Resolution: Manually install hypervisor on the machine.

# Auto discovered systems are displayed without model information in Deployment wizard

This usually indicates that the firmware version installed on the system does not meet the recommended minimum requirements. Sometimes, a firmware update may not have registered on the system.

Resolution: Cold booting the system or reseating the Blade fixes this issue. The newly enabled account on the iDRAC must be disabled, and auto discovery reinitiated to provide model information and NIC information to OMIVV.

# NFS share is set up with ESXi ISO, but deployment fails with errors mounting share location

To find the solution:

1. Ensure that the iDRAC is able to ping the appliance.
2. Ensure that your network is not running too slow.
3. Ensure that the ports: 2049, 4001 - 4004 are open and the firewall is set accordingly.

# How do I force remove virtual appliance from vCenter

1. Go to **Https://<vcenter_serverIPAddress>/mob**
2. Enter the VMware vCenter admin credentials.
3. Click **Content**.
4. Click **ExtensionManager**.
5. Click **UnregisterExtension**.
6. Enter the extension key to unregister com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient, and then click **Invoke method**.
7. In the vSphere web client, turn off OMIVV and delete it. The key to unregister must be for the web client.

# Entering a Password in the Backup Now Screen Receives an Error Message

If you are using a low resolution monitor, the Encryption Password field is not visible from the BACKUP NOW window. You must scroll down the page to enter the encryption password.

## In vSphere web client, clicking Dell server management portlet or Dell icon returns 404 error

Check if the OMIVV appliance is running; if not, then restart it from the vSphere web client. Wait for a few minutes for the virtual appliance web service to start, and then refresh the page. If the error continues, try to ping the appliance by using the IP address or fully qualified domain name from a command line. If the ping does not resolve, review your network settings to ensure that they are correct.

## What should I do as firmware update failed

Check the virtual appliance logs to see if the tasks timed out. If so, iDRAC must be reset by performing a cold reboot. After the system is up and running, check to see if the update was successful by either running an inventory or by using the **Firmware** tab.

## What should I do as vCenter registration failed

vCenter registration can fail due to communication issues, therefore if you are experiencing these issues, a solution is to use a static IP address. To use a static IP address, in the Console tab of the OpenManage Integration for VMware vCenter, select **Configure Network** > **Edit Devices** and enter the correct **gateway** and **FQDN** (fully qualified domain name). Enter the DNS server name under Edit DNS Config.

ⓘ **NOTE:** Ensure that the virtual appliance can resolve the DNS server you entered.

## Performance during connection profile test credentials is slow or unresponsive

The iDRAC on a server has only one user (for example, only *root*) and the user is in a disabled state, or all users are in a disabled state. Communicating to a server in a disabled state causes delays. To fix this issue, you can either fix the disable state of the server, or reset iDRAC on the server to re-enable the root user to default setting.

To fix a server in a disabled state:

1. Open the Chassis Management Controller console, and select the disabled server.
2. To automatically open the iDRAC console, click **Launch iDRAC GUI**.
3. Navigate to the user list in the iDRAC console, and click one of the following:
   - iDRAC6: Select **iDRAC settings** > **Network/Security tab** > **Users tab**.
   - iDRAC7: Select **iDRAC settings** > **Users tab**.
   - iDRAC8: Select **iDRAC settings** > **Users tab**.
4. To edit the settings, in the User ID column, click the link for the admin (root) user.
5. Click **Configure User**, and then click **Next**.
6. In the **User Configuration** page for the selected user, select the check box next to Enable user, and then click **Apply**.

## Does OMIVV support VMware vCenter server appliance

Yes, OMIVV supports the VMware vCenter Server appliance since v2.1.

## Firmware level not updated when I have performed firmware update with Apply on Next reboot option and system was rebooted

To update firmware, run the inventory on the host after the reboot is completed. Sometimes, where the reboot event does not reach the appliance, the inventory is not automatically triggered. In such situation, you must rerun the inventory manually to get the updated firmware versions.

## Host still displayed under chassis even after removing host from vCenter tree

The hosts under the chassis are identified as part of the chassis inventory. After a successful chassis inventory, the host list under the chassis is updated. Therefore, even if the host is removed from the vCenter tree, the host is displayed under the chassis until the next chassis inventory is run.

## In Administration Console, Update Repository Path is not set to default path after I reset appliance to factory settings

After you reset the appliance, go to the **Administration Console**, and then click **APPLIANCE MANAGEMENT** in the left pane. In the **Appliance Settings** page, the **Update Repository Path** is not changed to the default path.

**Resolution:** In **Administration Console**, manually copy the path in the **Default Update Repository** field to the **Update Repository Path** field.

## After backup and restore of OMIVV, alarm settings are not restored

Restoring the OMIVV appliance backup does not restore all the Alarm settings. However, in the OpenManage Integration for VMware GUI, the **Alarms and Events** field displays the restored settings.

Resolution: In the OpenManage Integration for VMware GUI, in the **Manage** > **Settings** tab, manually change the**Events and Alarms** settings.

## Hypervisor deployment fails when NPAR is enabled on a target node and disabled in System Profile

Hypervisor deployment fails when a System Profile with a disabled NIC Partitioning (NPAR) is applied on a target machine. Here, NPAR is enabled on the target node and only one of the partitioned NIC, except partition 1 is selected as the NIC for the Management Tasks during the deployment process through the deployment wizard.

Resolution: If you are changing the NPAR status through System Profile during deployment, ensure that you select only the first partition for management network in the deployment wizard.

Version Affected: 4.1

## Available virtual appliance version displays wrong information when the available version is lesser than the current version

In the OMIVV Admin console, under **Appliance Management**, **Available Virtual Appliance Version** displays the modes RPM and OVF as available.

ⓘ **NOTE:** It is recommended that update repository path is set to the latest version and downgrading the virtual appliance version is not supported.

## The 267027 exception is thrown while adding a 12G bare-metal server with an Express license

During bare-metal discovery, if an incorrect credential is entered, the user account is automatically locked for few minutes. During this period, iDRAC becomes unresponsive and takes a few minutes before restoring normalcy.

**Resolution**: Wait for few minutes and retype the user credentials.

# During OS deployment on 14G, hardware profile apply fails due to iDRAC error

During OS deployment on 14G server, a configuration update job is created in iDRAC when the hardware profile is applied. However, the job fails sometimes and displays a message indicating that a Configuration job is already created.

**Resolution**: To clear the stale entries and retry the OS deployment, run the `racadm jobqueue delete -i JID_CLEARALL_FORCE` command.

# OMIVV RPM upgrade fails when proxy is configured with domain user authentication

If OMIVV appliance is configured with proxy to reach the internet and proxy is authenticated using NTLM authentication, then the RPM update fails due to the issues in the underlying yum tool.

**Version Affected**: OMIVV 4.0 and above

**Resolution / Work around**: Do Back up and Restore to update the OMIVV appliance.

# Unable to apply System Profile that has PCIe card in the FX chassis

The OS deployment fails on a target server if the source server has PCIe card information when using an FX chassis. The System profiles on the source server has different `fc.chassislot ID` than the one on the target server. OMIVV tries to deploy the same `fc.chassislot ID` on the target server but fails. The System profiles searches for exact instance( FQDD) while applying the profile, which works successfully on rack servers (identical), but may have few restrictions in modular servers. For example, in FC640, the System profiles created from one modular server cannot applied on other modular servers in the same FX chassis because of NIC level restrictions.

**Version Affected**: 4.1 and later.

**Resolution**: System profile taken from a FC640 server in slot 1 of a FX2s chassis can only be applied on another FC640 server residing in the slot 1 of another FX2s chassis.

# Drift Detection shows noncompliant for Modular servers that has PCIe card in the FX chassis

The System profiles searches for exact instance(FQDD) while comparing with the baseline, which works successfully on Rack servers (identical), but may have few restrictions in Modular servers. For example, in FC640, the System profile (Baseline) created from one modular server shows drift for other modular servers in the same FX chassis because of FQDD mismatches.

Version Affected: 4.1 and later.

Resolution: While creating System profile, clear the FQDDs that are not common with other servers.

# Unable to deploy an OS on PowerEdge serves when the iDRAC does not populate the MAC address of the selected NIC

The OS deployment fails on PowerEdge Servers when the iDRAC does not populate the MAC address for the selected NIC port.

Resolution: Update the respective NIC firmware and iDRAC firmware to the latest version and ensure that the MAC address is populated on the NIC port.

Version Affected: 4.3

## When deploying an OS, the Hardware Profile cannot be applied and the boot order cannot be configured without restarting the host

When applying the Hardware Profile, if the BIOS boot mode and NVMe settings are changed, the boot order cannot be configured without restarting the host device.

Resolution: Manually change the boot mode from system BIOS by launching the virtual console from iDRAC.

Version Affected: 4.3

## When creating a connection profile for the host having ESXi 6.5U1, the Service Tag of the host is not displayed on the Select Hosts page

When the OMIVV queries vCenter for the Service Tag of ESXi, vCenter cannot return the Service Tag because the Service Tag value is null.

Resolution: Update the ESXi version to ESXi 6.5U2 or ESXi 6.7 U1

Version Affected: 4.3

## Chassis object is not displayed on the left Navigator pane of the Dell EMC Chassis page

- After creating a chassis profile or connection profile of a chassis, the corresponding IP of the chassis is displayed on the **Objects** tab, but not in the left **Navigator** pane.
- After deleting a chassis on the **Summary** tab, if the back button is clicked, an error message is displayed.
- If the Service Tag link is clicked for an MX chassis in the **OMIVV Host Information** section or clicking chassis IP on the **Chassis Profile** page, a message is displayed indicating that either the permission or the object itself does not exist.

  Resolution: When operations such as removal, addition, or update of a chassis are performed, refresh the **Dell EMC Chassis** page to view the latest data.

  Version Affected: 4.3

## Dell icon is not displayed after backup and restore from an earlier OMIVV version to a later OMIVV version

After backup and restore from an earlier OMIVV version to a later OMIVV version, the following issues are observed:

- The Dell EMC logo is not displayed at vCenter.
- The 2000000 error
- The 3001 error

  Resolution:

  - Restart vSphere Web Client on the vCenter server.
  - If the issue persists:
    - For VMware vCenter Server Appliance, go to `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity` and for Windows vCenter, go to `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance and see if the old data exists, such as: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
    - Manually delete the folder corresponding to the earlier OMIVV version.

## When upgrading or downgrading some iDRAC firmware versions using OMIVV, even when the actual firmware update is successful, OMIVV may indicate that the job is failed.

During firmware update, when you downgrade or upgrade the iDRAC versions such as 3.20.20.20, 3.21.21.21, and 3.21.21.22, the job status is indicated as failed even when the job was successfully run.

Resolution: Refresh the inventory after the job failure and rerun the job for other components.

Version Affected: 4.3

## The deployment job fails when a server is in the UEFI mode and Secure boot feature is enabled

When the target sever is in UEFI mode and its secure boot feature is enabled, the deployment job on that server is unsuccessful.

Resolution: Even if the OS deployment job has failed, the device or server-side hypervisor would have got updated. Therefore, manually add the host IP and manage the server.

Version Affected: 4.3

## Configuring the System Lockdown mode at a cluster level sometimes displays a message "No hosts under the cluster has successful inventory"

Configuring the System Lockdown mode at a cluster level sometimes displays a message "No hosts under the cluster has successful inventory". This message is displayed even when the cluster has successfully inventoried the 14G hosts that are managed by OMIVV.

Resolution: Reboot the vCenter.

To reboot the vCenter, do the following:

1. Log in to the vSphere Web Client with a vCenter Single Sign-on Administrator account.
2. Go to **Administration** > **Deployment** > **Deployment** > **System Configuration**.
3. Click **Nodes**, select the vCenter Server Appliance node and click the **Related Objects** tab.
4. Reboot the vCenter node.

## Sometimes post RPM upgrade of OMIVV appliance, multiple entries in the logs are seen in vCenter Recent Tasks

Sometimes, after RPM upgrade, multiple entries are displayed in logs when viewed on vCenter Recent Tasks.

Resolution: Restart the vCenter services.

Version Affected: 4.3

# Bare-metal deployment issues

This section deals with issues found during the deployment process.

**Auto discovery and handshake prerequisites**

- Prior to running auto discovery and handshake, ensure that iDRAC and Lifecycle Controller firmware and BIOS versions meet the minimum recommendations.
- CSIOR must have run at least once on the system or iDRAC.

**Hardware configuration failure**

- Before initiating a deployment task, ensure that the system has completed CSIOR and is not in the process of rebooting.
- BIOS configuration should be run in clone mode so that the reference server is an identical system.
- Some controllers do not allow creation of a RAID 0 array with one drive. This feature is supported only on high-end controllers, and the application of such a hardware profile can cause failures.

## Enabling auto discovery on newly purchased system

The auto discovery feature of a host system is not enabled by default; instead, enablement must be requested at the time of purchase. If auto discovery enablement is requested at the time of purchase, DHCP is enabled on the iDRAC and admin accounts are disabled. It is not necessary to configure a static IP address for the iDRAC. It gets one from a DHCP server on the network. To use the auto discovery feature, a DHCP server or a DNS server (or both) must be configured to support the discovery process. CSIOR should already be run during the factory process.

If auto discovery was not requested at the time of purchase, it can be enabled as follows:

1. During the boot routine, press **Ctrl+E**.
2. In the iDRAC setup window, enable the NIC (blade servers only).
3. Enable Auto-Discovery.
4. Enable DHCP.
5. Disable admin accounts.
6. Enable **Get DNS server address from DHCP**.
7. Enable **Get DNS domain name from DHCP**.
8. In the **Provisioning Server** field, enter:

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

# 17

# Related Documentation

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 4.3** to access the following documents:

- *OpenManage Integration for VMware vCenter Version 4.3 Web Client User's Guide*
- *OpenManage Integration for VMware vCenter Version 4.3 Release Notes*
- *OpenManage Integration for VMware vCenter Version 4.3 Compatibility Matrix*

You can find the technical artifacts including white papers at https://www.dell.com/support.

**Topics:**

- Accessing documents from the Dell EMC support site

## Accessing documents from the Dell EMC support site

You can access the required documents using the following links:

- For Dell EMC Enterprise Systems Management documents — www.dell.com/esmmanuals
- For Dell EMC OpenManage documents — www.dell.com/openmanagemanuals
- For Dell EMC Remote Enterprise Systems Management documents — www.dell.com/esmmanuals
- For iDRAC and Dell Lifecycle Controller documents — www.dell.com/idracmanuals
- For Dell EMC OpenManage Connections Enterprise Systems Management documents — www.dell.com/esmmanuals
- For Dell EMC Serviceability Tools documents — www.dell.com/serviceabilitytools
- 1. Go to www.dell.com/manuals.
  2. Click **Choose from all products**.
  3. From **All products** section, click **Software & Security**, and then click the required link from the following:
     - **Enterprise Systems Management**
     - **Serviceability Tools**
     - **Dell Client Command Suite**
     - **Connections Client Systems Management**
  4. To view a document, click the required product version.
- Using search engines:
  - Type the name and version of the document in the search box.

# System specific attributes

## iDRAC

Table 45. System specific attributes iDRAC

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| DNS RAC Name | DNS RAC Name | NIC Information |
| DataCenterName | Data Center Name | Server Topology |
| Aisle Name | Aisle Name | Server Topology |
| Rack Name | Rack Name | Server Topology |
| Rack Slot | Rack Slot | Server Topology |
| RacName | Active Directory RAC Name | Active Directory |
| DNSDomainName | DNS Domain Name | NIC Static Information |
| Address | IPv4 Address | IPv4 Static Information |
| Net Mask | Net Mask | IPv4 Static Information |
| Gateway | Gateway | IPv4 Static Information |
| DNS1 | DNS Server 1 | IPv4 Static Information |
| DNS2 | DNS Server 2 | IPv4 Static Information |
| Address 1 | IPv6 Address 1 | IPv6 Static Information |
| Gateway | IPv6 Gateway | IPv6 Static Information |
| Prefix Length | IPV6 Link Local Prefix Length | IPv6 Static Information |
| DNS1 | IPV6 DNS Server 1 | IPv6 Static Information |
| DNS2 | IPv6 DNS Server 2 | IPv6 Static Information |
| DNSFromDHCP6 | DNS Server From DHCP6 | IPv6 Static Information |
| HostName | Server Host Name | Server Operating System |
| RoomName | RoomName | Server Topology |
| NodeID | System Node ID | Server Information |

## BIOS

Table 46. System specific attributes for BIOS

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| AssetTag | Asset Tag | Miscellaneous Settings |
| IscsiDev1Con1Gateway | Initiator Gateway | Connection 1 Settings |
| IscsiDev1Con1Ip | Initiator IP Address | Connection 1 Settings |
| IscsiDev1Con1Mask | Initiator Subnet Mask | Connection 1 Settings |

### Table 46. System specific attributes for BIOS

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| IscsiDev1Con1TargetIp | Target IP Address | Connection 1 Settings |
| IscsiDev1Con1TargetName | Target Name | Connection 1 Settings |
| IscsiDev1Con2Gateway | Initiator Gateway | Connection 1 Settings |
| IscsiDev1Con2Ip | Initiator IP Address | Connection 1 Settings |
| IscsiDev1Con2Mask | Initiator Subnet Mask | Connection 1 Settings |
| IscsiDev1Con2TargetIp | Target IP Address | Connection 1 Settings |
| IscsiDev1Con2TargetName | Target Name | Connection 1 Settings |
| IscsiInitiatorName | ISCSI Initiator Name | Network Settings |
| Ndc1PcieLink1 | Integrated Network Card 1 PCIe Link1 | Integrated Devices |
| Ndc1PcieLink2 | Integrated Network Card 1 PCIe Link2 | Integrated Devices |
| Ndc1PcieLink3 | Integrated Network Card 1 PCIe Link3 | Integrated Devices |
| UefiBootSeq | UEFI Boot Sequence | UEFI Boot Settings |

# RAID

### Table 47. System specific attributes for RAID

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| Enclousre Requested Configuration Mode | NA | NA |
| Enclosure Current Configuration Mode | NA | NA |

# CNA

### Table 48. System specific attributes for CNA

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| ChapMutualAuth | CHAP Mutual Authentication | iSCSI General Parameters |
| ConnectFirstTgt | Connect | iSCSI First Target Parameters |
| ConnectSecondTgt | Connect | iSCSI Second Target Parameters |
| FirstFCoEBootTargetLUN | Boot LUN | FCoE Configuration |
| FirstFCoEWWPNTarget | World Wide Port Name Target | FCoE Configuration |
| FirstTgtBootLun | Boot LUN | iSCSI First Target Parameters |
| FirstTgtChapId | CHAP ID | iSCSI First Target Parameters |
| FirstTgtChapPwd | CHAP Secret | iSCSI First Target Parameters |
| FirstTgtIpAddress | IP Address | iSCSI First Target Parameters |
| FirstTgtIscsiName | iSCSI Name | iSCSI First Target Parameters |
| FirstTgtTcpPort | TCP Port | iSCSI First Target Parameters |
| IP Auto-Configuration | IpAutoConfig | iSCSI General Parameters |
| IscsiInitiatorChapId | CHAP ID | iSCSI Initiator Parameters |

Table 48. System specific attributes for CNA

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| IscsiInitiatorChapPwd | CHAP Secret | iSCSI Initiator Parameters |
| IscsiInitiatorGateway | Default Gateway | iSCSI Initiator Parameters |
| IscsiInitiatorIpAddr | IP Address | iSCSI Initiator Parameters |
| IscsiInitiatorIpv4Addr | IPv4 Address | iSCSI Initiator Parameters |
| IscsiInitiatorIpv4Gateway | IPv4 Default Gateway | iSCSI Initiator Parameters |
| IscsiInitiatorIpv4PrimDns | IPv4 Primary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorIpv4SecDns | IPv4 Secondary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorIpv6Addr | IPv6 Address | iSCSI Initiator Parameters |
| IscsiInitiatorIpv6Gateway | IPv6 Default Gateway | iSCSI Initiator Parameters |
| IscsiInitiatorIpv6PrimDns | IPv6 Primary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorIpv6SecDns | IPv6 Secondary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorName | iSCSI Name | iSCSI Initiator Parameters |
| IscsiInitiatorPrimDns | Primary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorSecDns | Secondary DNS | iSCSI Initiator Parameters |
| IscsiInitiatorSubnet | Subnet Mask | iSCSI Initiator Parameters |
| IscsiInitiatorSubnetPrefix | Subnet Mask Prefix | iSCSI Initiator Parameters |
| SecondaryDeviceMacAddr | Secondary Device MAC Address | iSCSI Secondary Device Parameters |
| SecondTgtBootLun | Boot LUN | iSCSI Second Target Parameters |
| SecondTgtChapPwd | CHAP Secret | iSCSI Second Target Parameters |
| SecondTgtIpAddress | IP Address | iSCSI Second Target Parameters |
| SecondTgtIscsiName | iSCSI Name | iSCSI Second Target Parameters |
| SecondTgtTcpPort | TCP Port | iSCSI Second Target Parameters |
| UseIndTgtName | Use Independent Target Name | iSCSI Secondary Device Parameters |
| UseIndTgtPortal | Use Independent Target Portal | iSCSI Secondary Device Parameters |
| VirtFIPMacAddr | Virtual FIP MAC Address | Main Configuration Page |
| VirtIscsiMacAddr | Virtual iSCSI Offload MAC Address | Main Configuration Page |
| VirtMacAddr | Virtual MAC Address | Main Configuration Page |
| VirtMacAddr[Partition:n] | Virtual MAC Address | Partition n Configuration |
| VirtWWN | Virtual World Wide Node Name | Main Configuration Page |
| VirtWWN[Partition:n] | Virtual World Wide Node Name | Partition n Configuration |
| VirtWWPN | Virtual World Wide Port Name | Main Configuration Page |
| VirtWWPN[Partition:n] | Virtual World Wide Port Name | Partition n Configuration |
| World Wide Node Name | WWN | Main Configuration Page |
| World Wide Node Name | WWN[Partition:n] | Partition n Configuration |

# FC

**Table 49. System specific attributes for FC**

| Attribute Name | Display Attribute Name | Group Display Name |
|---|---|---|
| VirtualWWN | Virtual World Wide Node Name | Port Configuration Page |
| VirtualWWPN | Virtual World Wide Port Name | Port Configuration Page |

# Customization attributes

Table 50. Customization attributes

| FQDD | Attributes | OMIVV Customization |
|---|---|---|
| BIOS | Virtualization Technology | Always Enabled |
| iDRAC | Collect System Inventory on Restart | Always Enabled |
| RAID | IncludedPhysicalDiskID | If IncludedPhysicalDiskID value is Auto Select then we are removing that value |
| RAID | RAIDPDState | Removed |
| iDRAC | User Admin Password<br>Password | Only iDRAC enabled users will have " Password " link to enter the password. |

C

# Additional information

The following Dell technical white papers available at **delltechcenter.com** provide more information about the system profile configuration template, attributes, and work flows:

- *Server Cloning with Server Configuration Profiles*
- *Server Configuration XML File*
- *Configuration XML Workflows*
- *Configuration XML Workflow Scripts 133*
- *XML Configuration File Examples*

# Component vs. baseline version comparison matrix

Table 51. Component vs. baseline version comparison matrix

| Drift Type | | | | |
|---|---|---|---|---|
| **Hardware** | **Associated Baseline** | **Target Component** | **Scenario** | **Compliance Status** |
| | Available | Available | Hardware component matches with the associated baseline. | Compliant |
| | Available | Available | Hardware component not matches with the associated baseline. | Non-compliant |
| | Not available | Available | The comparison status is not calculated and ignored. | Compliant |
| | Available | Not available | Hardware component version is available in the associated baseline but the component or attribute is not available. | Non-compliant |
| | Not available | Not available | The comparison status is not calculated and ignored. | Compliant |
| **Firmware** | **Associated Baseline** | **Target Component** | **Scenario** | **Compliance Status** |
| | Available | Available | Firmware component matches with the associated baseline. | Compliant |
| | Available | Available | Firmware component not matches with the associated baseline. | Non-compliant |
| | Available | Not available | The comparison status is not calculated and ignored. | Compliant |
| | Not available | Not available | The comparison status is not calculated and ignored. | Compliant |
| **Driver** | **Associated Baseline** | **Target Component** | **Scenario** | **Compliance Status** |
| | Available | Available | Driver component matches with the associated baseline. | Compliant |
| | Available | Available | Driver component not matches with the associated baseline. | Non-compliant |
| | Not available | Available | The comparison status is not calculated and ignored. | Compliant |
| | Available | Not available | Driver component version is available in the associated baseline but the component or attribute is not available or new component is available. | Non-compliant |
| | Not available | Not available | The comparison status is not calculated and ignored. | Compliant |