OpenManage Integration for VMware vCenter Version 5.0

User's Guide

September 2019
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

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 reduce the complexity of managing your data center by streamlining the tasks associated with the management and monitoring of Dell EMC server infrastructure in the vSphere environment.

Whats new in this release

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

- Support for HTML-5 Client
- Support for PowerEdge R6515 and PowerEdge R7515 servers
- Enhancement in the system profile to support the following:
  - System profile types—Basic and Advanced
  - System profile edit
  - 12G and 13G PowerEdge servers
- Added support for vSphere 6.7 U3, vSphere 6.7 U2, and vSphere 6.5 U3
- Enhancement in the deployment to support the following:
  - System profile baselining based on the associated cluster profile for cluster
  - System Profile Configuration Preview
- Enhancement in the configuration compliance:
  - Support for firmware and hardware baselining for vSphere clusters
  - Cluster level view of drift details with vCenter context
- Support for context-sensitive help
- Enhancement in the repository profile to support online repositories—Dell EMC Default Catalog and Validated MX Stack Catalog
- Support for MX chassis management module firmware update
- Enhancement in admin console to support reset backup settings
- Enhancement in deployment mode to support for 2000 hosts with extra large mode
- Support for dual network adapter for OMIVV
- Dashboard to monitor host and chassis

Important notes

The following are the important items to note before upgrading to OMIVV 5.0:

1. From OMIVV 5.0 onwards, only VMware vSphere Client (HTML-5) is supported and the vSphere Web Client (FLEX) is not supported.
2. 11G servers are not supported. Only the 12G and later generations servers are retained after restore.
3. Hardware profiles and deployment templates are not supported. System profiles now have two types, where Basic is intended to replace the same settings that were captured in the Hardware Profile. For deployment, the deployment process asks what system profiles (configuration) and ISO repository (hypervisor image) you want to use for the deployment.

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: ● PowerEdge server details such as memory—quantity and type, NIC, PSU, processors, and RAC ● Warranty information at server, cluster, and data center level ● Chassis details such as Chassis Management Controller (CMC) or Management Module information, chassis power supply, KVM status, fan or thermal details, warranty information, switch, server, and storage details ● Support for an MX chassis relationship in the Multi-Chassis Management (MCM) configuration. ● Fabric information for an MX chassis MCM configuration ● QuickSync hardware information for an MX chassis
Monitor and send alerts	The monitoring and alerting includes the following functionalities: ● Detect key hardware faults and perform virtualization-aware actions. For example, migrate workloads or place host in a maintenance mode. ● Provide intelligence such as inventory, events, alarms to diagnose server and chassis problems. ● Support for VMware Proactive HA feature.
Firmware updates	The cluster-aware server firmware update includes the following: ● Update supported servers to the most recent version of BIOS and firmware.
Drift detection for clusters	● Firmware compliance for clusters ● Driver compliance for vSAN clusters ● Hardware compliance **NOTE:** Hardware compliance is not supported for hosts that are managed using chassis credential profile.
Driver updates	Driver updates for vSAN clusters.
Deployment	Deployment includes the following: ● Create and deploy system profiles. ● 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 warranty database of Dell and enable for easy online warranty upgrading.
Security role and permissions	Security role and permissions include the following functionalities: ● Integrate with standard vCenter authentication, rules, and permissions. ● Support for iDRAC Lockdown Mode in 14th Gen servers.
Support for OEM server	The following OMIVV features are supported: ● Inventory ● Monitor and send alerts.

Table 1. OMIVV features (continued)

Features	Description
	- Firmware update - Deployment - Service Information - Security role and permissions
MX chassis firmware update	Provides an option to update management module firmware for MX chassis.

NOTE: From OMIVV 5.0 onwards, only VMware vSphere Client (HTML-5) is supported and the vSphere Web Client (FLEX) is not supported.

2

About Administration Console

You can administer the OpenManage Integration for VMware vCenter and its virtual environment using either of the two administrations portals mentioned below:

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

Register new vCenter server

Your account should have the necessary privileges to create a server. For more information about the required privileges, see Required privileges for non-administrator users on page 13.

You can register the OMIVV appliance after the OMIVV is installed. The OMIVV uses the administrator user account or a non-administrator user account with necessary privileges for vCenter operations. A single OMIVV appliance instance can support 15 vCenter servers and up to 2,000 ESXi hosts.

To register a new vCenter server, do the following:

1. Go to https://*<ApplianceIP/hostname/>*.
2. On the **VCENTER REGISTRATION** page, in the right pane, click **Register New vCenter Server**.
   The **REGISTER A NEW vCENTER** page is displayed.
3. In the **REGISTER A NEW VCENTER** dialog box, under **vCenter Name**, perform the following tasks:
   a. In the **vCenter Server IP or Hostname** box, enter the vCenter IP address or FQDN of the host.

      NOTE: Dell EMC recommends you to register OMIVV with the VMware vCenter using a Fully Qualified Domain Name (FQDN). For all registrations, the hostname of vCenter must 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 information is present in both forward and reverse lookup zones in your DNS server.

   b. In the **Description** box, enter a description—optional.
4. Under **vCenter User Account**, perform the following steps:
   a. In the **vCenter User Name** box, enter the user name of administrator or a non-administrator user name with the required privileges.
   b. In the **Password** box, enter the password.
   c. In the **Verify Password** 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 WebClient from which you can access the OMIVV features.

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 the 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.

NOTE: If you want to upload a customized Certificate Signing Request (CSR) to OMIVV, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed on the WebClient. To fix this issue, unregister, and reregister the appliance with the vCenter.

Register vCenter server by non-administrator user

To perform the following tasks, ensure that you have vCenter Administrator privileges.

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. Create a role or modify existing role with a required privileges for the role.

   For more information about the list of privileges required for the role, see Required privileges for non-administrator users.

   For the steps required to create or modify a role and select privileges in the vSphere Client (HTML-5), see the VMware vSphere documentation
2. Assign a user to the newly created role after you define a role and select privileges for the role.

   For more information about assigning a role to privilege, see the VMware vSphere documentation.

   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. After registration is complete, assign the Dell privileges to the role created or modified in step 1. See Assign Dell privileges to existing role on page 14.

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 must have the following privileges:

While registering a vCenter server with OMIVV by a non-administrator user, a 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
    - Change settings
    - Connection
    - Maintenance

        - Network configuration
        - Query patch
        - Security profile and firewall

        NOTE: If you are using vCenter 6.5 or upgrading to vCenter 6.5 or later, ensure that you assign the modify cluster privilege.

        - 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: If you are using vCenter 6.5 or upgrading to vCenter 6.5 or later, ensure that you assign the modify cluster privilege,

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

NOTE: If a vCenter server is registered using non-administrator user to access any OMIVV features, non-administrator user must have Dell privileges. For more information about assigning Dell privileges, see Assign Dell privileges to existing role on page 14.

Assign Dell privileges to existing role

If specific pages of OMIVV are accessed with no Dell privileges that are assigned to the logged-in user, the 2000000 error is displayed.

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

1. Log in to the vSphere Client (HTML-5) with administrative rights.
2. In vSphere Client (HTML-5), expand **Menu**, click **Administration → Roles**.
3. From the **Roles provider** drop-down list, select a vCenter server.
4. From the **Roles** list, select **Dell-Operational**, and then click **PRIVILEGES**.
5. To assign the Dell privileges, click the edit icon [✏].
   The **Edit Role** page is displayed.
6. In the left pane, click **Dell**, and then select the following Dell privileges for the selected role, and then click **NEXT**:
    - Dell.Configuration
    - Dell.Deploy-Provisioning
    - Dell.Inventory
    - Dell.Monitoring
    - Dell.Reporting

For more information about the available OMIVV roles within vCenter, see Security roles and permissions.

7. Edit the role name and enter description for the selected role, if required.
8. Click **FINISH**.
   Log out and log in from the vCenter. The user with necessary privileges can now perform the OMIVV operations.

Update 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 OMIVV 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 tasks to import the new certificate for OMIVV:

1. Go to https://*<ApplianceIP/hostname/>*.
2. In the left pane, click **VCENTER REGISTRATION**.
   The registered vCenter servers are displayed in the working pane.
3. To update the certificate for a vCenter server IP or hostname, click **Update**.

Modify vCenter login credentials

You can modify the vCenter login credentials with administrative privileges or a non-administrator user with necessary privileges.

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

1. Go to https://*<ApplianceIP/hostname/>*.
2. In the **Login** dialog box, type the password, and then click **Login**.
3. In the left pane, click **VCENTER REGISTRATION**.
   The registered vCenter servers are displayed in the working pane.
4. To open the **MODIFY USER ACCT** window, under **Credentials**, click **Modify** for a registered vCenter.
5. If incorrect credentials are entered, a message is displayed. Enter valid vCenter user name, password, and reenter to verify the password.
6. To change the password, click **Apply**. To cancel an update, click **Cancel**.

Unregister OpenManage Integration for VMware vCenter

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

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 click **Edit**. To disable Proactive HA, in the **Proactive HA Failures and Responses** screen, clear the check box against **Dell Inc** provider.

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

1. Go to https://*<ApplianceIP/hostname/>*.
2. On the **VCENTER REGISTRATION** page, in the **vCenter Server IP or Hostname** table, click **Unregister**.

   NOTE: Ensure to select the correct vCenter because OMIVV can be associated with more than one vCenter.

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

   NOTE: After unregistering OMIVV, log out and log in from the vSphere Client (HTML-5). If the OMIVV icon is still visible, then restart the Client services for both vSphere Client (HTML-5) and Web Client (FLEX).

Upload license to Administration Portal

You can use this option to upload OMIVV host license.

1. Go to https://*<ApplianceIP/hostname/>*.
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 working pane.
4. Click **Upload License**.
5. In the **UPLOAD LICENSE** dialog box, click **Browse** to go to the license file, and then click **Upload**.

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

Manage the OMIVV appliance

The OMIVV appliance management enables you to manage the OpenManage Integration for VMware vCenter network, NTP, and HTTPS information, and enables an administrator to perform the following actions:

- Restart the OMIVV appliance. See Restart OMIVV appliance on page 16.
- Update the OMIVV appliance, and configure an update repository location. See Update OMIVV appliance and repository location on page 16
- Upgrade OMIVV appliance using RPM. See Upgrade OMIVV appliance using RPM on page 17.
- Upgrade OMIVV appliance using backup and restore. See Upgrade OMIVV appliance using backup and restore on page 18.
- Generate and download the troubleshooting bundle. See Generate and download the troubleshooting bundle on page 20.
- Set up HTTP proxy. See Set up HTTP proxy on page 20.
- Set up Network Time Protocol servers. See Set up Network Time Protocol servers on page 20.
- Configure deployment mode. See Configure deployment mode on page 21.
- Extended monitoring See Extended monitoring on page 22.
- Generate a Certificate Signing Request (CSR). See Generate a Certificate Signing Request (CSR) on page 22.
- Upload HTTPS certificate. See Upload HTTPS certificate on page 22.
- Set up global alerts. See Set up global alerts on page 23.

Access the appliance management

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

1. Go to https://*<ApplianceIP/hostname/>*.
2. In the **Login** dialog box, enter the password.
3. To configure the appliance management section, in the left pane, click **APPLIANCE MANAGEMENT**.

Restart OMIVV appliance

1. On the **APPLIANCE MANAGEMENT** page, click **Restart the Virtual Appliance**.
2. To restart the OMIVV appliance, in the **Restart Virtual Appliance** dialog box, click **Apply**.

Update OMIVV appliance and repository location

- To ensure that all data is protected, perform a backup of the OMIVV database before updating the OMIVV appliance. See Manage backup and restore on page 18.
- The OMIVV appliance requires Internet connection to display the available upgrade mechanisms and perform the RPM upgrade. Ensure that the OMIVV appliance has Internet connection. If you require a proxy network, based on the environment network settings, enable the proxy settings, and enter the proxy data. See Setting up the HTTP proxy.
- Ensure that the **Update Repository Path** is valid.
- Ensure that you log out from all vSphere Client (HTML-5) sessions to the registered vCenter servers.

- Before logging into to any of the registered vCenter servers, 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.

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

   For the available OMIVV appliance version, the applicable RPM and OVF OMIVV appliance upgrade mechanisms are displayed with a tick mark [✓].

   The following are the possible upgrade mechanism options available for you to perform either of the tasks for the upgrade mechanism:

Option	Description
1	If a tick mark is displayed against RPM, you can do an RPM upgrade from the existing version to the latest available version. See Upgrade OMIVV appliance using RPM on page 17.
2	If a tick mark is displayed against OVF, you can take a backup of the OMIVV database from the existing version, and restore it in the latest available appliance version. See Upgrade OMIVV appliance using backup and restore on page 18.
3	If a tick mark 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 OMIVV appliance, perform the mentioned tasks for the upgrade mechanisms as applicable from the version of OMIVV.

Upgrade OMIVV appliance using RPM

Ensure that you are upgrading to a version of the appliance that is greater than the current one.

1. On the **APPLIANCE MANAGEMENT** page, based on your network settings, enable proxy and enter proxy setting data, if necessary. See Setting up HTTP proxy .

   For the available OMIVV appliance version, the applicable RPM and OVF OMIVV appliance upgrade mechanisms are displayed with a tick mark [✓].

2. To upgrade the OMIVV plug-in from an existing version to the available 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**.

3. Compare the available OMIVV appliance version and current OMIVV appliance version.
4. To apply the update to the OMIVV appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
5. In the **UPDATE APPLIANCE** dialog box, click **Update**.
   After you click **Update**, you are logged out from the **ADMINISTRATION CONSOLE** window.
6. Close the web browser.

   Once the appliance is RPM upgraded, ensure that you clear the browser cache before logging in to the Dell admin portal.

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

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

Upgrade OMIVV appliance using backup and restore

Dell EMC recommends not to change or remove cluster or host that is managed by OMIVV after taking backup and before restoring the backup file. If the cluster or host that is managed by OMIVV is changed or removed, reconfigure profiles (for example, Host credential profile, cluster profile) associated with those clusters and hosts after restore.

Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes Dell health update provider for Proactive HA clusters that are registered on vCenter by the OMIVV plugin.

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

1. Back up the data of earlier releases.
2. Turn off the older OMIVV appliance from vCenter.
3. Deploy the new OpenManage Integration appliance OVF.
4. Power on the OpenManage Integration new appliance.
5. Set up the network and time zone for the new appliance.

   ⓘ **NOTE:** Dell EMC recommends retaining the identity (IP or FQDN) of the earlier OMIVV appliance for the new OMIVV appliance.

   ⓘ **NOTE:** If the IP address for the new appliance is different from the IP address of the older appliance the Proactive HA feature may not work properly. In such a scenario, disable and enable the Proactive HA for each cluster where Dell EMC host is present.

6. The OMIVV appliance comes with default certificate. If you want to have a custom certificate for your appliance, update the same. See Generate a Certificate Signing Request (CSR) on page 22 and Upload HTTPS certificate on page 22. 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. For more information, see . the Verify installation topic in Installation Guide
9. After the upgrade, Dell EMC recommends running the inventory again on all the hosts that the OMIVV plugin manages.

   The events and alarms settings are not enabled after restoring the appliance. You can enable the Events and Alarms settings again from the **Settings** tab.

   If you upgrade from an earlier version of OMIVV to the available version, all the scheduled job continues to run.

   ⓘ **NOTE:** If the identity (IP or FQDN) of the new OMIVV version Y is changed from the OMIVV version X, configure the trap destination for the SNMP traps to point to the new appliance. For 12G and later servers, the identity change is fixed by running the inventory on these hosts. While running the inventory on 12G hosts, if SNMP traps do not point to the new IP, those hosts are listed as noncomplaint. To fix host compliance issues, see Fix a non-compliant host on page 67.

   After backing up and restoring from an earlier version of OMIVV to an updated version, if you observe that the 200000 message is displayed, or the Dell EMC logo is not displayed , or the OMIVV UI is not responding on the vCenter UI, do the following:

   - Restart vSphere Client services for both vSphere Client (HTML-5) and vSphere Web Client (FLEX) on the vCenter server.
   - If the issue persists:
     - For VMware vCenter Server Appliance: Go to—`/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity`. For Windows vCenter, go to the following folders in the vCenter appliance and check if the old data corresponding to the earlier version exists—`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity` folder in the vCenter appliance.

       An example old data is com.dell.plugin.OpenManage—
       com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX.
     - Manually delete the folder corresponding to the earlier OMIVV version and restart vSphere Client services for both vSphere Client (HTML-5) and Web Client (FLEX).

Manage backup and restore

By using the Administrator Console, you can perform backup and restore related tasks.

- Configure backup and restore

- Schedule automatic backups
- Perform an immediate backup
- Restore the database from backup
- Reset backup and restore settings on page 20

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

1. Go to `https:\\<ApplianceIP|hostname>`.
2. In the **Login** dialog box, type the password.
3. In the left pane, click **BACKUP AND RESTORE**.

Configure backup and restore

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

NOTE: The NTP settings are not saved and restored.

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Edit**.
2. On the highlighted **SETTINGS AND DETAILS** area, do the following:
   a. In **Backup Location**, type the path of the backup files.
   b. In **Username**, enter the user name.
   c. In **Password**, enter the password. The % sign is not supported at the end of the password.
   d. In **Enter the password used to encrypt backups**, type the encrypted password in the box.

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

Schedule automatic backups

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

1. On 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 on which you want to run the backup jobs.
4. In **Time for Backup (24 Hour, HH: mm)**, enter the time in the HH: mm format.
   The **Next Backup** is populated with the date and time of the next scheduled backup.
5. Click **Apply**.

Perform immediate backup

1. On 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 **Use location and encryption password from the Backup settings** 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, "!, @, #, $, %, and *". There is no character limitation for forming a password.
4. Click **Backup**.

Restore OMIVV database from backup

After restoring OMIVV from a previous version:

- 11G bare-metal servers are not supported. Only the 12G and later generations servers are retained after restore.
- Hardware Profiles and Deployment Templates are not supported. Dell EMC recommends using System Profile for deployment.
- Deployment tasks that are scheduled on 11G servers and/or using Hardware Profile based Deployment Templates are canceled.
- All 11G servers are removed from Credential Profiles and consumed licenses are relinquished.
- Repository Profiles will use only 64-bit bundles.

  > ⓘ **NOTE:** If you perform backup and restore from 4.x to 5.x, a warning symbol is displayed against the cluster profile name because OMIVV does not support 32-bit firmware bundle in 5.x. To use the latest changes for the cluster profile, edit the cluster profile.
- Firmware Update jobs that are scheduled on 11G servers are canceled.

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

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Restore Now**.
2. In the **RESTORE NOW** dialog box, enter the path for **File Location** along with the backup .gz file in the CIFS or NFS format.
3. Enter the **Username**, **Password**, and **Encryption Password** for the backup file.
   The encryption password can contain alphanumeric characters and special characters, such as, “!, @, #, $, %, and *”.
4. To save your changes, click **Apply**.
   The appliance is restarted. To verify the installation, see . the Verify installation topic in Installation Guide.

   After restore is complete, close the browser and clear the browser cache before logging in to the admin portal.

Reset backup and restore settings

Using reset settings feature, you can reset settings to the unconfigured state.

1. On the **BACKUP AND RESTORE SETTINGS** page, click **Reset Settings**.
2. In the **Reset Settings** dialog box, click **Apply**.
   The appliance is restarted.

Generate and download the troubleshooting bundle

To generate the troubleshooting bundle, ensure that you log in to admin portal.

The troubleshooting bundle contains logging information of OMIVV that can be used to assist in resolving issues or sent to Technical Support.

1. On the **APPLIANCE MANAGEMENT** page, click **Generate Troubleshooting Bundle**.
2. Click **Download Troubleshooting Bundle**.

Set up HTTP proxy

1. On the **APPLIANCE MANAGEMENT** page, scroll down to **HTTP PROXY SETTINGS**, and then click **Edit**.
2. Select **Enabled** to enable the use of HTTP proxy settings.
3. Enter the proxy server address in **Proxy Server Address**.
4. Enter the proxy server port in **Proxy Server Port**.
5. Select **Yes** to use proxy credentials.
6. If using proxy credentials, enter the user name in **Username**.
7. Type password in **Password**.
8. Click **Apply**.

Set up Network Time Protocol servers

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

1. On the **APPLIANCE MANAGEMENT** page, click **Edit** in the **NTP Settings** area.
2. Select **Enabled**. Enter the hostname or IP address of a preferred and secondary NTP server and click **Apply**.

3. After configuring NTP, start the terminal console and select the **Sychronize date and time over the network** check box.

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

Configure deployment mode

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

Ensure that the following system requirements for the required deployment modes are fulfilled by assigning these resources to the VM containing OMIVV:

Table 2. System requirements for deployment modes

Deployment modes	Number of hosts	Number of CPUs	Memory (GB)	Minimum Storage
Small	Up to 250	2	8	95 GB
Medium	Up to 500	4	16	95 GB
Large	Up to 1,000	8	32	95 GB
X Large mode	Up to 2,000	12	32	95 GB

ⓘ **NOTE:** MX chassis firmware update feature is supported only on medium, large, and extra large deployment modes.

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

1. On the **APPLIANCE MANAGEMENT** page, scroll down to **Deployment Mode**.
   The configuration values of the deployment mode such as **Small**, **Medium**, **Large**, and **X Large** are displayed. By default, the mode is set to **Small**.
2. To edit a deployment mode based on an environment, click **Edit**.
3. In the **Edit** mode, ensure that the prerequisites are fulfilled and select the required deployment mode.
4. Click **Apply**.
   The allocated CPU and memory are verified against the required CPU and memory for the set deployment mode, and one of more of the following events occur:
   - If the verification fails, an error message is displayed.
   - If the verification is successful, the OMIVV appliance restarts and the deployment mode is 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 the appliance is restarted to enable the deployment mode to be updated.

ⓘ **NOTE:** During the OMIVV appliance bootup, the allocated system resources are verified against the set deployment mode. If the allocated system resources are less than the set deployment mode, the OMIVV appliance does not boot to the login page. To boot the OMIVV appliance, Close the OMIVV appliance, update the system resources to the existing set deployment mode, and complete the downgrade deployment mode task.

Downgrade deployment mode

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

Upgrade deployment mode

1. Clear the browser cache before logging in to the Dell admin portal.
2. Turn on the OMIVV appliance.
3. Log in to the Administration Console.

4. Change the deployment mode to the required level.

Extended monitoring

Ensure to enable Extended Monitoring to support OpenManage Management Pack for vRealize Operations Manager. It is recommended to perform extended monitoring through the 'Medium' deployment mode.

Ensure to enable SNMP Trap Monitoring to support SNMP alerts for OpenManage Management Pack for vRealize Operations Manager. This allows the user to monitor the health status of the server or chassis in real time.

1. Go to https://*<ApplianceIP/hostname/>*.
2. In the left pane, click **APPLIANCE MANAGEMENT**.
3. On the **Appliance Management** page, scroll down to **Extended Monitoring**.
4. To edit the extended monitoring settings, click **Edit**.
5. In the edit mode, enable or disable the extended monitoring and SNMP Trap Monitoring, and then click **Apply**.

Generate a Certificate Signing Request (CSR)

Before registering an OMIVV to a vCenter, ensure that you upload the CSR.

Generating a new 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. On 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**.
2. If you continue with the request, in the **GENERATE CERTIFICATE SIGNING REQUEST** dialog box, enter information about the common name, organization, locality, state, country, and email address. Click **Continue**.
3. Click **Download**, and then save the resulting CSR to an accessible location.

Upload HTTPS certificate

Ensure that the certificate uses the PEM format.

You can use the HTTPS certificates for secure communication between OMIVV appliance and host systems. To set up this type of secure communication, send the CSR certificate to a signing authority, and then upload the resulting CSR using the admin 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.

1. On the **APPLIANCE MANAGEMENT** page, click **Upload Certificate** in the **HTTPS CERTIFICATES** area.
2. Click **OK** in the **UPLOAD CERTIFICATE** dialog box.
3. To upload the certificate, click **Browse**, and then click **Upload**.

   > **NOTE:** If you want to upload a customized CSR to OMIVV, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed on the vSphere Client (HTML-5). To fix this issue, unregister, and re-register the appliance with the vCenter. For more information, see Manage un-registration and re-registration topic in Installation Guide.

After upload HTTPs certificate task is complete, close the browser session and access admin portal in a new browser session.

Restore default HTTPS certificate

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

After restore default HTTPs certificate task is complete, close the browser session and access admin portal in a new browser session.

Set up global alerts

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

1. Go to https://*<ApplianceIP/hostname/>*.
2. In the **Login** dialog box, enter the password.
3. In the left pane, click **ALERT MANAGEMENT**. To enter new vCenter alert settings, click **Edit**.
4. Enter numeric values in the following fields:
   - **Current number of alerts**
   - **Maximum number of alerts**
   - **Number of days to retain alerts**
   - **Timeout for duplicate alerts (seconds)**
5. To save your settings, click **Apply**.

About OMIVV VM console

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

- Configure network settings
- Change the OMIVV appliance password
- Configure NTP and setting the local time zone
- Reboot the OMIVV appliance
- Reset the OMIVV appliance to factory settings
- Log in using read-only role
- Log out from console

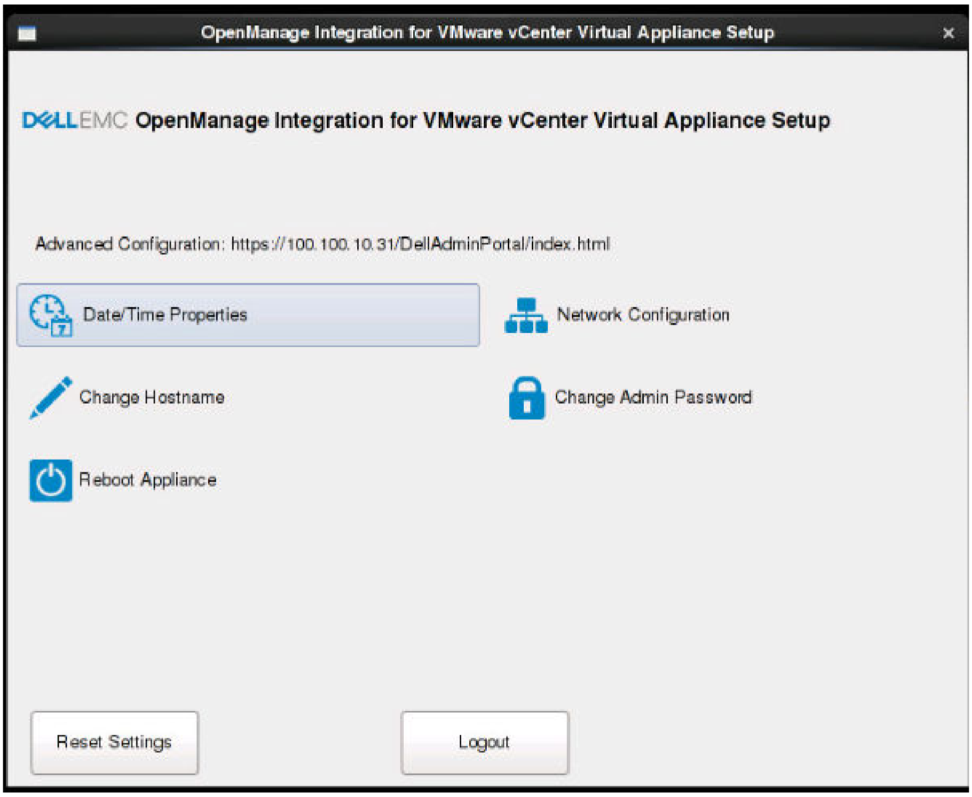
Open OMIVV VM console

To open the OMIVV VM console, launch web or remote console of OMIVV appliance.

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

Configure OMIVV appliance

1. Power on the VM.
2. In the right-pane, click **Launch Web Console**.
3. Log in as an administrator (the default user name is `admin`).
4. If you are logging in for the first time, follow the instructions on the screen to set the password (Admin and ReadOnly users).
5. To configure the OMIVV time zone information, click **Date/Time Properties**.


OpenManage Integration for VMware vCenter Virtual Appliance Setup
DELLEMC OpenManage Integration for VMware vCenter Virtual Appliance Setup
Advanced Configuration: https://100.100.10.31/DellAdminPortal/index.html
Date/Time Properties
Network Configuration
Change Hostname
Change Admin Password
Reboot Appliance
Reset Settings
Logout

NOTE: When the OMIVV appliance is not able to retrieve an IP address from the network (DHCP), `0.0.0.0` is displayed as the IP address. To resolve this, you must manually configure the static IP.

a. On the **Date and Time** tab, select the **Synchronize date and time over the network** check box. The **Synchronize date and time over the network** check box is enabled only after NTP is configured successfully using the Admin portal. For more information about configuring NTP, see Set up Network Time Protocol servers on page 20.

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

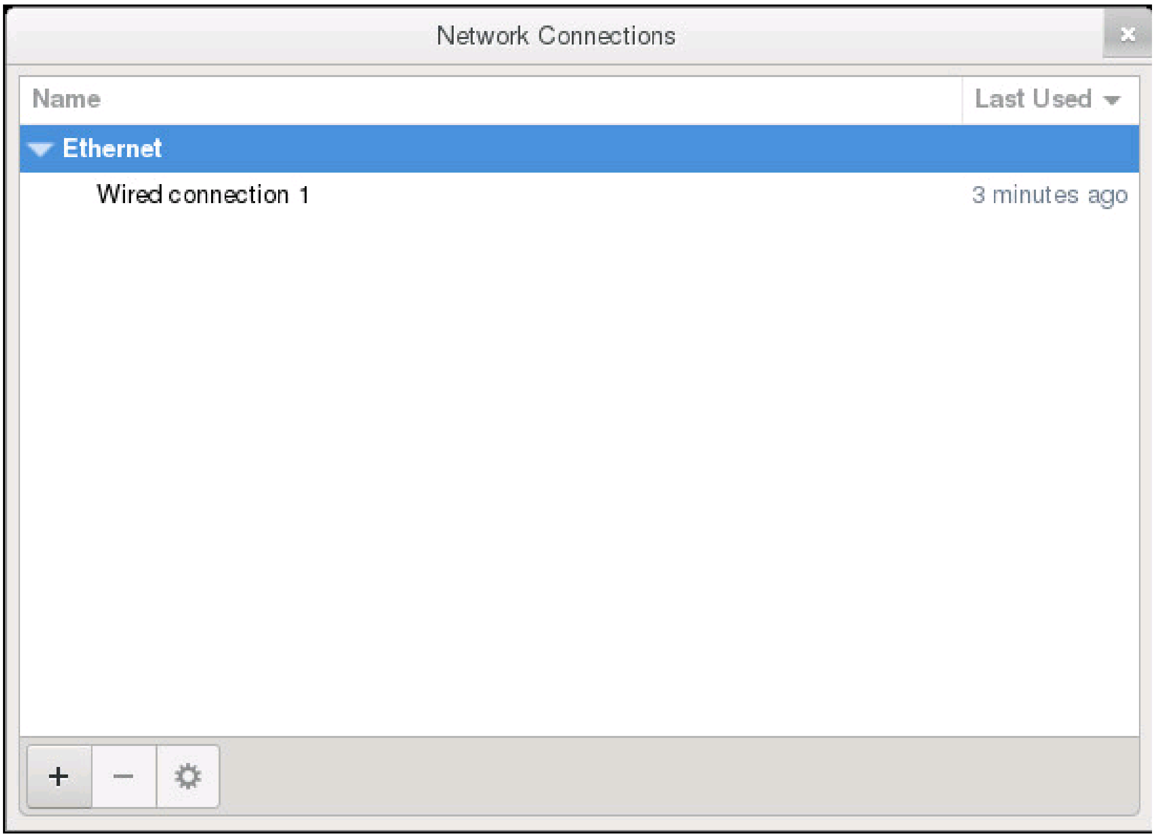
6. To configure network of the OMIVV appliance, click **Network Configuration**.

   To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and OME-Modular).

   If vSphere network and out-of-band network are maintained as separate isolated network in your environment, OMIVV requires access for both the networks. In this case, OMIVV appliance must be configured with two network adapters. Dell EMC recommends configuring both the networks as part of the initial configuration.

   If you can access the out-of-band network using the vSphere network, do not configure two network adapters for the OMIVV appliance. For more information about configuring a second NIC, see Configure OMIVV appliance with two network adapters on page 26.

7. Select **Wired Connection 1** and click ⚙.



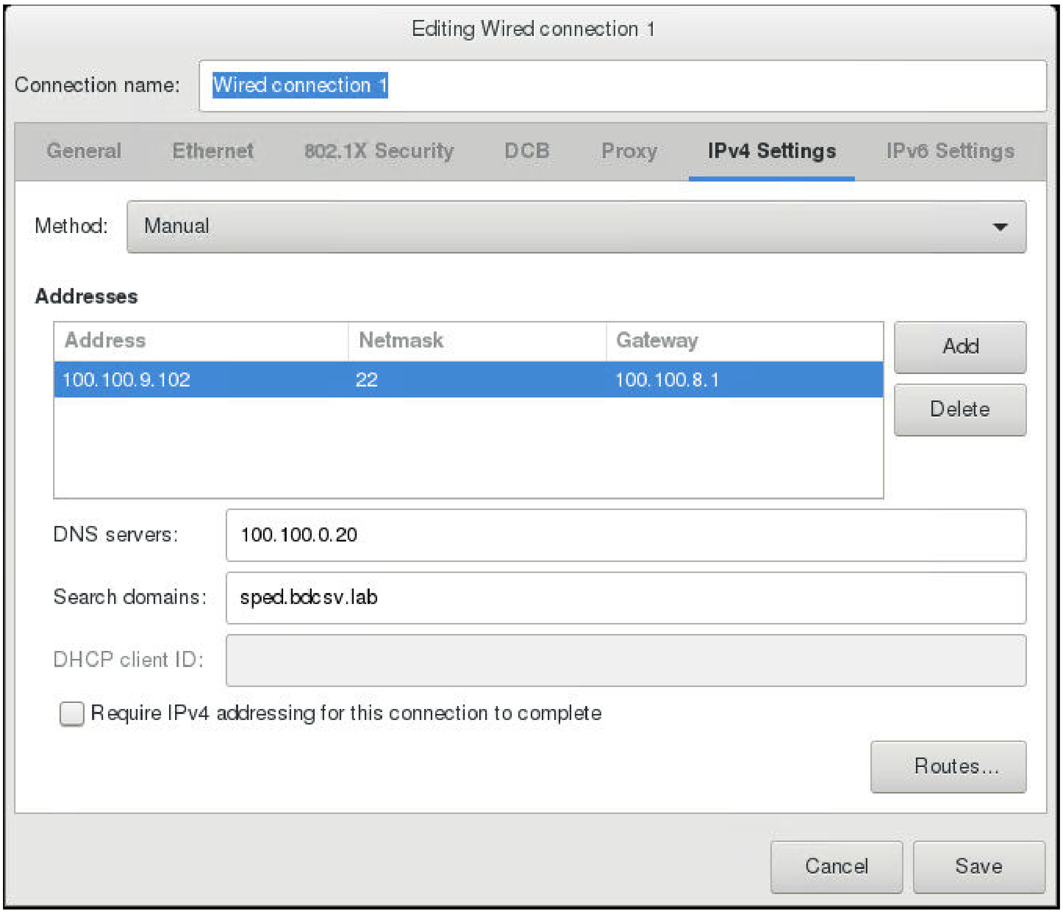
a. Click the **IPv4 Settings** tab, select **Manual** from the **Method** drop-down list, and click **Add**.

   NOTE: If you select Automatic (DHCP), do not enter any IP address because the OMIVV appliance will automatically receive IP from the DHCP server during the next restart.

b. Enter a valid IP, netmask (in the Classless Inter-Domain Routing (CIDR) format), and gateway information.
   If you enter an IP address in the **Netmask** box, it is automatically converted to its respective CIDR format.

c. Enter the DNS server IP and domains to be searched for respectively in the **DNS Servers** and **Search Domains** boxes respectively.

d. Select the **Require IPV4 addressing for this connection to complete** check box and click **Save**.



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
100.100.9.102	22	100.100.8.1

DNS servers: 100.100.0.20

Search domains: sped.bdcsv.lab

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

NOTE:

Sometimes, after you configure the OMIVV appliance with a static IP, the OMIVV terminal utility page does not immediately refresh and display the updated IP. To resolve this issue, exit the OMIVV terminal utility, and then log in again.

8. To change the hostname of the OMIVV appliance, click **Change Hostname**.
   a. Enter a valid hostname, and click **Update hostname**.

      NOTE: If any vCenter servers are already registered with the OMIVV appliance, unregister and re-register all the vCenter instances. For more information, see the Manage un-registration and re-registration topic in the Installation Guide.

9. Restart the appliance.

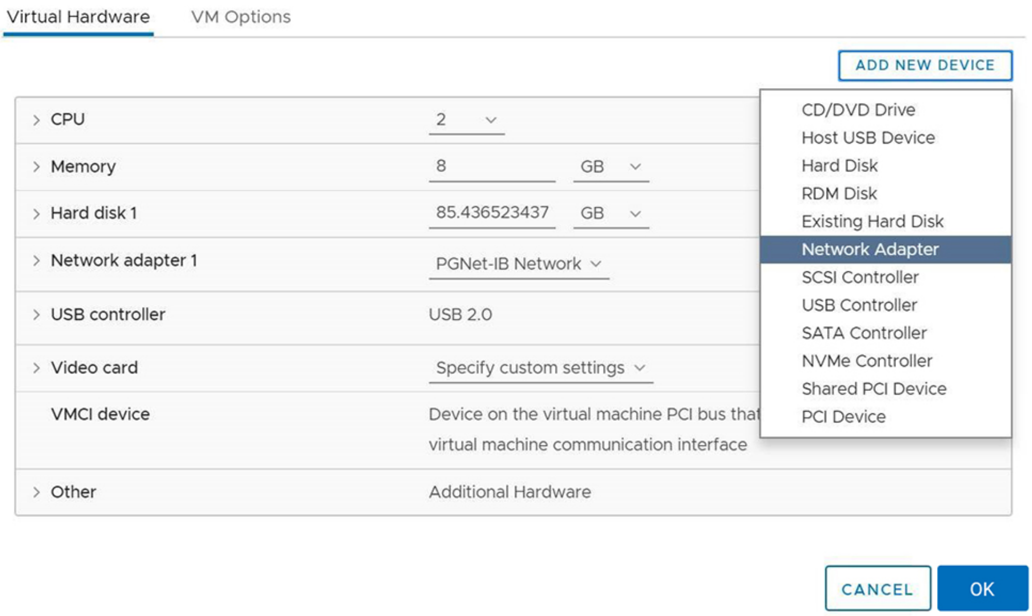
Configure OMIVV appliance with two network adapters

To manage the Dell EMC servers in your vSphere environment, OMIVV requires access to both the vSphere network (vCenter and ESXi management network) and out-of-band network (iDRAC, CMC, and OME-Modular). If vSphere network and out-of-band network are maintained as separate isolated network in your environment, OMIVV requires access for both the networks. In this case, OMIVV appliance must be configured with two network adapters. If the out-of-band network can be accessed using the vSphere network then, do not configure two network adapters for the OMIVV appliance.

Ensure that you have the following information ready for both the out-of-band network and vSphere network:

- IP address, netmask (in the CIDR format), and gateway of the appliance (if static)
- Default gateway—It is mandatory to configure the default gateway to only one network that has an Internet connection. It is recommenced to use vSphere network as the default gateway.
- Routing requirements (Network IP, Netmask, and gateway)—For other external networks that cannot be reached to either through directly or using default gateway, configure the static routes.
- DNS requirements—The OMIVV supports DNS configuration for only one network. For more information about DNS configuration, go to step 9 (b) in this topic.

1. Shut down the OMIVV appliance.
2. Edit the VM settings using the vSphere Client (HTML-5) and add the additional Network adapter. To edit the VM settings, right-click VM, and then click **Edit Settings**.
3. Click **ADD NEW DEVICE**, select **Network Adapter**.



CPU 2

Memory 8 GB

Hard disk 1 85.436523437 GB

Network adapter 1 PGNet-IB Network

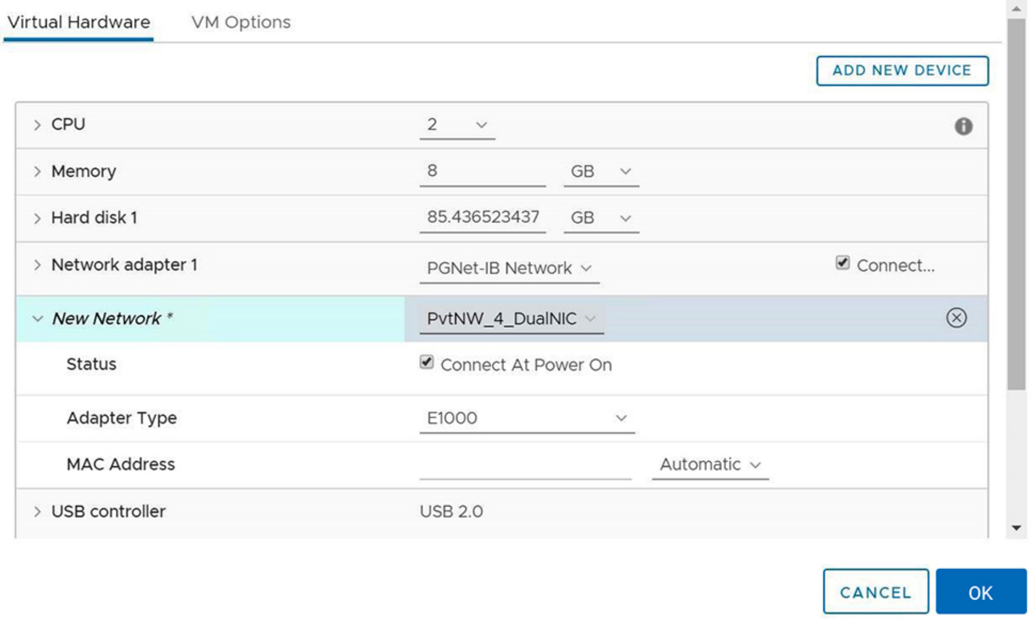
USB controller USB 2.0

Video card Specify custom settings

VMCI device Device on the virtual machine PCI bus that virtual machine communication interface

Other Additional Hardware

   a. Select the appropriate network for the network adapter, and then select the **Connect At Power On** check box.
   b. Select the **E1000** adapter type from the drop-down menu. OMIVV supports only E1000 type of network adapter.



CPU 2

Memory 8 GB

Hard disk 1 85.436523437 GB

Network adapter 1 PGNet-IB Network ☑ Connect...

New Network * PvtNW_4_DualNIC

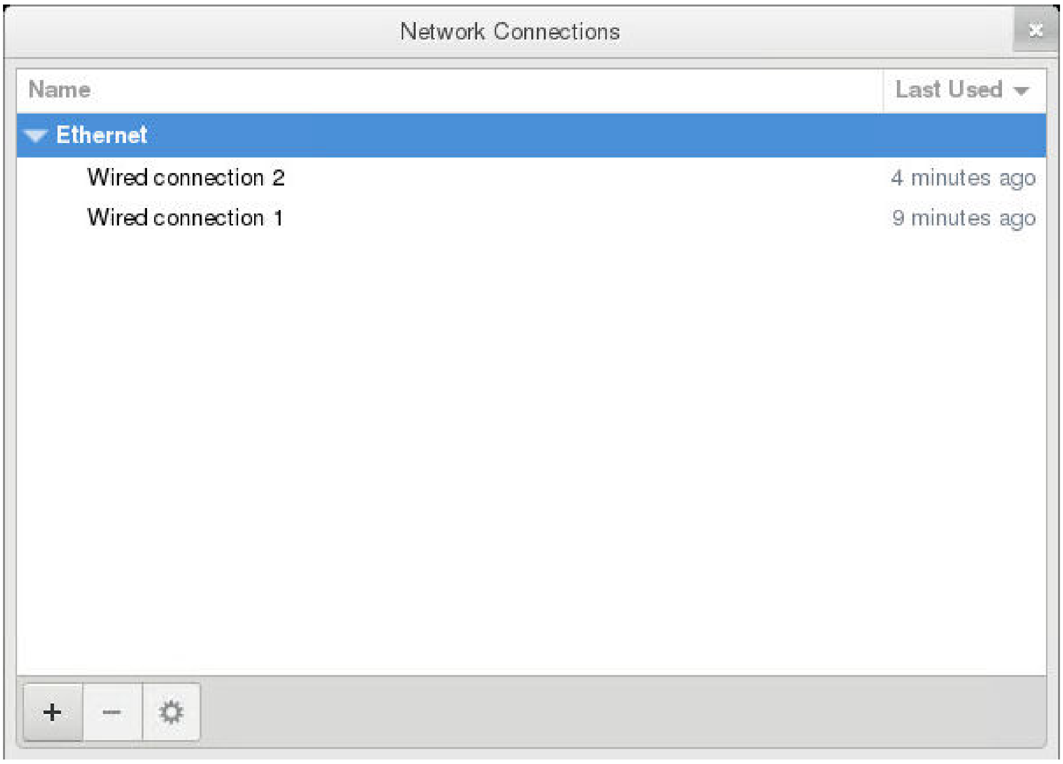
Status ☑ Connect At Power On

Adapter Type E1000

MAC Address Automatic

USB controller USB 2.0

4. Power on the VM. Log in as an administrator (the default user name is Admin), and then press **Enter**.
5. On the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, select **Network Configuration**. The **Network Connections** page displays two NICs.



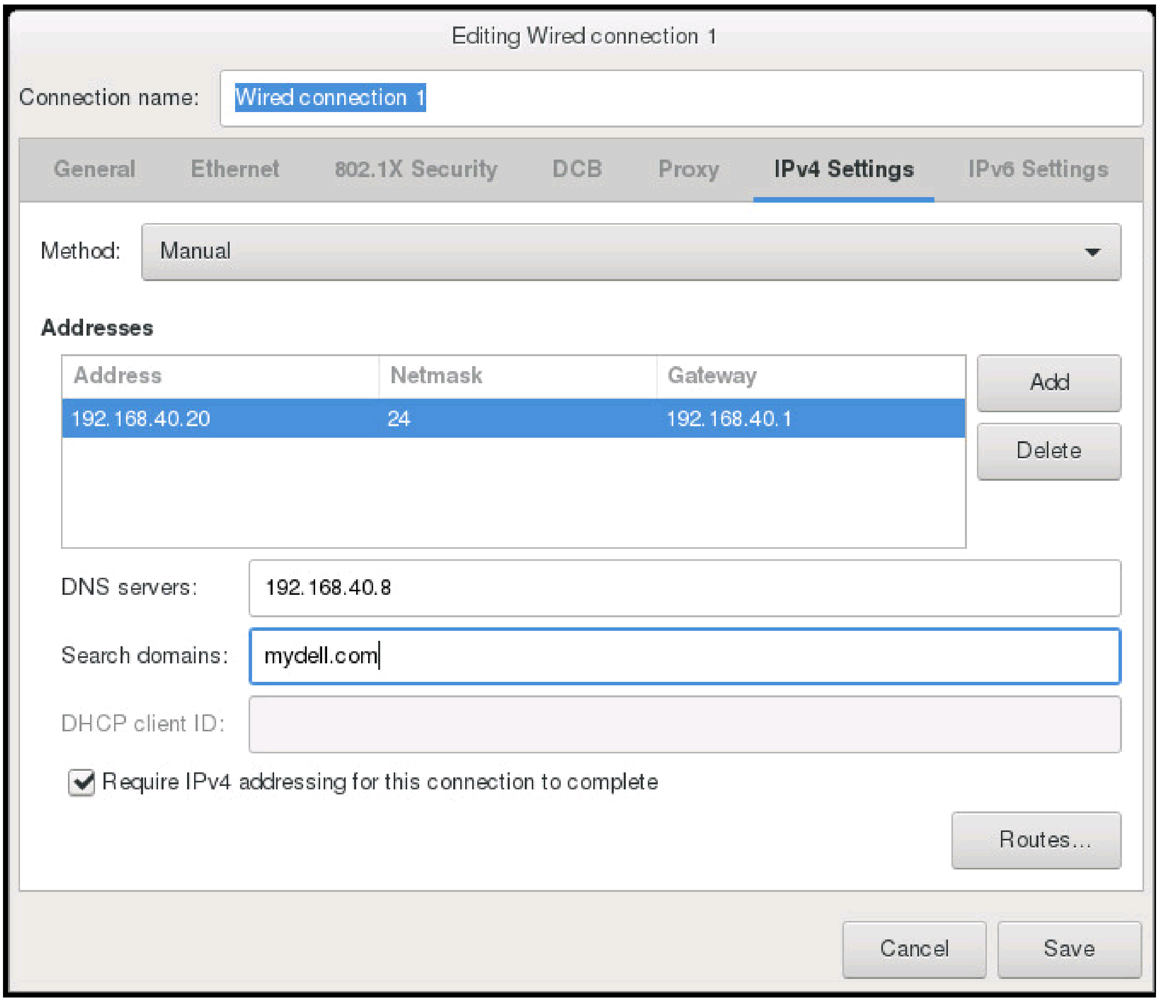
Network Connections

Name	Last Used
Ethernet	
Wired connection 2	4 minutes ago
Wired connection 1	9 minutes ago

⚠ **WARNING: Do not use "+" to add any new network interface. It is mandatory to use the vSphere Edit Settings to add a network adapter.**

6. Select the NIC that you want to configure and click ⚙.
7. To identify the correct NIC, use the MAC ID displayed on the **Ethernet** tab, and then compare it against the MAC ID displayed in the vSphere Client (HTML-5).

   Ensure that you do not change the default MAC address that is listed in the **Ethernet** tab.
8. Click the **General** tab and select the **Automatically connect to this network when it is available** check box.
9. Click the **IPv4 Settings** tab and do the following:



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.40.20	24	192.168.40.1

DNS servers: 192.168.40.8

Search domains: mydell.com

DHCP client ID:

☑ Require IPv4 addressing for this connection to complete

a. Select **Manual** or **Automatic (DHCP)** from the **Method** drop-down list.

b. If you select the **Manual** method, click **Add**, and then enter the valid IP address, Netmask (in the CIDR format), and gateway details. It is recommended to use the static IP in case if you want to control over the priority of the DNS servers (primary and secondary DNS entries).

   Typically, vSphere elements of data center such as vCenter and ESXi hosts are managed using hostname or FQDN. iDRAC, CMC, and OME-Modular are managed using IP addresses. In this case, Dell EMC recommends you to configure the DNS settings only for the vSphere network.

   If both vSphere network and iDRAC management network are managed by using hostname or FQDN, DNS server must be configured in such a manner that it resolves the hostname or FQDN for both the networks. For more information, see the CentOS documentation.

   NOTE: The last configured DNS server becomes the primary DNS irrespective of which network the DNS is configured for.

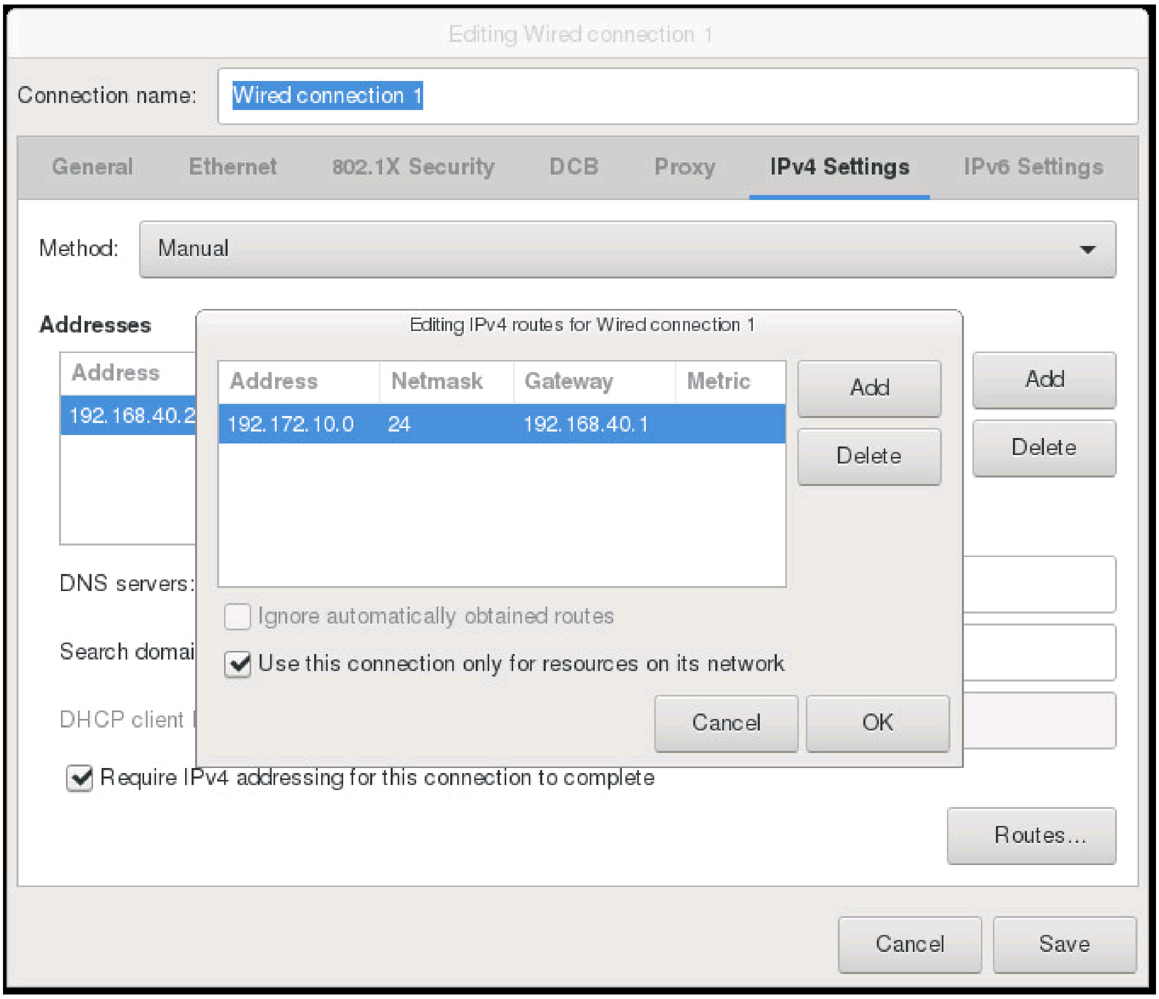
c. Enter the DNS server IP and domains to be searched for in the **DNS Servers** and **Search Domains** boxes respectively.

d. Select the **Require IPV4 addressing for this connection to complete** check box and click **SAVE**.

e. If you do not want to use this network as the default network (gateway), click **Routes**, and then select the **Use this connection only for resources on its network** check box.

   NOTE: Adding multiple networks as default gateways may result in network issues and OMIVV functions may get affected.

f. If you want to reach to any external network using the known gateways, click **Add** on the same page, and then add the network IP address, netmask (in the CIDR format), and gateway details.



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address
192.168.40.2

Editing IPv4 routes for Wired connection 1

Address	Netmask	Gateway	Metric
192.172.10.0	24	192.168.40.1	

□ Ignore automatically obtained routes

☑ Use this connection only for resources on its network

☑ Require IPv4 addressing for this connection to complete

Typically, the network that you have configured as the default gateway does not require any manual route configuration because the gateway is capable of providing the reachability. However, for networks where default gateway is not configured (the **Use this connection only for resources on its network** check box is selected), a manual route configuration may be required. Because the default gateway is not configured for this network to reach external networks, manual routing configurations are required.

NOTE: Incorrect routing configuration may abruptly stop the network interface from responding. Ensure to configure the routing entries appropriately.

g. Click **OK**.

10. Click **Save** . To configure another NIC, repeat the tasks 6–10.
11. Go to the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Reboot Appliance**. The network configuration is complete only after restarting the OMIVV appliance.

NOTE:

After the appliance is successfully restarted, the NICs start working as configured. The status of NICs can be viewed by logging in as **readonly** user and running the following commands: `ifconfig`, `ping`, and `route -n`.

Change OMIVV appliance password

You can change the OMIVV appliance password in the vSphere Client by using the console.

1. Open the OMIVV VM console. See Open OMIVV VM console on page 23.
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 letter.

4. Enter a new password in **Enter new Admin Password**, and click **Change Password**.
5. Retype the new password in **Please Confirm Admin Password**, and press **Enter**.

Configure NTP and setting local time zone

1. Open the OMIVV VM console. See Open OMIVV VM console on page 23.
2. To configure the OMIVV time zone information, click **Date/Time Properties**.

   Ensure to enter the NTP details in Admin console. For more information, see Set up Network Time Protocol servers on page 20.
3. On the **Date and Time** tab, select **Synchronize date and time over the network**.
   The **NTP Servers** window is displayed.
4. To add another NTP server IP or hostname (if required), click the **Add** button, and then press **TAB**.
5. Click **Time Zone**, select the applicable time zone, and then click **OK**.

Change hostname of OMIVV appliance

1. On the OMIVV setup utility, click **Change Hostname**.

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

2. Enter an updated hostname.
   Type the domain name in the format: *<hostname>*.
3. Click **Update Hostname**.
   The appliance hostname is updated and main menu page is displayed.
4. To reboot the appliance, click **Reboot Appliance**.

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

Reboot OMIVV appliance

1. Open the OMIVV VM console. See Open OMIVV VM console on page 23.
2. Click **Reboot Appliance**.
3. To reboot the appliance, click **Yes**.

Reset OMIVV appliance to factory settings

1. Open the OMIVV VM console. See Open OMIVV VM console on page 23.
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**.
   If you click **Yes**, the OMIVV appliance is reset to the factory default settings and all other settings and existing data is deleted.

   After the factory reset is complete, register vCenters to OMIVV appliance again.

> **NOTE:** When the OMIVV appliance is reset to factory default settings, any updates that you had done on the network configuration are preserved. These settings are not reset.

Read-only user role

There is a unprivileged user called "readonly" with shell access for diagnostic purposes. The read-only user has limited privileges to run few commands.

3

Monitor hosts and chassis using dashboard

The dashboard displays the following:

- The health status of hosts and chassis
- Warranty status of hosts and chassis
- Hosts and vCenter license information
- Configuration compliance status
- Jobs states
- Total number of compliant bare-metal servers that are available for deployment
- Quick references

Health

The **Health** section displays the health status of all the OMIVV-managed hosts and chassis. The hosts that are displayed here are configured using the same Platform Service Controller (PSC).

The status of each host and chassis refreshes after the completion of a periodic health metric task or SNMP event from host and chassis.

The following list describes the different health states of the hosts and the chassis:

- **Healthy**—Displays the count of host and chassis that are in healthy state.
- **Warning**—Displays the count of host and chassis that require corrective action, but does not immediately affect the system.
- **Critical**—Displays the count of host and chassis that have critical issues with one or more components in host or chassis and these issues must be fixed immediately.
- **Unknown**—Displays the count of host and chassis that are in unknown state. The host or chassis shows Unknown state when the host or chassis is not reachable or health state is unknown.

NOTE: When several traps for the same server are received in a minute, health metric, and extended metric jobs for the server may fail to run. The health status of those servers is reported as Unknown until the next successful health metrics job.

To view more information about hosts, click **VIEW HOST**.

To view more information about chassis, click **VIEW CHASSIS**.

Warranty

The number of hosts that are displayed under this warranty category indicates the hosts that belong to vCenter servers configured using the PSC. To get the warranty information about host and chassis, ensure that you enabled the warranty expiration notification on the **Settings** page.

The **Warranty** section provides the following information about hosts and chassis:

- **Healthy**—Displays the number of hosts and chassis for which remaining warranty days are above warning threshold.
- **Warning**—Displays the number of hosts and chassis for which remaining warranty days are below warning threshold.
- **Critical**—Displays the number of hosts and chassis for which remaining warranty days are below critical threshold.
- **Unknown**—Displays the number of hosts and chassis whose warranty is unknown.

Licenses

The **Licenses** section displays the following information:

- The total number of available host and vCenter licenses
- The total number of host and vCenter licenses that are in use.

To purchase license, click **BUY LICENCE**.

Ready for Deployment

The number of bare-metal servers lists only the compliant bare-metal servers that are discovered using OMIVV. To deploy the bare-metal servers, click **DEPLOY**.

Configuration Compliance

The **Configuration Compliance** section displays the hosts that are part of cluster which is associated with the cluster profile. The hosts that are displayed here are configured using the same Platform Service Controller (PSC). To view the configuration compliance status of hosts, click **VIEW COMPLIANCE**.

Jobs

The **Jobs** section displays the jobs that are scheduled using OMIVV. The job details are displayed only for last 7 days. The pie chart displays the total number jobs in **Successful**, **In Progress**, **Failed**, **Scheduled**, and **Cancelled** states. To filer the job states in the pie chart, click the job states.

You can view the different types of jobs and total number jobs in Successful, In progress, Failed, Scheduled, and Canceled states for the following jobs:

- Deployment Jobs. For more information, see Deployment jobs on page 71.
- Host Firmware Update Jobs. For more information, see Host firmware update jobs on page 72.
- Chassis Firmware Update Jobs. For more information, see Chassis firmware update jobs on page 71.
- System Lockdown Jobs. For more information, see System Lockdown Mode jobs on page 73.

To view the status of all the jobs, click **VIEW**.

Quick References

This section provides the quick references to the following features:

- Start Initial Configuration Wizard. See Initial configuration on page 84
- Host Credential Profile. See Host credential profile on page 35
- Management Compliance. See Management Compliance on page 66
- Chassis Credential Profile. See Chassis credential profile on page 40
- Cluster Profile. See Cluster profile on page 49
- Deployment. See Deployment on page 56

4

Manage hosts using host credential profile

Host credential profile

A host credential profile stores the iDRAC and host credentials that OMIVV uses to communicate with the servers. Each server must be associated to a host credential profile to be managed by OMIVV. You can associate multiple servers to a single host credential profile.

The PowerEdge MX chassis host can be managed using a single unified chassis management IP. The hosts present in the PowerEdge MX chassis with an iDRAC IP disabled have to be managed using chassis credential profile. To manage the PowerEdge MX chassis using a chassis credential profile, see Create chassis credential profile on page 40. Dell EMC recommends managing the PowerEdge MX chassis hosts with an iDRAC IP using host credential profile to get complete OMIVV functions.

Related tasks

Create host credential profile on page 35

Edit host credential profile on page 37

View host credential profile on page 38

Test host credential profile on page 39

Delete host credential profile on page 39

Create host credential profile

If the number of added hosts exceeds the license limit for creating a host credential profile, you cannot create a host credential profile.

Before using the Active Directory (AD) credentials with a host credential profile, ensure that:

- The user account exists in AD.
- The iDRAC or host is configured for an AD–based authentication.

1. On the OMIVV home page, click **Compliance & Deployment** > **Host Credential Profile**.
2. On the **Create Host Credential Profile** page, click **CREATE NEW PROFILE**.
3. On the **Host Credential Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
4. On the **Name and Credentials** page, do the following:
   a. Enter the profile name and description. The description field is optional.
   b. From the **vCenter Name** list, select an instance of vCenter on which you want to create the host credential profile.

      NOTE: If you select **All Registered vCenters** while creating the host credential profile, test connection fails for all hosts running ESXi 6.5 or later that have the WBEM service disabled. In such case, Dell EMC recommends completing the host credential profile wizard actions, run the inventory on hosts, and then test the host credential profile again.

   c. In the **iDRAC Credentials** area, enter the iDRAC local credentials or AD credentials.

      - To enter the local credentials of iDRAC, perform the following tasks:
        - Enter the user name in the **User Name** box. The user name is limited to 16 characters. For information about defining user names, see the *iDRAC User's Guide* available at **dell.com/support**.
        - Enter password. For more information about the recommended characters in user names and passwords, see the *iDRAC User's Guide* available at **dell.com/support**.
        - To download and store the iDRAC certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.

- To enter the credentials for an iDRAC that is already configured and enabled for AD, select the **Use Active Directory** check box.

  ⓘ **NOTE:** The iDRAC account requires administrative privileges for updating firmware and deploying an OS.

  - Enter the user name in the **Active Directory User Name** box. Enter 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.
  - Enter password.

    The AD credential can be either same or separate for both the iDRAC and hosts.
  - To download and store the iDRAC certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.

d. In the **Host Root** area, enter the host local credentials or AD credentials.

- To enter the local credentials of ESXi host, perform the following tasks:
  - The default username is **root**. You cannot edit it.
  - Enter password.
  - To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
- To enter the credentials for hosts that are already configured and enabled for AD, select the **Use Active Directory** check box.
  - Enter the user name in the **Active Directory User Name** box. Enter 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.
  - Enter password.
  - To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.

ⓘ **NOTE:** For hosts running ESXi 6.5 U2 and later versions, OMIVV can obtain the iDRAC information even if incorrect host credentials are entered.

5. Click **Next**.

   The **Select Hosts** page is displayed.

   ⓘ **NOTE:** If you try to manage all the OMIVV-managed hosts in a single host credential profile, it may take few minutes to display the Dell inventory notification in vCenter. This delay might be seen when you add large number of hosts to a host credential profile for the first time. Subsequent inventory runs normally.
6. On the **Select Hosts** page, expand the tree view and select the hosts, and then click **OK**.
   - Click **ADD HOST** to add or remove hosts from the **Associated Hosts** page.

     ⓘ **NOTE:** Do not add a PowerEdge MX server with a disabled iDRAC IPv4 to a host credential profile. These servers are managed using a chassis credential profile.

   The selected hosts are displayed on the **Associated Hosts** page.
7. To test the connection, select one or more hosts, and click **BEGIN TEST**. Dell EMC recommends you to test the connection for all configured hosts.

   ⓘ **NOTE:** Even after entering valid credentials, the test connection operation may fail for host, and a message is displayed indicating that invalid credentials are entered. This issue is observed if ESXi is blocking the access. Multiple attempts to connect the ESXi by using incorrect credentials blocks you from accessing ESXi for 15 minutes. Wait 15 minutes and retry the operation.

   - To stop the test connection process, click **ABORT TEST**.

   You can view the test connection results in the **TEST RESULTS** section.

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

   ⓘ **NOTE:** Testing iDRAC connectivity in a host credential profile using an incorrect password locks the iDRAC access to the appliance until the penalty time configured in iDRAC. Retry with the correct password after the penalty time specified in the IP filtering and blocking settings in iDRAC.
8. Click **Finish**.

Related tasks

Edit host credential profile on page 37

Delete host credential profile on page 39

Related information

Host credential profile on page 35

Edit host credential profile on page 37

Delete host credential profile on page 39

Test host credential profile on page 39

Edit host credential profile

You can edit the credentials of multiple host credential profiles at a time.

1. On the **Name and Credentials** page, do the following:
    a. Edit the profile name and description.
    b. In the **iDRAC Credentials** area, edit the iDRAC local credentials or AD credentials.

        > **NOTE:** If you select **All Registered vCenters** while creating the host credential profile, the test connection may fail for all hosts running ESXi 6.5 or later with WBEM service disabled. Dell EMC recommends that you complete the host credential profile wizard actions, run the inventory on the hosts, and test the host credential profile connection again.

        - To change the local credentials of iDRAC, perform the following tasks:
            - Change the user name in the **User Name** box. The user name is limited to 16 characters. For information about defining user names, see the *iDRAC User's Guide* available at **dell.com/support**.
            - Change password.
            - To download and store the iDRAC certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
        - To change the credentials for an iDRAC that is already configured and enabled for AD, select the **Use Active Directory** check box.

            > **NOTE:** The iDRAC account requires administrative privileges for updating firmware and deploying an OS.

            - Change the user name in the **Active Directory User Name** box. Enter the user name in one of the formats such as `domain\username` or `username@domain`. The user name is limited to 256 characters. For more information about defining user names, see the *Microsoft Active Directory Documentation*.
            - Change password.
            - To download and store the iDRAC certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.
    c. In the **Host Root** area, enter the host local credentials and AD credentials.
        - To change the local credentials of ESXi host, do either of the following:
            - The default username is **root**. You cannot edit it.
            - Change password.
            - To download and store the host certificate and validate it during all the future connections, select the **Enable Certificate Check** check box.
        - To change the credentials for hosts that are already configured and enabled for AD, select the **Use Active Directory** check box.
            - Change the user name in the **Active Directory User Name** box. Enter 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.
            - Change password.
            - To download and store the host certificate and validate it during all future connections, select the **Enable Certificate Check** check box.
2. Click **Next**.

The **Associated Hosts** page is displayed.

3. To add or remove the hosts from the associated hosts list, on the **Associated Hosts** page, click **ADD HOST**.

   > **NOTE:** Do not add a PowerEdge MX server with a disabled iDRAC IPv4 to a host credential profile. These servers are managed using a chassis credential profile.

   The selected hosts are displayed on the **Associated Hosts** page.

4. To test the connection, select one or more hosts, and then click **BEGIN TEST**. Dell EMC recommends that you test the connection for all configured hosts.

   > **NOTE:** Even after entering valid credentials, the test connection operation may fail for host, and a message is displayed indicating that invalid credentials are entered. This issue is observed if ESXi is blocking the access. Multiple attempts to connect the ESXi by using incorrect credentials blocks you from accessing ESXi for 15 minutes. Wait 15 minutes and retry the operation.

   - To stop the test connection, click **ABORT TEST**.

   You can view the test connection results in the **TEST RESULTS** section.

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

5. Click **Finish**.

   > **NOTE:** The Date Modified and Last Modified By fields include changes that you perform through the vSphere Client interface for a host credential profile. Any changes that the OMIVV appliance performs on the respective host credential profiles do not affect these two fields.

Related tasks

Create host credential profile on page 35

Delete host credential profile on page 39

Related information

Host credential profile on page 35

Create host credential profile on page 35

Delete host credential profile on page 39

Test host credential profile on page 39

View host credential profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Host Credential Profile**.
   A table displays all the host credential profiles along with the following information:

   - **Profile Name**—Name of the host credential profile
   - **Description**—Profile description, if provided
   - **vCenter**—FQDN, or hostname, or IP address of the associated vCenter
   - **Associated Hosts**—The hosts that are associated with the host credential profile. If more than one associated hosts are present, use the expand icon to display all.
   - **iDRAC Certificate Check**—Indicates if the iDRAC certificate is verified when creating a host credential profile.
   - **Host Root Certificate Check**—Indicates if the host root certificate is verified when creating a host credential profile.
   - **Date Created**—Date when the host credential profile is created.
   - **Date Modified**—Date when the host credential profile is modified.
   - **Last Modified By**—Details of the user who modified the host credential profile.

   > **NOTE:** If the PowerEdge MX host is managed using the chassis credential profile, the OMIVV indicates it as associated to a chassis credential profile. For more information, see View chassis credential profile on page 42.

2. If you want to remove or add the column names from the wizard, click ▥.

   By default, the **Date Modified** and **Last Modified** columns are not selected. To select these columns, click ▥.

3. To export the host credential profile information, click ⇥.

Related information

Host credential profile on page 35

Test host credential profile

Using the test credential profile feature, you can test the host and iDRAC credentials. Dell EMC recommends selecting all the hosts.

1. On the OMIVV home page, select a host credential profile that has associated hosts, and then click **TEST**.
   The **Test Host Credential Profile** page is displayed.
2. Select all the associated hosts and click **BEGIN TEST**.
   a. To stop the test connection, click **ABORT TEST**.

   Test connection results for both iDRAC and host credentials are displayed.

Related tasks

Create host credential profile on page 35
Edit host credential profile on page 37

Related information

Host credential profile on page 35

Delete host credential profile

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

OMIVV does not manage the hosts that are part of the host credential profile that you deleted, until those hosts are added to another host credential profile.

1. On the **Host Credential Profile** page, select a profile, and click **DELETE**.
2. When prompted to confirm, click **DELETE**.
   The selected profile is removed from the host credential profile list.

Related tasks

Create host credential profile on page 35
Edit host credential profile on page 37

Related information

Host credential profile on page 35
Create host credential profile on page 35
Edit host credential profile on page 37

5

Manage chassis using chassis credential profile

Chassis credential profile

A chassis credential profile stores the chassis credentials that OMIVV uses to communicate with the chassis. OMIVV manages and monitors the chassis which are associated to a chassis credential profile. You can assign multiple chassis to a single chassis credential profile.

The PowerEdge MX chassis host can be managed using a single unified chassis management IP. The hosts present in the PowerEdge MX chassis with an iDRAC IP disabled have to be managed using chassis credential profile. Dell EMC recommends managing the PowerEdge MX chassis hosts with an iDRAC IP using host credential profile to get complete OMIVV functions. For more information about managing MX chassis, see Manage PowerEdge MX chassis on page 106.

Related tasks

Create chassis credential profile on page 40
Edit chassis credential profile on page 41
View chassis credential profile on page 42
Delete chassis credential profile on page 43

Create chassis credential profile

- To create a chassis credential profile, you must have the following privileges:
  - M1000e, VRTX, and FX2 chassis—Read and Set SNMP trap destination
  - PowerEdge MX chassis—Administrator
- Before using the Active Directory (AD) credentials with a host credential profile, ensure that:
  - The user account exists in AD.
  - The CMC or OME-Modular is configured for AD-based authentication.

1. On the OMIVV home page, click **Compliance & Deployment** > **Chassis Credential Profile** > **CREATE NEW PROFILE**.
2. On the **Chassis Credential Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
3. On the **Name and Credentials** page, do the following:
   a. Enter profile name and description. The description is optional.
   b. In the **User name** text box, enter the user name with administrative rights, which is typically used to log in to the Chassis Management Controller (CMC) or OpenManage Enterprise-Modular (OME-Modular).
   c. In the **Password** text box, enter the password.
   d. In the **Verify Password** text box, enter the same password that you have entered in the **Password** text box. The passwords must match.
4. On the **Select Chassis** page, select an individual chassis or multiple chassis using the check boxes next to the **IP/Host Name** column, and then click **OK**.
   The selected chassis is displayed on the **Associated Chassis** page. To add or remove the chassis from the associated chassis list, click **ADD CHASSIS**.

   If the selected chassis is already associated with a chassis credential profile, the following message is displayed: *Selecting a chassis currently associated to another profile will remove the chassis from that Chassis Credential Profile. A chassis credential profile without associated chassis will be deleted.*

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.

Test connection 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

The test result is displayed in the **Test Results** section as **Passed** or **Failed**. To test the chassis connectivity manually, select the chassis and click **BEGIN TEST**.

For a PowerEdge 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 fails and test result status is indicated as Fail. The lead chassis IP link is displayed. Click the lead chassis IP link to discover the complete MCM group.

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

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

5. Click **FINISH**.

   Ensure that you have at least one successfully validated chassis to complete the tasks in the wizard.

   To add the PowerEdge MX chassis, see Add PowerEdge MX Chassis on page 107.

Related tasks

Edit chassis credential profile on page 41
Delete chassis credential profile on page 43

Related information

Chassis credential profile on page 40
Edit chassis credential profile on page 41
Delete chassis credential profile on page 43
Test chassis credential profile on page 43

Edit chassis credential profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Chassis Credential Profile**.
2. On the **Chassis Credential profile** page, click **EDIT**.
3. On the **Name and Credentials** page, do the following:
   a. Edit the profile name and description. The description is optional.
   b. In the **User name** text box, change the user name with administrative rights, which is typically used to log in to the Chassis Management Controller (CMC) or OpenManage Enterprise-Modular (OME-Modular).
   c. In the **Password** text box, change the password.
   d. In the **Verify Password** text box, enter the same password that you have entered in the **Password** text box. The passwords must match.
4. On the **Select Chassis** page, select or remove the chassis using the check boxes next to the **IP/Host Name** column, and then click **OK**.
   The selected chassis is displayed on the **Associated Chassis** page. To add or remove the chassis from the associated chassis list, click **ADD CHASSIS**.

   If the selected chassis is already associated with a host credential profile, the following message is displayed: *Selecting a chassis currently associated to another profile will remove the chassis from that Chassis Credential Profile. A chassis credential profile without associated chassis will be deleted.*

   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.

   Test connection 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

The test result is displayed in the **Test Results** section as **Passed** or **Failed**. To test the chassis connectivity manually, select the chassis and click **BEGIN TEST**.

For a PowerEdge 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 fails and test result status is indicated as Fail. The lead chassis IP link is displayed. Click the lead chassis IP link to discover the complete MCM group.

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

NOTE: Only successfully validated chassis is associated with a chassis credential profile.

5. Click **FINISH**.

   Ensure that you have at least one successfully validated chassis to complete the tasks in the wizard.

   To add a PowerEdge MX chassis, see Add PowerEdge MX Chassis on page 107.

Related tasks

Create chassis credential profile on page 40
Delete chassis credential profile on page 43

Related information

Chassis credential profile on page 40
Create chassis credential profile on page 40
Delete chassis credential profile on page 43
Test chassis credential profile on page 43

View chassis credential profile

After you create one or more chassis credential profiles, you can view the chassis and the associated chassis on the chassis credential profile page.

1. On the OMIVV home page, click **Compliance & Deployment** > **Chassis Credential Profile**.

   A table displays all the chassis credential profile along with the following information:

   - **Profile Name**—The name of the chassis credential profile
   - **Description**—Profile description
   - **Chassis IP/Host Name**—The chassis IP or hostname link

     For a Multi-chassis Management (MCM) group, the lead chassis (▥) and the member chassis (▥) are listed in hierarchy.

     NOTE: For an PowerEdge MX chassis in an MCM configuration, OMIVV manages all the lead and member chassis using lead chassis only. All the lead and members are associated to the same chassis credential profile to which lead chassis is associated.

     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 parentheses.

   - **Chassis Service Tag**—The unique identifier that is assigned to a chassis.
   - **Date Modified**—The date when the chassis credential profile is modified.
2. 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**

3. To export the chassis credential profile information, click ⇥.

Related information

Chassis credential profile on page 40

Test chassis credential profile

Using chassis test credential profile feature, you can test the credentials of a chassis that is associated with the chassis credential profile. Dell EMC recommends selecting all the chassis.

1. On the OMIVV home page, click **Compliance & Deployment** > **Chassis Credential Profile**.
2. Select a chassis credential profile and click **TEST**.
3. On the **Test Chassis Credential Profile** page, select the associated chassis and click **BEGIN TEST**.
   a. To stop the test connection, click **ABORT TEST**.

   Test result is displayed in the **Test Result** column.

Related tasks

Create chassis credential profile on page 40

Edit chassis credential profile on page 41

Delete chassis credential profile

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

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

1. On the OMIVV home page, click **Compliance & Deployment** > **Chassis Credential Profile** > **DELETE**.
2. Select a chassis credential profile that you want to delete.
3. When prompted to confirm, click **DELETE**.

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

Related tasks

Create chassis credential profile on page 40

Edit chassis credential profile on page 41

Related information

Chassis credential profile on page 40

Create chassis credential profile on page 40

Edit chassis credential profile on page 41

6

Manage firmware and driver repositories using repository profile

Repository profile

A repository profile enables you to create and manage driver or firmware repositories.

You can use the firmware and driver repository profiles to:

- Update firmware of hosts
- Update driver for hosts that are part of vSAN clusters.
- Create cluster profile and baseline the clusters.

The default OMIVV firmware catalogs are:

- **Dell EMC Default Catalog**: A factory-created firmware repository profile that uses Dell EMC Online catalog to get the latest firmware information. If the appliance does not have an Internet connection, modify this repository to point to a local CIFS, or NFS, or HTTP, or HTTPs based shares. For more information about modifying this catalog, see Edit or customize Dell Default Catalog on page 46.

  You can select Dell EMC Default Catalog as the default catalog to update the firmware of vSphere hosts which are not associated with any cluster profile.

- **Validated MX Stack Catalog**: A factory-created firmware repository profile that uses the Dell EMC online catalog to get the validated firmware information for MX chassis and its corresponding sleds. For more information about modifying this catalog, see Edit Validated MX Stack Catalog on page 47. For more information about the Validated MX Stack catalog, see the technical white paper available at MX7000 Firmware Update.

  NOTE: You cannot use Dell EMC Default Catalog and Validated MX Stack Catalog repository profiles to baseline the vSAN clusters.

Related tasks

Create repository profile on page 44

Edit repository profile on page 45

View repository profile on page 47

Delete repository profile on page 47

Create repository profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **Repository Profile**.
2. On the **Repository Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
3. On the **Profile Name and Description** page, enter profile name and description. The description field is optional and limited to 255 characters.
4. Click **NEXT**.
   The **Profile Settings** page is displayed.
5. On the **Profile Settings** page, select **Firmware** or **Driver**.

   The following are applicable for driver repository profile:

   - Driver repository profile can have a maximum of 10 drivers. If more files are present, the selection of driver is random.
   - Only offline driver bundles (.zip files) are used.

- For driver repository, download the offline driver bundles (.zip files) and save to the shared location by providing the full path of the shared location. OMIVV automatically creates the catalog inside the OMIVV appliance. Driver bundles are available at https://my.vmware.com/web/vmware/downloads
- OMIVV requires write access to the CIFS or NFS.
- Files within the subfolders are ignored.
- Files exceeding 10-MB sizes are ignored.
- Driver repository is applicable only for vSAN clusters.

6. In the **Repository Share Location** area, perform the following tasks:
   a. Enter the repository share location (NFS or CIFS).
   b. For CIFS, enter the credentials.

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

      ⓘ **NOTE:** For SMB 1.0 share used for driver repository, add the file separator at the end of the directory path.
7. To validate the catalog path and credentials, click **BEGIN TEST**.

   To continue creating a repository profile, you must complete this validation process.

   The test connection results are displayed.
8. Click **NEXT**.
   The **Synchronize with repository location** page is displayed.
9. Click **NEXT**.
   The **Summary** page is displayed that provides the information about the repository profile.
10. Click **FINISH**.
    After creating the catalog, it downloads, parses, and the status is displayed on the home page of the repository profile.

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

Related tasks

Edit repository profile on page 45

Delete repository profile on page 47

Related information

Repository profile on page 44

Edit repository profile on page 45

Delete repository profile on page 47

Initial configuration on page 84

Edit repository profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Repository Profile** > **EDIT**.
2. On the **Profile Name and Description** page, edit profile name and description and then click **NEXT**.
3. On the **Profile Settings** page, select **Firmware** or **Driver**.

   The following are applicable for driver repository profile:

   - Driver repository profile can have a maximum of 10 drivers. If more files are present, the selection of driver is random.
   - Only offline driver bundles (.zip files) are used.
   - For driver repository, download the offline driver bundles (.zip files) and save to the shared location by providing the full path of the shared location. OMIVV automatically creates the catalog inside the OMIVV appliance. Driver bundles are available at https://my.vmware.com/web/vmware/downloads
   - OMIVV requires write access to the CIFS or NFS.
   - Files within the subfolders are ignored.
   - Files exceeding 10-MB sizes are ignored.
   - Driver repository is applicable only for vSAN clusters.
4. In the **Repository Share Location** area, perform the following tasks:
   a. Enter the repository share location (NFS or CIFS).
   b. For CIFS, enter the credentials.

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

5. To validate the catalog path and credentials, click **BEGIN TEST**.

   This validation is mandatory to continue further.

   Test connection results are displayed.
6. Click **NEXT**.
   The **Synchronize with repository location** page is displayed.
7. On the **Synchronize with repository location** page, select the **Synchronize with repository location** check box, and then click **NEXT**.
   To only update the profile name or review information, clear the **Synchronize with repository location** check box so that the catalog remains unchanged in OMIVV. For more information about synchronize with repository location, see Synchronize with repository location on page 47.
8. On the **Summary** page, review the profile information, and then click **FINISH**.

Related tasks

Create repository profile on page 44

Edit or customize Dell Default Catalog on page 46

Edit Validated MX Stack Catalog on page 47

Delete repository profile on page 47

Related information

Repository profile on page 44

Create repository profile on page 44

Delete repository profile on page 47

Edit or customize Dell Default Catalog

1. On the **Repository Profile** page, select **Dell Default Catalog**.
2. On the **Profile Name and Description** page, edit the profile description, and then click **NEXT**.
3. On the **Specify the Repository Location** section, select any one of the following:
   - **Dell Default Online**—The repository profile is set to **Dell Online** (`https://downloads.dell.com/catalog/Catalog.gz`). OMIVV uses Dell EMC Online as a source for catalog and update packages.
   - **Custom Online**—OMIVV uses **Custom Online** (HTTP or HTTPS share) as a source for catalog and update packages. When you create a custom repository using Server Update Utility (SUU), ensure that the signature file for the catalog (`catalog.xml.gz.sign`) is present in the catalog file folder.
   - **Shared Network Folder**—OMIVV uses shared network folder (CIFS or NFS) as a source for catalog and update packages.

   a. If you select **Custom Online**, enter the catalog online path.
   b. If you select **Shared Network Folder**, enter the catalog file location (NFS or CIFS).
4. To validate the catalog path and credentials, click **BEGIN TEST**.
   Test connection results are displayed.
5. On the **Synchronize with repository location** page, select the **Synchronize with repository location** check box, and then click **NEXT**.
   To only update the profile name or review information, clear the **Synchronize with repository location** check box so that the catalog remains unchanged in OMIVV. For more information about synchronize with repository location, see Synchronize with repository location on page 47.
6. On the **Summary** page, review the profile information, and then click **FINISH**.

Related information

Edit repository profile on page 45

Edit Validated MX Stack Catalog

1. On the **Repository Profile** page, select **Validated MX Stack Catalog**, and then click **EDIT**.
2. You can edit only the following:
   a. The catalog description.
   b. The **Synchronize with repository location** check box.

      To only update the profile name or review information, clear the **Synchronize with repository location** check box so that the catalog remains unchanged in OMIVV. For more information about synchronize with repository location, see Synchronize with repository location on page 47.

Related information

Edit repository profile on page 45

Synchronize with repository location

The Dell Default Catalog and Validated MX Stack repository profiles automatically check for changes after every 24 hours or at every reboot and updates automatically.

To update the offline catalogs, complete the following steps:

1. Update the catalog in the offline store (CIFS or NFS) using DRM or SUU. In case of drivers, replace the driver bundles.
2. Edit the repository profile and select the **Synchronize with repository location** check box to capture changes for the OMIVV to reference. This process takes a few minutes.
3. To update the firmware in a configuration compliance baseline, ensure to edit the respective cluster profiles and save.

View repository profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Repository Profile**.
   A table displays all the repository profiles along with the following information:
   - **Profile Name**—The name of the repository profile
   - **Description**—The profile description
   - **Type**—The type of the repository (firmware or driver)
   - **Share Path**—The NFS, or CIFS, or HTTP, or HTTPS path
   - **Last Successfully Updated Time**—The date and time when a repository profile is updated.
   - **Last Refresh Status**—The catalog download and parsing status
2. If you want to remove or add the column names from the wizard, click ▥.
3. To export the repository profile information, click ⇥.

Related information

Repository profile on page 44

Delete repository profile

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

1. On the **Repository Profile** page, select a repository profile, and then click **DELETE**.
2. In the delete confirmation dialog box, click **DELETE**.

Related tasks

Create repository profile on page 44

Edit repository profile on page 45

Related information

Repository profile on page 44
Create repository profile on page 44
Edit repository profile on page 45

Capture baseline configuration using cluster profile

Cluster profile

A cluster profile enables you to capture the configuration baseline (hardware configuration, firmware, or driver versions) and maintain the required state for clusters by identifying any drift against the configuration baseline.

To create a cluster profile, ensure that you have any one of these profiles: system profile, firmware repository profile, driver repository profile, or its combinations. Dell EMC recommends using homogeneous servers (same model, same hardware configuration, and same firmware level) for the clusters being baselined.

- After the cluster profile is created, firmware and driver repository profiles must be parsed before it can be used for a cluster profile creation.
- After the cluster profile is created, a current snapshot of the associated firmware and driver repository is created for the baseline. If the original repositories change, the cluster profile must be updated again to reflect the changes. Else, any updates that are performed on the original repositories are not updated to the cluster profile snapshots.
- After the cluster profile is created, it triggers the drift detection job.
- When a cluster is associated with a cluster profile, it overrides previous cluster profile associations, if any.
- If multiple standalone vCenters are registered to OMIVV, Dell EMC recommends creating separate cluster profiles for each vCenter.
- Baselining of drivers is supported only on vSAN clusters.

  NOTE: The drivers installed outside of OMIVV is not considered for baseline.

Related tasks

Create cluster profile on page 49

Edit cluster profile on page 50

View cluster profile on page 51

Delete cluster profile on page 51

Create cluster profile

- To create a cluster profile, ensure that you have any one of these profiles—System Profile, Firmware Repository Profile, Driver Repository Profile, or its combinations.
- Cluster must be present in the vCenter.
- Host credential profile must be created for at least one host in cluster and inventoried successfully.

1. On the OMIVV home page, **Compliance & Deployment** > **Profiles** > **Cluster Profile** > **CREATE NEW PROFILE**.
2. On the **Cluster Profile** page of the wizard, read the instructions, and click **GET STARTED**.
3. On the **Profile name and Description** page, enter the profile name and description, and then click **NEXT**.
   Profile name can be up to 200 characters and description can be up to 400 characters.
4. On the **Associate Profile (s)** page, select any one of the following profiles, or its combinations:
   - System Profile—Selecting a system profile sets the configuration baseline for the servers in the cluster. For Basic and Advanced system profile types, the system profile name is displayed in the following format: Basic_<*system profile name*>, Advanced_<*system profile name*>
   - Firmware Repository Profile—Selecting a firmware repository creates the firmware or BIOS baseline for the servers in the cluster. Online repositories are not supported for baselining vSAN clusters.
   - Driver Repository Profile—Selecting a driver repository creates the driver baseline for the servers in the cluster. At a time, you can associate a maximum of 10 drivers to a baseline. Baselining of drivers is supported only on vSAN clusters.

5. Click **NEXT**.
   The **Associate Cluster (s)** page is displayed.
6. On the **Associate Cluster (s)** page, perform the following tasks:
   a. Select an instance of a registered vCenter server.
   b. To associate the clusters, click **BROWSE**.
      To select the cluster, ensure that you have at least one host that is associated to the cluster, which is successfully managed by OMIVV.
   c. Click **OK**.
      The selected clusters are displayed on the **Associate Cluster(s)** page.
   d. Click **NEXT**.
7. On the **Schedule Drift Detection** page, select the date and time, and then click **NEXT**.
   The **Summary** page is displayed that provides the information about the cluster profile.
8. Click **FINISH**.
   The drift detection job runs immediately after the cluster profile is saved and later runs during the scheduled time. View the job completion status on the Jobs page.

   ⓘ **NOTE:** If the number of nodes that are managed by OMIVV is modified after creating the cluster profile for a cluster, the collection size gets updated automatically during the subsequent drift detection jobs.

Related tasks

Edit cluster profile on page 50
Delete cluster profile on page 51

Related information

Cluster profile on page 49
Edit cluster profile on page 50
Delete cluster profile on page 51
Initial configuration on page 84

Edit cluster profile

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

If the associated driver repository, or firmware repository, or system profile is changed and if you want to use the latest changes for the cluster profile, select a cluster profile, click **EDIT**, click **NEXT** in the wizard, and then click **Finish**.

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **Cluster Profile**.
2. Select a cluster profile and click **EDIT**.
3. On the **Profile Name and Description** page, edit the description, and then click **NEXT**.
4. On the **Associate Profile(s)** page, you can change the profile combinations.
5. On the **Associate Cluster(s)** page, you can change the vCenter instance and associated clusters.
6. On the **Schedule Drift Detection** page, you can change the drift detection schedule.
7. Review the updated information on the **Summary** page, and then click **FINISH**.
   The drift detection job runs immediately after the cluster profile is saved and later runs during the scheduled time.

Related tasks

Create cluster profile on page 49
Delete cluster profile on page 51

Related information

Cluster profile on page 49
Create cluster profile on page 49

View cluster profile

1. On the OMIVV page, click **Compliance & Deployment** > **Profiles** > **Cluster Profile**.
   A table displays all the cluster profiles along with the following information:

   - **Profile Name**—The name of the cluster profile
   - **Description**—The profile description
   - **Associated System Profile**—The associated system profile name For Basic and Advanced system profile types, the system profile name is displayed in the following format: Basic_<*system profile name*>, Advanced_<*system profile name*>
   - **Associated Firmware Repository Profile**—The associated firmware repository profile name
   - **Associated Driver Repository Profile**—The associated driver repository profile name

     > **NOTE:** For a PowerEdge MX host managed using a chassis credential profile, configuration drift is not calculated.

   - **vCenter**—The vCenter instance associated with the cluster profile
   - **Last Successfully Updated Time**—The date and time when the cluster profile is updated.

   If the associated driver repository, or firmware repository, or system profile is updated, a warning symbol is displayed with the profile name.

   > **NOTE:** If you perform backup and restore from 4.x to 5.x, a warning symbol is displayed with the profile name because OMIVV does not support 32-bit firmware bundle in 5.x.

   If you want to use the latest changes for the cluster profile, perform the following:

   a. Select the cluster profile and click **EDIT**.
   b. Continue to click **NEXT** without changing any properties.
   c. Click **FINISH**.

      The cluster profile is synced with the updated driver or firmware repository, and then the warning symbol disappears.

2. If you want to remove or add the column names from the wizard, click ◫.
3. To export the cluster profile information, click ⇨.

Related information

Cluster profile on page 49

Delete cluster profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **Cluster Profile**.
2. Select a cluster profile, and then click **DELETE**.
3. In the **Delete Confirmation** dialog box, click **DELETE**.
   If the cluster profile is deleted, the corresponding drift detection job is also deleted.

Related tasks

Create cluster profile on page 49
Delete cluster profile on page 51

Related information

Cluster profile on page 49
Create cluster profile on page 49
Edit cluster profile on page 50
Delete cluster profile on page 51

8

Deployment

To deploy system profile and ISO profile, ensure that the servers are displayed in the Deployment Wizard and all the servers are as per the following requirements:

- Meet specific hardware support information mentioned in the *OpenManage Integration for VMware vCenter Compatibility Matrix*.
- Meet minimum supported versions of the iDRAC firmware and BIOS. See the *OpenManage Integration for VMware vCenter Compatibility Matrix* for specific firmware support information.
- 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 an OS with OMIVV. OMIVV enables deployment on IDSDM, or local hard drives, or BOSS card.
- Ensure that there is a route between the vCenter, OMIVV, and the iDRAC networks, if vCenter, OMIVV, and iDRAC are connected to different networks. This is applicable only If the OMIVV appliance is not configured with two network adapters.
- Ensure that Collect System Inventory on Reboot (CSIOR) is enabled. Before initiating auto/manual discovery, ensure that retrieved data is current by performing a hard reboot on the server.
- For auto discovery of bare-metal servers either order the Dell EMC servers with auto discovery or 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 deploying an OS if OMIVV is not used for hardware configuration:
    - Enable the Virtualization Technology (VT) flag in BIOS.
    - The virtual driver, IDSDM, and BOSS are set to first boot disk.
- Verify that the BIOS setting for VT is automatically enabled even if the BIOS configuration is not part of the system profile, if OMIVV is used for hardware configuration. If a virtual drive is not configured on the target system, the Express or Clone RAID configuration is required.
- Ensure that the custom ESXi images that contain all the Dell EMC drivers are available for deployment. You can find the correct images from **dell.com/support** by going to the **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 download the custom Dell EMC ISO images, see Download custom Dell EMC ISO images on page 65.

View bare-metal servers

On the **Bare-metal Servers** page, you can:

- View the bare-metal servers discovered using auto discovery and manual discovery.

  The information such as **Service Tag**, **Model name**, **iDRAC IP**, **Server Status**, **System Lockdown Mode**, **Compliance Status**, and **iDRAC License Status** are displayed.

  The following are the different states of the bare-metal servers:

    - **Unconfigured**—The server is added to OMIVV and waiting to be configured.
    - **Configured**—The server is configured with all hardware information that is required for a successful OS deployment.
    - **Quarantined**—The servers cannot perform tasks such as OS deployment and firmware update because the servers are excluded from any OMIVV actions.

- View the compliance status of the bare-metal servers.

  A bare-metal server is non-compliant if:

    - 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 installed.
    - LOM or NIC is not present.
    - System Lockdown Mode is turned on.

- To view more information about the compliance issue, click **DETAILS** in the lower horizontal pane.

You can also perform the following tasks on the **Bare-metal Servers** page:

- Manual discovery of bare-metal servers
- Remove bare-metal servers
- System Profile and ISO Profile deployment
- Refresh bare-metal servers
- Purchase or renew iDRAC license

Device discovery

Discovery is the process of adding supported bare-metal server. After a server is discovered, you can use it for system profile and iso profile deployment. For more information about the list of supported servers, see *OpenManage Integration for VMware vCenter Compatibility Matrix*.

Prerequisites:

- The network connectivity from the bare-metal server's iDRAC to the OMIVV virtual machine is required.
- The hosts with existing OS should not be discovered into OMIVV, instead they should be added to the vCenter. Add them to a host credential profile.
- To deploy OS on SD card and to use system profile features in 12G and 13G bare-metal PowerEdge servers, ensure that iDRAC 2.50.50.50 and later is installed.

Auto discovery

Auto discovery is the process of adding bare-metal server. Once a server is discovered, use it for OS and hardware deployment. Auto discovery is an iDRAC feature that removes the need to manually discover a bare-metal server using OMIVV.

Related tasks

Remove bare-metal servers on page 55
Refresh bare-metal servers on page 56

Related information

Manual discovery of bare-metal servers on page 55

Auto discovery prerequisites

Before attempting to discover the PowerEdge bare-metal servers, ensure that OMIVV is 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 iDRAC of the Dell EMC bare-metal server to the OMIVV appliance.

NOTE: The hosts with existing OS should not be discovered using OMIVV, instead add the OS to a host credential profile.

For auto discovery to function, the following conditions must be met:

- Power—ensure that you connect the server to the power outlet. The server does not need to power on.
- Network connectivity—ensure that the iDRAC of the server has network connectivity and communicates with the provisioning server over port 4433. You can obtain the IP address of provisioning server by using a DHCP server or manually specify it in the iDRAC configuration utility.
- Extra network settings—To resolve DNS names, enable Get DNS server address in DHCP settings.
- Provisioning service location—ensure that iDRAC knows the IP address or hostname of the provisioning service server. See Provisioning service location.
- Account access disabled—if there are any iDRAC accounts with administrator privileges, first disable them from the iDRAC web console. Once auto discovery completes successfully, the administrative iDRAC account is re-enabled with deployment credentials that are entered on the **Settings** page. For more information about deployment credentials, see Configure deployment credentials on page 80.
- Auto discovery enabled—ensure that the iDRAC of the server has auto discovery that is enabled so that the auto discovery process can begin. For more information, see Enable or disable administrative accounts in iDRAC on page 54.

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 Configuration Utility, 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.

Enable or disable administrative accounts in iDRAC

Before setting up auto discovery, disable all IDRAC accounts except one which does not have admin access. After auto discovery, you can enable all accounts except the root account.

NOTE: Before disabling the admin privilege, Dell EMC recommends creating nonadmin user account in iDRAC.

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 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.
    - For iDRAC9: Go to **iDRAC Settings** > **Users** > **Local Users**.
4. In the **Local 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 1–8 after you have successfully set up auto discovery, but select the **Enable User** check box now, and click **Apply**.

Manually configure PowerEdge 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. 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 on the **Bare-metal Servers** page.

NOTE: For auto discovered servers, the credentials that are provided under **Settings** > **Appliance 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 host credential profile are set.

To enable auto discovery manually on the target machine, perform the following steps for 12th and later generation servers:

1. On the target system, 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 that is discovered upon next server boot. After successful auto discovery, the root user gets enabled, and the **Enable Auto-Discovery** flag is disabled automatically.

Manual discovery of bare-metal servers

You can manually add a bare-metal server that is not added using the auto discovery process. Once added, the server is displayed in the list of servers on the **Bare-metal Servers** page.

1. On the OMIVV home page, click **Compliance & Deployment** > **Deployment** > **DISCOVER**.
   The **Add Server** dialog box is displayed.
2. In the **Add Server** dialog box, do the following:
   a. In the **iDRAC IP Address** box, enter an iDRAC IPv4.
   b. Enter the iDRAC credentials.
3. Click **OK**.
   Adding server may take a few minutes.

   When the discovery operation is in progress, you can close the **Add Server** page. Discovery process proceeds in the background. The discovered server is displayed on the **Bare-metal Servers** page. The time out value for the manual discovery is set to 15 minutes.

   To view more information about the bare-metal server, select a server. The information such as license expiry, BIOS version, and system lockdown mode are displayed in the lower-most horizontal pane of the page.

Related concepts

Auto discovery on page 53

Related tasks

Remove bare-metal servers on page 55
Refresh bare-metal servers on page 56

Related information

Remove bare-metal servers on page 55
Refresh bare-metal servers on page 56

Remove bare-metal servers

You can manually remove a server that has been auto that is discovered or manually added.

1. On the OMIVV home page, click **Compliance & Deployment** > **Deployment** > **DELETE**.
2. Select a bare-metal server, and then click **OK**.

Related concepts

Auto discovery on page 53

Related tasks

Manual discovery of bare-metal servers on page 55
Refresh bare-metal servers on page 56

Related information

Manual discovery of bare-metal servers on page 55
Refresh bare-metal servers on page 56

Refresh bare-metal servers

The refresh operation rediscovers the bare-metal servers by connecting to iDRAC and collecting the basic inventory.

ⓘ **NOTE:** If you perform the refresh operation on the "Configured" bare-metal servers, the server status changes to the "Non-configured" state because the refresh operation rediscovers the server.

1. On the OMIVV home page, click **Compliance & Deployment** > **Deployment** > **REFRESH**.
2. On the **Refresh Bare-metal Servers** page, select a server, and click **OK**.
   Refreshing bare-metal servers data may take few minutes. While the operation is in progress, you can close the **Refresh Bare-metal Servers** page, rediscover process proceeds in background. The rediscovered server is displayed on the **Bare-metal Servers** page.

Related concepts

Auto discovery on page 53

Related tasks

Manual discovery of bare-metal servers on page 55
Remove bare-metal servers on page 55

Related information

Manual discovery of bare-metal servers on page 55
Remove bare-metal servers on page 55

Purchase or renew iDRAC license

The status of the bare-metal servers shows non-compliant when they do not have a compatible iDRAC license. A table displays the status of the iDRAC license. Select a noncomplaint bare-metal server to view more information about the iDRAC license.

1. To renew iDRAC license, on the OMIVV home page, click **Compliance & Deployment** > **Compliance** > **Deployment**.
2. Select a bare-metal server for which iDRAC license is noncompliant, and click **RENEW/PURCHASE IDRAC LICENSE**.
3. Log in to the Dell Digital Locker and update or purchase a new iDRAC license.
4. After you install an iDRAC license, click **REFRESH**.

Deployment

Before deploying system profile and ISO profile, ensure that the following are available:

- Host Credential Profile. To create a host credential profile, click **CREATE**. For more information about creating Host Credential Profile, see Create host credential profile on page 35.
- Bare-metal server. To discover a bare-metal server, click **DISCOVER**. For more information about discovering bare-metal servers, see Manual discovery of bare-metal servers on page 55.
- System Profile. To create a system profile, click **CREATE**. For more information about creating system profile, see Create system profile on page 61.
- ISO Profile. To create an ISO profile, click **CREATE**. For more information about creating ISO profile, see Create an ISO profile on page 64.

By using the **System Profile and ISO Profile Deployment** wizard, you can perform:

- System profile deployment

  For more information, see Deploy system profile (configuration of the hardware) on page 57.

- ISO profile deployment

  For more information, see Deploy ISO profile (ESXi installation) on page 57.

- System profile and ISO profile deployment

For more information, see Deploy system profile and ISO profile on page 59.

To launch the deployment wizard, go to **Compliance & Deployment** > **Deployment** > **DEPLOY**.

Deploy system profile (configuration of the hardware)

1. On the **System Profile and ISO Profile Deployment Checklist** page of the deployment wizard, verify the deployment checklist, and then click **GET STARTED**.

   You can perform the deployment only on the compliant bare-metal servers. For more information, see View bare-metal servers on page 52.
2. On the **Select Server (s)** page, select one or more servers.
   The **Select Deployment Options** page is displayed.
3. On the **Select Deployment Options** page, select **System Profile (Configuration of the hardware)**.
4. From the **System Profile** drop-down menu, select an appropriate system profile, and then click **NEXT**.

   For basic and advanced system profile types, the system profile name is displayed in the following format: Basic_<*system profile name*>, Advanced_<*system profile name*>.

   The **Configuration Preview** page is displayed. The **Configuration Preview** enables you to preview about the import operation of a server configuration profile (success or failure) on the selected server (s).
5. To create a preview job on iDRAC, on the **Configuration Preview** page, select an iDRAC IP, and then click **PREVIEW**. This is an optional task.
   The system profile preview operation may take few minutes to complete. The comparison status is displayed in the **Result** column.

   The following are the comparison results:

   - Completed—The preview job is successfully run. For more information about the comparison results, click **View Details** in the **Details** column.
   - Not completed—The preview job is not successfully run on the iDRAC. Ensure that iDRAC is accessible and perform iDRAC reset, if required. For more information about the job, see the OMIVV logs and the logs at iDRAC console.
6. On the **Schedule Deployment Job** page, do the following:
   a. Enter the deployment job name and description. The description is an optional field.
   b. To run the deployment job immediately, click **Run Now**.
   c. To schedule the job to run later, click **Schedule later**, and then select the date and time.
   d. Select the **Go to the Jobs page after the job is submitted** check box.
      You can track the status of the job on the **Jobs** page. For more information, see Deployment jobs on page 71.
7. Click **FINISH**.

Deploy ISO profile (ESXi installation)

You can perform the deployment only on the compliant bare-metal servers. For more information, see View bare-metal servers on page 52.

1. On the **System Profile and ISO Profile Deployment Checklist** page of the deployment wizard, verify the deployment checklist, and then click **GET STARTED**.
2. On the **Select Server (s)** page, select one or more servers.
   The **Select Deployment Options** page is displayed.
3. On the **Select Deployment Options** page, select **ISO Profile (ESXi installation)**.
4. From the **vCenter Name** drop-down menu, select an instance of vCenter.
5. To select the vCenter destination container, click **BROWSE**, and select an appropriate data center or cluster on which you want to deploy an OS.
6. From the **ISO Profile** drop-down menu, select an appropriate ISO profile.
7. Under **Installation Target**, select any one of the following:

   - **First boot disk**—deploys an OS on the Hard Disk Drive (HDD), Solid State Drive (SSD), or virtual drive created by RAID controllers.
   - **Internal Dual SD Module (IDSDM)**—deploys an OS on the IDSDM. 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 **First boot Disk** option is available.

  - ○ If any one of the selected servers does not support an IDSDM or BOSS module, or if IDSDM or BOSS is not installed in the servers during deployment then the deployment operation on those servers is skipped. To deploy the OS on the first boot disk of the servers, select the **Deploy the hypervisor to the first boot disk for servers that do not have an available Internal Dual SD Module** check box.

    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 OS 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.

- **BOSS**—deploys an OS on the BOSS card. If BOSS is available on at least one of the selected servers, the BOSS option is enabled. If not, only the **First boot Disk** option is available.

  If you are using OMIVV to deploy an OS on the BOSS controller, ensure that system 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 www.dell.com/support.

8. On the **Select Host Credential Profile** page, perform the following tasks:
   a. To use the same host credential profile for all hosts, click **YES**, and then select the host credential profile from the drop-down menu.
   b. To select the individual host credential profile for each server, click **NO**, and then select the host credential profile from the drop-down menu.

   NOTE: In host credential profile, Dell EMC recommends associating the user which is used to discover the bare-metal, else the discovered user gets disabled in iDRAC after OS deployment.
9. On the **Configure Network Settings** page, perform the following tasks:
   a. Enter a Fully Qualified Host Name (FQDN) for the server. 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. Create a DNS record that resolves the IP address with the FQDN. 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.

      NOTE: If vCenter is registered with OMIVV using FQDN, ensure that the ESXi host could resolve the FQDN using DNS resolution .

   b. Select the NIC for managing the server. Select the appropriate NIC which is connected to server.

      NOTE: Ensure that you select the management NICs based on the network connectivity to the OMIVV. The **APPLY SETTINGS TO ALL SERVERS** option is not applicable for management NIC selection.

   c. Select the OMIVV appliance NIC connected to host. For more information, see Prerequisites to deploy host with two network adapters on page 59.
   d. Select any one of the following networking options:
      - For static, enter the preferred DNS server, alternate DNS server, IP address, subnet mask, and default gateway.
      - **Use VLAN**—When a VLAN ID is provided, it is applied to the management interface of an OS during deployment and tags all traffic with the VLAN ID. Server Identification assigns new names and network identification to deployed servers. For more information, see VLAN support on page 59.
      - **Use DHCP**—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.

10. On the **Schedule Deployment Job** page, do the following:
    a. Enter the deployment job name and description.
    b. To run the deployment job immediately, click **Run Now**.
    c. To schedule the job to run later, click **Schedule later**, and then select the date and time.
    d. Select the **Go to the Jobs page after the job is submitted** check box.
    You can track the status of the job on the **Jobs** page. For more information, see Deployment jobs on page 71.
11. Click **FINISH**.

    NOTE: After performing OS deployment on bare-metal servers, OMIVV clears all the iDRAC jobs.

Deploy system profile and ISO profile

You can perform the deployment only on the compliant bare-metal servers. For more information, see View bare-metal servers on page 52.

1. On the **System Profile and ISO Profile Deployment Checklist** page of the deployment wizard, verify the deployment checklist, and then click **GET STARTED**.
2. On the **Select Server (s)** page, select one or more servers.
   The **Select Deployment Options** page is displayed.
3. On the **Select Deployment Options** page, select **System Profile (Configuration of the hardware)** and **ISO Profile (ESXi installation)**.
4. From the **vCenter Name** drop-down menu, select an instance of vCenter.
5. To select the vCenter destination container, click **BROWSE**, and select an appropriate data center or cluster on which you want to deploy an OS.
6. To use the system profile associated with the cluster profile which is associated with the selected cluster, click **confirm**.
   - To select any other system profile, click **Select another**. Dell EMC recommends selecting the system profile that is associated with the cluster to avoid a configuration compliance drift.
7. From the **ISO Profile** drop-down menu, select an appropriate ISO profile, and then click **NEXT**.
8. To create a preview job on iDRAC, on the **Configuration Preview** page, select an iDRAC IP, and then click **PREVIEW**. This is an optional task.
   The system profile preview operation may take few minutes to complete. The comparison status is displayed in the **Result** column.

   The following are the comparison results:

   - Completed—The preview job is successfully run. For more information about the comparison results, click **View Details** in the **Details** column.
   - Not completed—The preview job is not successfully run on the iDRAC. Ensure that iDRAC is accessible and perform iDRAC reset, if required. For more information about the job, see the OMIVV logs and the logs at iDRAC console.
9. Complete the tasks 7–10 listed in the Deploy ISO profile (ESXi installation) on page 57 topic.

Prerequisites to deploy host with two network adapters

The following are the deployment prerequisites for two network adapters:

- Host can have either iDRAC and vCenter management NIC in the same network or in the two distinct networks.
- The ISO image can be saved in any of the networks.
- The OS deployment wizard displays both the OMIVV networks. Ensure that you select the correct vCenter network and OMIVV network applicable to the environment.

VLAN support

OMIVV supports OS 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 VLANs using VLAN ID. When a VLAN ID is provided, it is applied to the management interface of an OS during deployment and tags all traffic with the VLAN ID.

Ensure that the VLAN provided during deployment communicates with both the OMIVV appliance and the vCenter server. The deployment of an OS 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: Ensure that you select the management NICs based on the network connectivity to the OMIVV. The **APPLY SETTINGS TO ALL SERVERS** option is not applicable for management NIC selection.

Deployment job timing

The system profile and ISO profile deployment can take between 30 minutes to several hours to complete, depending on multiple 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 the system profile and ISO profile deployment varies with deployment type, complexity, and number of deployment jobs running simultaneously. 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.

The following table displays the average value, and may vary based on factors like configuration of the server, generation of the server, and number of bare metal servers scheduled for deployment:

Table 3. Approximate deployment time for a single server

Deployment type	Approximate time per deployment
ISO profile only	Between 30–130
System profile only	5–6 minutes
System profile and ISO profile	30–60 minutes

Server status within deployment sequence

The servers that are discovered during auto discovery or manually 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 statuses to check the hardware configuration status.

Table 4. Server states in the deployment sequence

Server state	Description
Unconfigured	The server is added to OMIVV and is waiting to be configured.
Configured	The server is configured with all hardware information that is required for a successful OS deployment.

System profile

The system profile captures the component-level settings and configuration of iDRAC, BIOS, RAID, Event Filters, FC, and NICs. These configurations can be applied to other identical servers during an operating system deployment on bare-metal servers. The system profile can be used in cluster profile to maintain baseline for configuration.

Prerequisites

Before creating or editing the system profile, ensure that:

- The CSIOR feature is enabled on the reference server and reference server have been restarted after enabling CSIOR so that the data returned from iDRAC is up-to-date.
- The OMIVV has performed a successful inventory operation for each reference host that is managed by the vCenter.
- Bare-metal servers have the minimum required BIOS and firmware versions installed. For more information, see the *OMIVV Compatibility Matrix* available on the support site.
- The reference server and target servers are homogeneous (same model, same hardware configuration, and same firmware level).
- The hardware (for example, FC, NIC, and RAID controller) is present in the identical slots of the reference server and target servers.
- Before you include or exclude any attribute from the default selection, hover over attribute name to understand the details of the attribute.
- The iDRAC user that is used to discover the iDRAC is selected when you configure the iDRAC users in system profile.

  NOTE: Do not clear the attributes that are linked with the iDRAC user which is used to discover the bare-metal, else system profile deployment job fails.
- You do not change the username of iDRAC user that is used to discover the iDRAC, This results in connectivity issue with iDRAC, the system profile deployment job fails without applying any attributes.

Before creating the system profile, Dell EMC recommends configuring the reference server attribute and value as required, and then apply it to all the required target servers.

The system profiles search for an 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 that are 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, Dell EMC recommends having a reference system profile from each slot of the chassis and applies these system profiles across the chassis for the corresponding slots only.

ⓘ **NOTE:** A 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.
- You cannot import system profile by using the Express license of iDRAC9 firmware 3.00.00.00. You must have an Enterprise license.

Related tasks

Create system profile on page 61
Edit system profile on page 62
View system profile on page 63
Delete system profile on page 63

Create system profile

Dell EMC recommends using Google Chrome to create or edit System Profile.

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **System Profile** > **CREATE NEW PROFILE**.
2. On the **Create System Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
3. On the **Name and Description** page, do the following:
   a. Enter profile name and description. The description field is an optional field.
   b. Select any one of the following system profile types:
      - Basic—Displays the minimal set of attributes for iDRAC, BIOS, RAID, NIC, and FC.
      - Advanced—Displays all the attributes for iDRAC, BIOS, RAID, NIC, FC, and EventFilters.
4. On the **Reference Server** page, to select a reference server that is either a host or a bare-metal, click **SELECT**.

   The server selection may be disabled because of any one of the following reasons:

   - The server is either a noncompliant host or noncompliant bare-metal server.
   - A deployment job is either scheduled or running on the server.
   - The server is managed using the chassis credential profile.

   The **Extract Confirmation** dialog box is displayed.
5. To extract the system configuration from the reference server, click **OK**.
   Extracting the system configuration from the reference server might take few minutes.
6. Review the reference server details and click **NEXT**.
   - To change the reference server on the **Select Reference Server** page, click **BROWSE**.

     If the reference server is of bare-metal type, only its iDRAC IP is displayed. If the reference server itself is a host server, both the iDRAC and host (FQDN) IPs are displayed.

   The **Profile Settings** page is displayed.
7. On the **Profile Settings** page, you can view or modify the profile settings for the components such as iDRAC, BIOS, RAID, NIC, CNA, FCoE, and EvenFilters based on the configuration of the reference server. By default, platform-specific and read-only attributes are not listed. For more information about platform-specific attributes, see System specific attributes on page 153.

ⓘ **NOTE:** Pseudo attributes are not displayed in system profile. For more information, see the Server Configuration XML File document.

Before selecting the attributes other than the attributes that are selected by default, check the nature of attribute, dependency, and other details.

If you select the attributes other than the attributes that are selected by default, the following message is displayed:

These attributes may affect other dependent attributes, or are destructive in nature, or dissolve server identity, or affect security of the target servers.

ⓘ **NOTE:** For 12th and 13th generation of PowerEdge servers, some of the attributes may not map dependency properly in OMIVV. For example, Memory Operating Voltage component of BIOS is Read-only unless the system profile is set to **Custom** in **System BIOS Settings**.

a. Expand each component to view the setting options such as **Instance**, **Attribute Name**, **Value**, **Destructive**, **Dependency**, and **Group**.

   If the dependency text is not available, a blank field is displayed.

   ⓘ **NOTE:** You can use the **Search** field to filter data specific to all the columns except **Value**.

b. It is mandatory to set the values for attributes marked with red exclamation mark. This option is available only for the iDRAC enabled user with valid user name.

8. Click **NEXT**.
   The **Summary** page displays information about the profile details and the attribute statistics of the system configurations.

   The total number of attributes, total number of enabled attributes, and total number of destructive attributes are displayed under the attribute statistics.
9. Click **FINISH**.
   The saved profile is displayed on the **System Profile** page.

   Some attributes of System Profile are overridden for the OMIVV to be functional. For more information about customized attributes, see Customization attributes on page 158. For more information about the System Profile configuration template, attributes, and workflow, see Additional information on page 157.

Related information

System profile on page 60

Initial configuration on page 84

Edit system profile

Dell EMC recommends using Google Chrome to create or edit System Profile.

1. On the **Create System Profile** page, select a System Profile, and then click **EDIT**.
2. On the **Name and Description** page, change the profile name and description. The description is optional.

   ⓘ **NOTE:** After creating the Basic or Advanced system profile, you cannot modify the profiles.

3. On the **Reference Server** page, to change the reference server that is either a host or a bare-metal, click **SELECT**.

   The server selection may be disabled because of any one of the following reasons:

   - The server is either a noncompliant host or bare-metal server.
   - A deployment job is either scheduled or running on the server.
   - The server is managed using the chassis credential profile.

   The **Extract Confirmation** dialog box is displayed.
4. To extract the system configuration from the reference server, click **OK**.
   Extracting the system configuration from the reference server might take few minutes.
5. Review the reference server details and click **NEXT**.

   - To change the reference server on the **Select Reference Server** page, click **BROWSE**. If the reference server is of bare-metal type, only its iDRAC IP is displayed. If the reference server itself is a host server, both the iDRAC and host (FQDN) IPs are displayed.

The **Profile Settings** page is displayed.

6. On the **Profile Settings** page, you can view or modify the profile settings for the components such as iDRAC, BIOS, RAID, NIC, CNA, FCoE, and EvenFilters based on the configuration of the reference server. By default, platform-specific and read-only attributes are not listed. For more information about platform-specific attributes, see System specific attributes on page 153.

   If you try to modify few attributes, the following warning message is displayed:

   These attributes may affect other dependent attributes, or are destructive in nature, or dissolve server identity, or affect security of the target servers.

   > **NOTE:** After editing the system profile, if the password of iDRAC users that is used to discover the bare-metal server is modified, the updated password is ignored and replaced with password that is used to discover the bare-metal servers.

   a. Expand each component to view the setting options such as Instance, attribute name, value, destructive, dependency, and group.

      If the dependency text is not available, a blank field is displayed.

   b. It is mandatory to set the values for attributes marked with red exclamation mark. This option is available only for the iDRAC enabled user with valid user name.

7. Click **NEXT**.
   The **Summary** page displays information about the profile details and the attribute statistics of the system configurations.

   The total number of attributes, total number of enabled attributes, and total number of destructive attributes are displayed under the attribute statistics.

8. Click **FINISH**.
   The saved profile is displayed on the **System Profile** page.

   Some attributes of System Profile are overridden for the OMIVV to be functional. For more information about customized attributes, see Customization attributes on page 158. For more information about the System Profile configuration template, attributes, and workflows, see Additional information on page 157.

Related information

System profile on page 60

View system profile

1. On the OMIVV home page, click **Compliance & Deployment** > **System Profile**.
   A table displays all the system profiles along with the following information:
   - **Profile Name**—The name of the system profile
   - **Description**—The profile description
   - **Reference Server**—The iDRAC IP from which the system configuration details are extracted.
   - **Server Model**—The model name of the reference server
2. If you want to remove or add the column names from the wizard, click ▥.
3. To export the system profile information, click ⇨.

Related information

System profile on page 60

Delete system profile

Deleting a system profile that is part of a running deployment task might cause the deletion job to fail.

1. On the **System Profile** page, select a system profile, and then click **DELETE**.
2. In the delete confirmation dialog box, click **DELETE**.

Related information

System profile on page 60

ISO profile

An ISO profile contains the folder path for the Dell EMC customized ESXi ISO image file that is saved on the NFS or CIFS folders. An ISO profile is used in the deployment wizard.

Related tasks

Create an ISO profile on page 64
Edit an ISO profile on page 64
View an ISO profile on page 65

Create an ISO profile

An ISO profile requires Dell EMC customized ISO file location on an NFS or CIFS.

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **ISO Profile** > **CREATE NEW PROFILE**.
2. On the **ISO Profile** page of the wizard, read the instructions, and then click **GET STARTED**.
3. On the **Profile Name and Description** page, enter the profile name and description. The description is an optional field.
4. In the **Installation Source (ISO)** box, enter the ISO file location (NFS or CIFS).

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

   a. If using CIFS, enter the credentials.
5. From the **ESXi Version** drop-down list, select an ESXi version.

   Select the correct ESXi version so that the appropriate installation boot script is used. If you select an incorrect ESXi version deployment may fail.
6. To verify the ISO file path accessibility and credentials, click **BEGIN TEST**.
   Test results are displayed.
7. Click **FINISH**.

Related information

ISO profile on page 64

Edit an ISO profile

1. On the OMIVV home page, click **Compliance & Deployment** > **Profiles** > **ISO Profile**.
2. Select an ISO profile, click **EDIT**.
3. On the **Profile Name and Description** page, edit the profile name and description. The description is an optional field.
4. In the **Installation Source (ISO)** box, change the ISO file location (NFS or CIFS).

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

   a. If using CIFS, enter the credentials.
5. From the **ESXi Version** drop-down list, select an ESXi version.

   Select the correct ESXi version so that the appropriate installation boot script is used. If you select an incorrect ESXi version, the deployment may fail.
6. To verify the ISO file path and authentication, click **BEGIN TEST**.
   Test results are displayed.
7. Click **FINISH**.

Related information

ISO profile on page 64

View an ISO profile

1. On the OMIVV home page, click **Compliance & Deployment** > **ISO Profile**.
   A table displays all the ISO profiles along with the following information:
   - **Profile Name**—The name of the profile
   - **Description**—The profile description
   - **Installation Source**—The ISO file location (NFS or CIFS)
   - **ESXi Base Version**—The ESXi base version
2. If you want to remove or add the column names from the wizard, click ▥.
3. To export an ISO profile information, click ⇥.

Related information

ISO profile on page 64

Delete an ISO profile

Deleting an ISO profile that is part of a running deployment task can cause the task to fail.

1. On the OMIVV home page, **Compliance & Deployment** > **Profiles** > **ISO Profile**.
2. Select an ISO profile, click **DELETE**.
3. In the confirmation dialog box, click **DELETE**.

Download custom Dell EMC ISO images

The custom ESXi images that contain all Dell EMC drivers are required for deployment.

1. Open a browser and go 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**.

9

Compliance

Management Compliance

To view and manage hosts in OMIVV, each host must meet certain criteria. If the hosts do not meet the compliance criteria, OMIVV will not manage and monitor them. OMIVV displays details about the noncompliance host, and enables you to fix the noncompliance, where applicable.

The host is non-compliant if:

- The host is not associated to a Host Credential Profile.
- The Collect System Inventory on Reboot (CSIOR) feature 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 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 that are provided in host credential a profile is invalid. Or, there are no free slots in iDRAC, or iDRAC Lockdown Mode is turned on—only in 14G and later hosts.
- OMIVV fails to enable the WBEM service on hosts running ESXi 6.5 and later.
- The iDRAC firmware version is lower than 2.50.50.50. The iDRAC version 2.50.50.50 or higher is required only to use the system profile feature.
- iDRAC license is not compatible (iDRAC Express is the minimum requirement). The servers without a compatible iDRAC license cannot be used for monitoring and updating the firmware.

△ **CAUTION: Even if non-compliant, the hosts in the Lockdown mode are not displayed in the compliance tests. Ensure to manually check the compliance level. A message is displayed when manually checked. Ignore the message. 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.**

On the **Management Compliance** page, you can perform the following tasks:

- Fix compliance. For more information, see Fix a non-compliant host on page 67.
- Run inventory. The run inventory job link is active if the iDRAC status is **non-compliant** or **Unknown** for any one of the hosts that are associated to a host credential profile.
- Renew iDRAC License. For information, see Fix iDRAC license compliance on page 68.
- Add OEM hosts. For more information about adding OEM hosts, see Add OEM hosts on page 68.

Related tasks

View non-compliant hosts on page 66

Fix a non-compliant host on page 67

View non-compliant hosts

1. On the OMIVV home page, click **Compliance & Deployment** > **Management Compliance**.

A table displays all the non-compliant hosts along with the following information:

- **Host**—The FQDN or IP address of the host
- **Model**—The model name of the server
- **Credential Profile**—The host credential profile name
- **CSIOR Status**—The CSIOR status (**ON** or **OFF**). The CSIOR status shows **Undetermined** for hosts that are managed using chassis,
- **SNMP Trap Status**—The SNMP Trap Status (**Configured** or **Not Configured**).
- **Hypervisor**—The hypervisor name and version

- **WBEM Status**—The WBEM status (**Compliant** or **Non-compliant**). The CSIOR status shows **Not applicable** for hosts that are managed using chassis.
- **iDRAC Firmware Version**—The iDRAC firmware version
- **iDRAC License Status**—The iDRAC License status (**Compliant** or **Non-compliant**).

  ⓘ **NOTE:** When a PowerEdge MX host is managed using a chassis credential profile, the iDRAC Firmware version is displayed as **Not Applicable** on the **Management Compliance** page. This is because iDRAC firmware compliance is not applicable for 14G and later servers.

Related information

Management Compliance on page 66

Fix a non-compliant host

The host is non-compliant if:

- The host is not associated to a Host Credential Profile.
- The Collect System Inventory on Reboot (CSIOR) feature 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 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 that are provided in host credential a profile is invalid. Or, there are no free slots in iDRAC, or iDRAC Lockdown Mode is turned on—only in 14G and later hosts.
- OMIVV fails to enable the WBEM service on hosts running ESXi 6.5 and later.
- The iDRAC firmware version is lower than 2.50.50.50. The iDRAC version 2.50.50.50 or higher is required only to use the system profile feature.
- iDRAC license is not compatible (iDRAC Express is the minimum requirement). The servers without a compatible iDRAC license cannot be used for monitoring and updating the firmware.

1. On the OMIVV home page, click **Compliance & Deployment** > **Management Compliance**.
2. Select a non-compliant host, click **Fix Compliance**.
3. On the welcome page of the wizard, read the instructions, and then click **GET STARTED**.
4. On the **Select Hosts** page, select one or more non-compliant hosts and click **NEXT**.

   - If the hosts are not associated to a host credential profile, the following warning message is displayed:

     There are selected hosts that are not assigned to a Host Credential Profile. To allow OMIVV to run a compliance check, you must add these hosts to a Host Credential Profile

     To exclude the hosts that are not assigned to host credential profile, click **CONTINUE**.

     To add the hosts to a Host Credential Profile page, Click **Cancel** and go to the host credential profile page. For more information about creating host credential profile, see Create host credential profile on page 35.

     The hosts present in an MX chassis with an iDRAC IPv4 disabled have to be managed using chassis credential profile. To associate these hosts to chassis credential profile, you have to add the chassis using Add MX Chassis on the **Dell EMC Chassis** page and associate the chassis to a chassis credential profile.

   To update iDRAC firmware and BIOS version:

   a. On the **Update iDRAC firmware and BIOS version** page, select one or more hosts on which you want to update the firmware version.
   b. Click **NEXT**.
   c. On the **Reboot Hosts** page, view the ESXi hosts that must be restarted.
   d. If you want to automatically put hosts in maintenance mode and reboot when required, select the check box, and then click **NEXT**.
   e. On the **Summary** page, review the summary of actions, and then click **FINISH**.

   To turn on CSIOR:

   a. On the **Select Hosts** page, select one or more non-compliant hosts and click **NEXT**.
   b. On the **Turn on CSIOR** page, select one or more hosts for which you want to turn on CSIOR, and click **NEXT**.
   c. On the **Summary** page, review the summary of actions, and then 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 host credential 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 and later 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 enabling OMIVV to enable the WBEM service for those hosts during inventory.

Related information

Management Compliance on page 66

Fix iDRAC license compliance

The compatible iDRAC license is one of the compliance criteria for hosts. If hosts do not have compatible iDRAC license, those hosts listed as noncompliant hosts on the **Management Compliance** page. You can click a noncomplaint host to view the details such as iDRAC expiation date, license type, and license description. The **RUN INVENTORY** is active if the iDRAC compliance status is **non-compliant** or **Unknown** for any one of the hosts that are associated to a host credential profile.

1. To fix the iDRAC license compliance, on the OMIVV home page, click **Compliance & Deployment** > **Compliance** > **Management Compliance**.
2. Select a host for which iDRAC license is noncompliant, and click **RENEW IDRAC LICENSE**.
3. Log in to the Dell Digital Locker and update or purchase a new iDRAC license.
   After you install an iDRAC license, run an inventory job for the host and return to this page after the inventory job is successfully complete.

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 servers are supported.
- Onboard OEM servers by using the **Add OEM Hosts** wizard. For more information about adding OEM hosts, see Add OEM hosts on page 68.

  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 host credential profile to manage these servers. For more information about creating a host credential profile, see Create host credential profile on page 35.
- After onboarding, all the host management processes will be similar to how Dell EMC PowerEdge servers are managed.
- Bare-metal and deployment features are also supported on OEM servers by using iDRAC.

Add 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.

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.

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 OMIVV home page, click **Compliance & Deployment** > **Compliance** > **Management Compliance** > **Add OEM Hosts**.
2. In the **Add OEM Hosts** window, from the **vCenter Instance** drop-down list, select an instance of vCenter.
3. From the **Host Credential Profile** drop-down list, select an appropriate host credential profile.
4. To add or remove the associated host, click **ADD HOST**.
   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 test connection results are displayed in the **Add OEM Hosts** window.

The **iDRAC Test** and **Host Test** columns displays the test connection result for **iDRAC Credentials** and **Host Credentials**.

To stop all the test connections, click **ABORT TEST**.

6. Click **OK**.
   The selected hosts are added to the selected host credential profile and inventory is triggered.

Configuration Compliance

The Configuration Compliance page displays the compliance status that is based on the drift detection for all the clusters that are associated with the cluster profile. In PSC environment with multiple vCenter servers, configuration compliance page list all the clusters from all the vCenters that belong to the same PSC registered with same appliance.

- Hardware Configuration Compliance—Displays the drift in attributes between the system profile that is used in the cluster profile and the associated hosts that are part of cluster.
- Firmware Compliance—Displays the firmware version drift between the firmware repository profile that is used in the cluster profile and the associated hosts that are part of cluster.
- Driver Compliance—Displays the driver version drift between the driver repository profile that is used in the cluster profile and the associated vSAN hosts that are part of cluster profile.

View configuration compliance

1. On the OMIVV home page, click **Compliance & Deployment** > **Compliance** > **Configuration Compliance**.
   A table displays clusters with associated cluster profile, system profile, firmware repository profile, and driver repository profile.

   For Basic and Advanced system profile types, the system profile name is displayed in the following format: Basic_<*system profile name*>, Advanced_<*system profile name*>.
2. On the **Configuration Compliance** page, select a cluster.
   The configuration compliance information and compliance status are displayed.

   The following information is displayed in the **Configuration Compliance** section:

   - **Cluster Name**—The name of the cluster
   - **Compliance Status**—Displays the compliance status (compliant or non-compliant). If any one of the hosts in the cluster is non-compliant, the status is displayed as non-compliant.
   - **Number of hosts**—The total number of hosts present in the cluster
   - **Schedule**—The day and time when the next drift detection job is scheduled.
   - **Last Drift Detection Time**—The date and time when the last drift detection job is completed.

   The **Compliance Status** section displays the compliance state of the hardware, firmware, and driver components. The different compliance states are:

   - **Compliant**—Displays the count of hosts that are compliant with associated hardware, firmware, and driver components.
   - **Non-compliant**—Displays the count of hosts that are non-compliant with associated hardware, firmware, and driver components.
   - **Not applicable**—Displays the count of not applicable hosts.

     Hardware drift is not applicable for the hosts that are managed using chassis credential profile.

     The driver drift is not applicable for the hosts that are part of vSphere cluster.

     If the cluster profile is created using the online catalog, the firmware compliance is not applicable for vSAN clusters.
3. To view the drift details, click **VIEW DRIFT REPORT**. This link is enabled only for non-compliant clusters. For more information about viewing drift report, see View drift report on page 70.

View drift report

The **Configuration Compliance Report** page displays the drift details of the hardware, firmware, and driver components.

The drift detection job status is displayed in the **Summary** section.

For Hardware:

- Host Name or IP—Indicates the host IP or hostname.
- Service Tag—Indicates the Service Tag of the host.
- Drift Status—Indicates the drift status (non-compliant or failed).
- Instance—Indicates the hardware component name.
- Group—Indicates the group name of the attributes.
- Attribute Name—Indicates the attribute name.
- Current Value—Indicates the current value of the attribute in the host.
- Baseline Value—Indicates the baseline value.
- Drift Type/Error—Indicates the reason for non-compliance. For more information about the drift type, see Component vs. baseline version comparison matrix on page 159.

> ⓘ **NOTE:** Drift detection job fails only when the host or iDRAC is not reachable. If the host or iDRAC is inventoried successfully, then the drift detection job shows successful. To check any other drift detection job failure reasons, see the **Drift Type/Error** column in drift report.

For firmware and driver:

- Host Name or IP—Indicates the host IP or hostname.
- Service Tag—Indicates the Service Tag of the host.
- Drift Status—Indicates the drift status.
- Component Name—Indicates the name of the component.
- Current Value—Indicates the current value of the attribute in the host.
- Baseline Value—Indicates the baseline value.
- Drift Type/Error—Indicates the reason for non-compliance. For more information about the drift type, see Component vs. baseline version comparison matrix on page 159.
- Criticality (for firmware)—Indicates the importance level of updating the version of an identified component.
- Recommendation (for driver)—Indicates the update recommendation of a driver component.

> ⓘ **NOTE:** If more than one version of firmware is available, the latest firmware version is always used for compliance comparison.

You can use the filter option to see the drift details based on the drift status.

> ⓘ **NOTE:** The 32-bit firmware bundle is not supported in 5.x. If the cluster profile is associated with 32-bit firmware bundle in 4.x version, the drift status is displayed as failed when you perform the backup and restore from 4.x to 5.x. Use the 64-bit firmware bundle with cluster profile and rerun the drift detection job.

10

Manage jobs

Deployment jobs

After the deployment tasks are complete, you can track the deployment job status on the **Deployment Jobs** page.

1. On the OMIVV home page, click **Jobs** > **Deployment Jobs**.
   A table displays all the deployment jobs along with the following information:
   - **Name**—The deployment job name
   - **Description**—The job description
   - **Scheduled Time**—The date and time when the job is scheduled.
   - **Status**—The status of the deployment job
   - **Collection Size**—The number of servers in the deployment job
   - **Progress Summary**—The job progress details of the deployment job
2. To view the more information about the servers in the deployment job, select a deployment job.

   The following information is displayed in the lower pane:
   - **Service Tag**
   - **iDRAC IP**
   - **Status**
   - **Warnings**
   - **Details**
   - **Start Date and Time**
   - **End Date and Time**
   - **More Details**

   a. To view more information about a deployment job, select a job and pause the pointer on the **Details** column.
   b. To view more information about the system profile-based jobs failure, click **More Details**.

      The following information is displayed:
      - 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**.
3. To stop the deployment job, click 🛑.
4. To purge the deployment jobs, click 🧹, select **Older than date and job Status**, and then click **Apply**.
   The selected jobs are then cleared from the **Deployment** jobs page.

Chassis firmware update jobs

After the chassis firmware update tasks are complete, you can view the status of the firmware update jobs on the **Chassis Firmware Update Jobs** page.

1. On the OMIVV home page, click **Jobs** > **Chassis Firmware Update**.
2. To view the latest log information, click the refresh icon.
   A table displays all the chassis firmware update jobs along with the following information:

- **Status**—The status of the firmware update job
- **Scheduled time**—The firmware update job scheduled time
- **Name**—The name of the job
- **Description**—The firmware update job description
- **vCenter**—The vCenter name
- **Collection Size**—The number of chassis in the firmware update job. The total number of chassis includes only lead and standalone chassis. The member chassis will not take part in it.
- **Progress**—The progress details of the firmware update job

3. To view more information about a particular job, select a job.
   The following information is displayed in the lower grid:

   - **Chassis Service Tag**—The Service Tag of the chassis
   - **Status**—The status of the job
   - **Start Time**—The firmware update job start time
   - **End Time**—The firmware update job end time

   For a PowerEdge MX chassis in an MCM configuration, the member gets updated first, and then the lead chassis. However, the start time for both member and lead is indicated as the same.

4. If you want to stop a scheduled firmware update that is not running, select the job that you want to stop, and click 🛑.

   WARNING: If you stop a firmware update job that is already submitted to MX chassis, the firmware might still get updated on the host, but OMIVV reports the job as canceled.

5. 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.
6. In the **Purge Firmware Update Jobs** dialog box, select **Older than date and job Status**, click **OK**.
   The selected jobs are then cleared from the **Chassis Firmware Update** jobs list.

Host firmware update jobs

After the chassis firmware update tasks are complete, you can view the status of the firmware update jobs on the **Host Firmware Update Jobs** page.

1. On the OMIVV home page, click **Jobs** > **Host Firmware Update**.
2. To view the latest log information, click the refresh icon.
   A table displays all the host firmware update jobs along with the following information:

   - **Status**—The status of the firmware update job
   - **Scheduled time**—The firmware update job scheduled time
   - **Name**—The name of the job
   - **Description**—The firmware update job description
   - **vCenter**—The vCenter name
   - **Collection Size**—The number of servers in the firmware update job
   - **Progress Summary**—The progress details of the firmware update job
3. To view more information about a particular job, select a job.
   The following information is displayed in the lower grid:

   - **Host Service Tag**—The Service Tag of the host
   - **Status**—The status of the job
   - **Start Time**—The firmware update job start time
   - **End Time**—The firmware update job end time

   NOTE: If firmware update job is scheduled with multiple Dell Update Packages and OMIVV fails to download some of the selected update packages, OMIVV will continue to update the successfully downloaded packages. Jobs page displays the status of the successfully downloaded packages.

4. If you want to stop a scheduled firmware update that is not running, select the job that you want to stop, and click 🛑.

   WARNING: If you stop 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.

5. 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.
6. In the **Purge Firmware Update Jobs** dialog box, select **Older than date and job Status**, click **OK**.
   The selected jobs are then cleared from the **Host Firmware Update** jobs list.

System Lockdown Mode jobs

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 credential profile.

After the System Lockdown configuration is complete, you can view the updated status of Lockdown Mode in the **System Lockdown Mode Jobs** page.

1. On the OMIVV home page, click **Jobs** > **System Lockdown Mode**.
   A table displays all the System Lockdown Mode jobs along with the following information:
   - **Name**—The System Lockdown Mode job name
   - **Description**—The job description
   - **Schedule Time**—The date and time when the System Lockdown Mode job is scheduled.
   - **vCenter**—The vCenter name
   - **Status**—The status of the System Lockdown Mode job
   - **Collection Size**—The number of servers in the System Lockdown Mode job
   - **Progress Summary**—The job progress details of the System Lockdown Mode job
2. To view the more information about the servers in the System Lockdown Mode job, select a System Lockdown Mode job.
   The following information is displayed in the lower grid:
   - **Service Tag**
   - **iDRAC IP**
   - **Host Name**
   - **Status**
   - **Details**
   - **Start Date and Time**
   - **End Date and Time**

   To view more information about a System Lockdown mode job, select a job and pause the pointer on the **Details** column.
3. To purge the System Lockdown Mode Jobs, click🧹, select **Older than date and job status**, and then click **APPLY**.
   The selected jobs are then cleared from the **System Lockdown Mode** jobs page.

Drift detection job

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.

NOTE: Drift detection job fails only when the host or iDRAC is not reachable. If the host or iDRAC is inventoried successfully, then the drift detection job runs successfully and you can view the drift details in the drift report. For more information about drift report, see View drift report on page 70.

1. On the OMIVV home page, click **Jobs** > **Drift Detection**.
   A table displays all the drift detection job along with the following information:
   - **Name**—The name of the drift detection job
   - **Last Run**—The date and time when the last drift detection job was run.
   - **Next Run**—The date and time when the next drift detection job is scheduled.
   - **Status**—The status of the drift detection job
   - **Collection Size**—The number of servers in the drift detection job

   - **Progress Summary**—The progress details of the drift detection job
2. To view the updated Drift Detection Job Details, click **Refresh**.
3. To view the more information about the servers in the drift detection job, select a drift detection job. The following information is displayed:
   - 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 ▶.

   In a baselined cluster, after adding a host device to the host credential profile or chassis credential profile, the drift detection job is automatically run on a newly added host.

View host inventory job

The **Host Inventory** page displays information about the latest inventory job run on a host that is associated to a Host Credential Profile.

1. On the OMIVV home page, click **Jobs** > **Inventory History** > **Host Inventory**.
2. Select a vCenter to view all the associated hosts inventory job information.
   - **vCenter**—The vCenter FQDN or IP address
   - **Hosts Passed**—The count of hosts for which inventory is successful.
   - **Last Inventory**—The date and time when the last inventory was run.
   - **Next Inventory**—The date and time when the next inventory is scheduled.

   The associated hosts details are displayed in the lower pane.

   - **Host**—The FQDN or IP address of hosts
   - **Status**—The inventory status of the hosts The options include:
     - **Successful**
     - **Failed**
     - **In Progress**
   - **Duration (MM:SS)**—The duration of the inventory job in minutes and seconds
   - **Start Date and Time**—The date and time when the inventory job started.
   - **End Date and Time**—The date and time when the inventory job completed

Related tasks

Run inventory job on page 74

Run inventory job

After the initial configuration is complete, inventory is triggered automatically for all hosts which are added to a host credential Profile.

1. To run inventory on-demand, click **Jobs** > **Inventory** > **Hosts Inventory**.
2. Click Run now [▶].
3. To see the status of the inventory job, click **Refresh**.

   After inventory job is complete, you can view the OMIVV host information about the **Summary** page.
4. To view the OMIVV host information, expand **Menu**, and then select **Hosts and Clusters**
5. In the left pane, select any host.
6. In the right pane, select **Monitor**, and then expand **OMIVV Host Information**.

The following information is displayed:

- Overview
- Hardware Inventory
- Storage
- Firmware
- Power Monitoring
- Warranty
- System Event Log

When the hosts are managed using the chassis credential profile, the firmware inventory data show few extra components such as Lifecycle Controller and Software RAID.

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

7. On the **Summary** page, in the **OMIVV Hosts Information** section, you can also perform the following actions:
   - Launch Remote Access Console (iDRAC)
   - Blink Server LED Indicator
   - Configure System Lockdown Mode

     When the hosts are managed using chassis, Configure System Lockdown Mode is not supported.
   - Run Firmware Update Wizard

Related information

View host inventory job on page 74

Modify host inventory job

After associating hosts to a Host Credential Profile, you must periodically schedule inventory to ensure that inventory information of hosts is up-to-date. Inventory Jobs displays the status of inventory jobs that are run on the hosts.

You can also modify the inventory schedule from the **Settings** > **Inventory Retrieval** page.

1. On the **Jobs** page, select a vCenter instance, and click 📅.
   The **Inventory Data Retrieval** dialog box is displayed.
2. Under the **Inventory Data** section, do the following:
   a. Select the **Enable Inventory Data Retrieval (Recommended)** check box.
   b. Select the inventory data retrieval day and time, and click **APPLY**.
   c. To reset the settings, click **CLEAR**.
   d. To run the inventory job now, on the **Jobs** page, click ▶.

   NOTE: For servers that do not have an iDRAC Express or Enterprise license, the inventory fails because the license upgrade is required for iDRAC.

   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 part of a chassis credential profile.

View chassis inventory job

The **Chassis Inventory** page displays information about the latest inventory job run on a chassis that is associated to a chassis credential profile.

1. On the OMIVV home page, click **Jobs** > **Invnetory** > **Chassis Inventory**.
2. To view the chassis inventory information, select a chassis.
   - **Chassis IP**—The IP address of the chassis
   - **Service Tag**—The Service Tag of the chassis The Service Tag is a unique identifier that is provided by the manufacturer for support and maintenance.
   - **Status**—The status of the chassis

- **Duration (MM:SS)**—The duration of the job in minutes and seconds
- **Start Date and Time**—The date and time when the inventory job started.
- **End Date and Time**—The date and time when the inventory job completed

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

ⓘ **NOTE:** The chassis inventory job 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.

Related tasks

Run chassis inventory job on page 76

Run chassis inventory job

1. On the OMIVV home page, click **Jobs** > **Chassis Inventory**.
2. Select a chassis and click Run now [▶].

   After the chassis inventory is complete, you can view the chassis information about the **Hosts & Chassis** > **Chassis** page.
3. To view the chassis information, on the **Chassis** page, select a chassis, and then click **VIEW**.

   ⓘ **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 triggers the chassis inventory.

Related information

View chassis inventory job on page 75

View hosts warranty

A warranty job is a scheduled task to get warranty information from www.dell.com/support on all systems. Ensure that the OMIVV appliance has Internet connectivity to extract warranty information. 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.

1. On the OMIVV home page, click **Jobs** > **Warranty** > **Host Warranty**.
2. Select a vCenter to view the associated host information.

   - **vCenters**—The lists of vCenters
   - **Hosts Passed**—The number of vCenter hosts that passed.
   - **Last Warranty**—The date and time when the last warranty job was run.
   - **Next Warranty**—The date and time when the next warranty job will run.

   The associated host information is displayed in the lower pane.

   - **Host**—The host IP address
   - **Status**—The status of the warranty job The options include:
     - Successful
     - Failed
     - In Progress
     - Scheduled
   - **Duration (MM:SS)**—The duration of the warranty job in MM:SS
   - **Start Date and Time**—The date and time when the warranty job started.
   - **End Date and Time**—The time the warranty job ended.

3. To run the host warranty on-demand, click Run now [▶].

Modify host warranty job

The warranty jobs are originally configured in the **Initial Configuration Wizard**. You can also modify warranty job schedules on the **Settings** > **Warranty Data Retrieval** page.

1. On the **Jobs** page, expand **Warranty**, and then select **Host Warranty**.
2. Select a vCenter and click 📅.
3. Under the **Warranty Data** section, do the following:
   a. Select the **Enable Warranty Data Retrieval (Recommended)** check box.
   b. Select the warranty data retrieval day and time, and click **APPLY**.
   c. To reset the settings, click **CLEAR**.

View chassis warranty

A warranty job is a scheduled task to get warranty information from Support.dell.com on all systems. 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.

1. On the OMIVV home page, click **Jobs** > **Warranty** > **Chassis Warranty**.

   A table displays all the chassis warranty job information.

   - **Chassis IP**—The host IP address
   - **Service Tag**—The Service Tag of the chassis
   - **Status**—The status of the warranty job The options include:
     - Successful
     - Failed
     - In Progress
     - Scheduled
   - **Duration (MM:SS)**—The duration of the warranty job in MM:SS
   - **Start Date and Time**—The date and time when the warranty job started.
   - **End Date and Time**—The time the warranty job ended.

2. To run the chassis warranty job on-demand, click Run now [▶].

11

Manage logs

View log history

1. On the **OpenManage Integration for VMware vCenter** page, to view all the logs, click **Logs**.

   The OMIVV log retrieval process retrieves all the logs from its database. This may take a few seconds based on the log size.

   - To export the logs data, click ⇨.
   - To sort the data in the grid, click a column header.
   - To navigate between pages, click previous and next icons.
   - To refresh the logs, click the refresh icon on the upper-left corner.

2. Click ▼ to filter the logs that is based on the following categories and or date range:

   Categories:

   - **All Categories**
   - **Information**
   - **Warning**
   - **Error**

   Date:

   - **Last Week**
   - **Last Month**
   - **Last Year**
   - **Custom Range**: If you select this option, specify start and end date by clicking the calender icon.

3. After selecting the required category and date, click **APPLY**.
   You can view the logs that are related to the selected category and or date range. The log data table displays 100 logs a page at a time.
4. To clear the filtered data, click **CLEAR FILTER**.

12

Manage OMIVV appliance settings

On the **Settings** page, you can perform the following tasks:

- Configure warranty expiration notification settings. For more information, see Configure warranty expiration notification on page 79.
- Configure the latest appliance version notification. For more information, see Configure latest appliance version notification on page 79.
- Override severity for Proactive HA alerts. For more information, see Override severity of health update notification on page 83.
- Initial Configuration. For more information, see Initial configuration on page 84
- Configure and view events and alarms. For more information, see Configure events and alarms on page 90.
- Schedule or modify data retrieval schedules for inventory and warranty. For more information, see Schedule inventory job on page 99 and Schedule warranty retrieval jobs on page 99.

Manage multiple appliances

If multiple vCenter instances share the same PSC and are registered with more than one instance of an OMIVV appliance, use the switch appliance wizard to switch between the different instances of OMIVV.

You can see the current instance of OMIVV on the home page.

1. On the **OMIVV** home page, click **CHANGE**.
    - **IP/Name**—The OMIVV appliance FQDN or IP
    - **Version**—The current version of the OMIVV appliance
    - **Compliance Status**—The status (**Compliant** or **Non-compliant**) of the OMIVV appliance based on the version
    - **Availability Status**—The availability status of the OMIVV appliance based on whether the OMIVV services are running. **OK** or **ERROR** is displayed to indicate the working status of OMIVV.
    - **Registered vCenter Servers**—The registered vCenter server FQDN or IP
    - **Actions**—The action name (**SELECT** or **SELECTED**)
2. On the **Switch OMIVV Appliance** page, click **SELECT**.
3. To confirm, click **YES**.
   You can view the change in the appliance IP on the home page.

Configure warranty expiration notification

Enable the warranty expiration notification to get notified if warranties for any of the hosts are nearing expiration.

1. On the OMIVV home page, click **Settings** > **Notifications** > **Warranty Expiration Notification**.
2. Select **Enable Warranty Expiration Notification for hosts**.
3. Select the number of days to be notified before the warranty expires.
4. Click **APPLY**.

Configure latest appliance version notification

To get notified about the availability of a new OMIVV version, select the **Enable Latest Version Notification (Recommended)** check box. Dell EMC recommends checking it on weekly basis. To use the latest appliance version notification features of OMIVV, you must have an Internet connection. If your environment requires a proxy to connect to Internet, ensure that you configure the proxy settings on the Admin portal.

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. On the OMIVV home page, click **Settings** > **Appliance Settings** > **Notifications** > **Latest Version Notification**.
2. Select the **Enable Latest Version Notification (Recommended)** check box.
3. To receive the latest appliance version notification, select the day and time.
4. Click **APPLY**.

Configure deployment credentials

OMIVV acts as a provisioning server. The deployment credentials enable you to communicate with iDRAC that uses the OMIVV plugin as a provisioning server in the auto discovery process. The deployment credentials enable you to set up iDRAC credentials to communicate securely with a bare-metal server that is discovered using auto discovery until the OS deployment is complete.

After the OS deployment process is successfully complete, OMIVV changes the iDRAC credentials as provided in the host credential profile. If you change the deployment credentials, all newly discovered systems using auto discovery are provisioned with the new iDRAC credentials from that point onwards. However, the credentials on servers that are discovered before the change of deployment credentials are not affected by this change.

1. On the OMIVV home page, click **Settings** > **Deployment Credentials**.
2. Enter the user name and password. The default user name is **root** and password is **calvin**.
   Ensure that you provide only the iDRAC supported characters and iDRAC local credentials.
3. Click **APPLY**.

Hardware component redundancy health—Proactive HA

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.

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. The moderately degraded states are represented as *Warning* in the **Type** column on the **Events** page.
- Critical (Severely degraded)—component has a critical failure.

> **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.

> **NOTE:**
>
> - When configuring events, it is recommended to select Post all Events option as event posting level. For more information about configuring events, see Configure events and alarms on page 90.
> - Proactive HA is available only on the platforms that support redundancy on power, fan, and IDSDM.
> - Proactive HA feature is not supported for PSUs for which redundancy cannot be configured (for example, cabled PSUs).

Related references

Proactive HA events on page 81

Related information

Override severity of health update notification on page 83

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:

Table 5. 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 ⓘ **NOTE:** When the hosts are added to Proactive HA 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:

Table 6. 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

Table 6. Proactive HA events (continued)

Event name	Description	Severity
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

Related tasks

Hardware component redundancy health—Proactive HA on page 80
Configure Proactive HA for Rack and Tower servers on page 82
Enable Proactive HA on clusters on page 83

Related information

Override severity of health update notification on page 83

Configure Proactive HA for Rack and Tower servers

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

1. Create a host credential profile and associate hosts to a host credential profile. See Create host credential profile on page 35.
2. Verify that hosts inventory is completed successfully. See View host inventory job on page 74.
3. Verify that the SNMP Trap destination in iDRAC is set as the OMIVV appliance IP address.

   NOTE: Ensure to confirm the availability of a host for a Proactive HA cluster from the logs data.
4. Enable Proactive HA on a cluster. See Enabling Proactive HA on a cluster.

Related references

Proactive HA events on page 81

Related information

Override severity of health update notification on page 83

Configure Proactive HA for Modular servers

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, because the chassis components (PSU and fan) failure affects all its associated servers.

1. Create a host credential profile and associate hosts with host credential profile. See Create host credential profile on page 35.
2. Verify that hosts inventory is completed successfully. See View host inventory job on page 74.

   ⓘ **NOTE:** Ensure to confirm the availability of a host for a Proactive HA cluster from the logs data.
3. Create a chassis credential profile for associated chassis. See Create chassis credential profile on page 40.
4. Verify that chassis inventory is completed successfully. See View chassis inventory job on page 75.
5. Launch CMC or OME-Modular and verify that the Trap destination for chassis is set as the OMIVV appliance IP address. For more information about configuring trap, see the CMC and OME-Modular User's Guide available at **dell.com/support**.
6. Enable Proactive HA on a cluster. See Enabling Proactive HA on a cluster.

Enable 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 host credential profile and successfully inventoried.
- For a modular server, the corresponding chassis must be added to the chassis credential profile and successfully inventoried.

1. In vSphere Client, expand **Menu**, and then select **Hosts and Clusters**.
   All the hosts and clusters are displayed in the left pane.
2. Select a cluster, in the right pane, click **vSphere DRS** > **EDIT**.
3. Select **vSphere DRS**, if not selected.
4. Select **Configure** > **vSphere Availability**, and then click **Edit**.
   The **Edit Cluster Settings** page is displayed.
5. On the **Edit Cluster Settings** page, select **Proactive HA**.
6. In the **Failures & Responses** section, from the drop-down menu, select **Manual** or **Automated** automation level.
7. 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.
8. Click **Providers** and select **Dell Inc** as a provider for the cluster.
9. Click **SAVE**.

After Proactive HA is enabled on a cluster, OMIVV initializes Proactive HA health and redundancy status and reports them to vCenter. Based on the health update notification from OMIVV, the vCenter server performs the manual or automatic action that you have selected for **Remediation**.

To override the existing severity, see Override severity of health update notification on page 83.

Related references

Proactive HA events on page 81

Related information

Override severity of health update notification on page 83

Override 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, click **Settings** > **Proactive HA Configuration**.
   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.
2. To change severity of a host or its component, in the **Override Severity** column, select the required status from the drop-down list.
   This policy applies to all the Proactive HA hosts across all vCenter servers that are registered with OMIVV.
3. Repeat step 2 for all the events that must be customized.
4. Perform any one of the following actions:
   a. To save the customization, click **APPLY**.
   b. To cancel the override severity settings, click **CANCEL**.

   To reset the override severity settings to default, click **RESET TO DEFAULT**.

Related references

Proactive HA events on page 81

Related tasks

Hardware component redundancy health—Proactive HA on page 80

Configure Proactive HA for Rack and Tower servers on page 82

Enable Proactive HA on clusters on page 83

Initial configuration

After you complete the basic installation of OMIVV and registration of the vCenters, the Initial Configuration Wizard is displayed automatically for the first time, when you launch OMIVV in vCenter.

If you want to launch the initial configuration wizard later, go to:

- **Settings** > **Initial Configuration Wizard** > **START INITIAL CONFIGURATION WIZARD**
- **Dashboard** > **Quick References** > **START INITIAL CONFIGURATION WIZARD**

1. On the **Welcome** page, read the instructions, and then click **GET STARTED**.
2. On the **Select vCenter** page, from the **vCenters** drop-down menu, select a specific vCenter or **All Registered vCenters**, and then click **NEXT**.

   ⓘ **NOTE:** If you have multiple vCenter servers that are part of the same PSC registered with the same OMIVV appliance, and if you choose to configure a single vCenter server, repeat step 2 until you configure each vCenter.
3. On the **Create Host Credential Profile** page, click **CREATE HOST CREDENTIAL PROFILE**.
   For more information about creating a host credential profile, see Create host credential profile on page 35.

   After hosts are added to a host credential profile, the IP address of OMIVV is automatically set as SNMP trap destination for host's iDRAC. OMIVV automatically enables the 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 non-complaint. To view and fix the non-compliance, see Fix a non-compliant host on page 67 .
4. On the **Configure Additional Settings** page, do the following:
   a. Schedule inventory jobs. For more information about scheduling the inventory job, see Schedule inventory job on page 99.
   b. Schedule warranty retrieval job. For more information about scheduling the warranty retrieval job, see Schedule warranty retrieval jobs on page 99.

      If you want to modify the inventory job schedule, go to **Settings** > **Inventory Data Retrieval**or **Jobs** > **Host Inventory**.

      If you want to modify the warranty retrieval job schedule, go to **Settings** > **Warranty Retrieval** > **Jobs** > **Warranty**.
   c. Configure events and alarms. For information about configuring events and alarms, see Configure events and alarms on page 90.
   d. To apply individual settings, click the **Apply** button separately, and then click **NEXT**.

It is highly recommended to enable all the additional settings. If any of the additional settings are not applied, a message is displayed indicating that the all the additional settings are mandatory.

5. On the **Next Steps** page, read the instructions, and then click **FINISH**.

   Dell EMC recommends associating your OMIVV hosts with a configuration baseline because it enables you to closely monitor the configuration changes happening in hosts and associated clusters. Configuration baseline can be created for any cluster once the hosts are successfully managed by OMIVV. To create a configuration baseline, do the following:

   - Create Repository Profile for Firmware and Driver—This helps you to define baselined firmware and driver versions.
   - Create System Profile—This helps you to define baselined hardware configurations for hosts.
   - Create Cluster Profile—To create successful baseline, select clusters and associate firmware, drivers, and hardware configurations.
   - The hosts present in a PowerEdge MX chassis with an iDRAC IPv4 disabled has to be managed using a chassis credential profile.

Related tasks

Create repository profile on page 44

Create system profile on page 61

Create cluster profile on page 49

View initial configuration status

On the Initial Configuration wizard page, you can perform the following:

- View initial configuration status

  Initial configuration status shows completed only when all the vCenters are configured with host credential profile, events and alarms, inventory and warranty jobs.

- Launch initial configuration wizard

View licensing information

When you upload OMIVV license, the number of supported hosts and vCenter servers are displayed in this tab.

To buy a software license, click **Buy License** next to **Software License**. For more information, see Buy software license on page 86.

The following information is displayed on the **Licensing** page:

License Type	Description
Host Licenses	● Licenses Available Displays the number of available licenses ● Licenses In Use Displays the number of licenses in use
vCenter Licenses	● Licenses Available Displays the number of available licenses ● Licenses In Use Displays the number of licenses in use

The **License Management** section displays the links to the following:

- Product licensing portal (Digital Locker)
- Admin console

Related concepts

OpenManage Integration for VMware vCenter licensing on page 86

Related tasks

Buy software license on page 86

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—you can purchase any number of host licenses that are managed by OMIVV. This license includes product support and OMIVV Appliance updates.

The OMIVV supports up to 15 vCenters. 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 15 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 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 keys, contact Dell Support by going to Order Support to locate the regional Dell Support phone number for your product.

Related tasks

Buy software license on page 86

Related information

View licensing information on page 85

Buy software license

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

1. Go to **Settings** > **Licensing** > **Buy License**, or **Dashboard** > **Buy License**, or **Admin Portal** > **vCenter Registration** > **Licensing** > **BUY NOW**.
2. Download and save the license file to a known location.
   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.

Related concepts

OpenManage Integration for VMware vCenter licensing on page 86

Related information

View licensing information on page 85

Access support information

Table 7. Information on the support page

Name	Description
Documentation Support	Provides the following documentation links: ● PowerEdge Servers ● OMIVV Manuals ● iDRAC with Lifecycle Controller
Administration Console	Provides a link to the Administration Console.
General Help	Provides a link to the Dell EMC support site.
Reset iDRAC	Provides a link to reset iDRAC that can be used when iDRAC is not responsive. This reset performs a normal iDRAC reboot. For more information about resetting iDRAC, see Reset iDRAC on page 87.
Before calling Tech Support	Provides tips on how to contact Dell EMC 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 Create and download troubleshooting bundle on page 87.
Dell EMC Recommendations	Provides a link to the Dell EMC Repository Manager (DRM) support page. The DRM is used to create a custom catalog, that can be used to update firmware and drift detection.

Create and download troubleshooting bundle

To generate the troubleshooting bundle, ensure that you log in to Admin portal.

The troubleshooting bundle contains OMIVV appliance logging information that can be used to help in resolving issues or sent to Technical Support.

1. On the **Support** page, click **Create and download troubleshooting bundle**.
   The **Troubleshooting Bundle** dialog box is displayed.
2. In the **Troubleshooting Bundle** dialog box, click **CREATE**.
   Depending on the size of the logs, creating the bundle may take some time.
3. To save the file, click **DOWNLOAD**.

Reset iDRAC

Resetting iDRAC performs a normal iDRAC reboot. After resetting iDRAC, the iDRAC is normally restarted but not the host. After resetting, iDRAC can be used only after few minutes. Reset only if an iDRAC is not responding on an OMIVV appliance.

- You can only apply this reset action on a host that is part of a host credential profile that has been inventoried at least once.
- Dell EMC recommends you to switch the host to maintenance mode, and then reset the iDRAC.
- After resetting the iDRAC, if the iDRAC becomes unusable or stops responding, hard reset the iDRAC. For information about hard reset, see the iDRAC User's Guide available at https://www.dell.com/support/.

While iDRAC is rebooting, you may see:

- Delay in communication while the OMIVV retrieves the host health status.
- All sessions currently opened to iDRAC are ended.
- A change in the DHCP address of iDRAC. If iDRAC uses DHCP for generating its IP address, then the iDRAC IP address may change. In this case, rerun the host inventory job to get the new iDRAC IP address in the inventory data.

1. On the **Support** page, click **RESET iDRAC**.
2. On the **iDRAC RESET** page, enter the hostname or IP address.

3. To confirm that you understand the iDRAC reset process, select the **I understand the effects of resetting iDRAC. Continue to reset iDRAC on the selected host** check box.
4. Click **RESET iDRAC**.

13

Manage vCenter settings

About events and alarms

On the **Settings** page, you can enable the events and alarms for hosts and chassis, select the event posting level, and restore default alarms. You can configure events and alarms for each vCenter or for all registered vCenters. The events and alarms corresponding to a chassis are associated with vCenter.

The following are the four event posting levels:

Table 8. Event posting level

Event	Description
Do not post any events	Do not allow OMIVV to forward any events or alerts into its associated vCenters.
Post all events	Post all events, including informal events, that the OMIVV receives from managed Dell EMC hosts into its associated vCenters. It is recommended to select the **Post all Events** option as an event posting level.
Post only critical and warning events	Posts only events with either a critical or warning into its associated vCenters.
Post only virtualization-related critical, and warning events	Post virtualization-related events that are 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, the critical hardware alarms can trigger the OMIVV appliance to put the host system into a maintenance mode. In certain cases, migrate the virtual machines to another host system. The OMIVV forwards events that are received from managed hosts to vCenter 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 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. Dell EMC recommends enabling the DRS before enabling the Dell alarms. For more information, see the VMware documentation.

The 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 the vCenter instance that might be impacted. Ensure that you confirm that the clusters are impacted before enabling events and alarms.

If you want to restore the default alarm settings, select the **Restore Alarms** option. This option 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 the **Restore Alarms** option.

NOTE: To receive the Dell events, ensure that you enable the required events in iDRAC, CMC, and Management Controller.

NOTE: The OMIVV 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 EMC alarms are enabled, the clusters should use DRS to ensure that the virtual machines that send critical events are automatically migrated.

Configure events and alarms

To receive events from the servers, ensure that the SNMP trap destination is set in iDRAC. OMIVV supports SNMP v1 and v2 alerts.

1. On the OMIVV home page, click **Settings** > **vCenter Settings** > **Events and Alarms**.
2. To enable alarms for all hosts and its chassis, click **Enable Alarms for all hosts and its chassis**.
   The **Enable the Dell EMC Alarm Warning** page displays the clusters and non-clustered host that might be impacted after enabling the Dell EMC alarms.

   ⓘ **NOTE:** The Dell EMC hosts that have alarms that are enabled to respond to some specific critical events by entering in to maintenance mode. You can modify the alarm, when required.

   ⓘ **NOTE:** In vCenter 6.7 U1 and 6.7 U2, the edit option fails. For editing alarm definitions, Dell EMC recommends using Web Client (FLEX).

   ⓘ **NOTE:** BMC Traps do not have Message IDs, so alerts will not have these details in OMIVV.
3. To accept the change, click **CONTINUE**.
   The alarms for all hosts and its chassis are enabled.
4. Select any one of the following event posting levels:
   - **Do not post any events**—Do not forward any events or alerts into its associated vCenters.
   - **Post all Events**—Post all the events including informational events, and events received from the managed hosts and chassis into its associated vCenters. Dell EMC recommends selecting the Post all Events option as an event posting level.
   - **Post only Critical and Warning Events**—Post only the critical and warning level events into its associated vCenters.
   - **Post only Vitalization-Related Critical and Warning Events**—Post the virtualization-related events received from hosts into its associated vCenters. Virtualization-related events are those that are most critical to hosts running VMs.
5. To save the changes, click **APPLY**.

   To restore the default vCenter alarm settings for all hosts and its chassis, click **RESTORE ALARMS**. It might take up to a minute before the change takes effect.

   The **RESTORE ALARMS** option is a convenient way to restore the default alarm configuration without uninstalling and reinstalling the product. If any Dell EMC alarm configurations are changed since installation, those changes are reverted using the **RESTORE ALARMS** option.

   ⓘ **NOTE:** The events and alarms settings are not enabled after restoring the appliance. You can enable the Events and Alarms settings again from the Settings tab.

Related tasks

View alarms and events setting on page 91
View chassis events on page 90
View chassis alarms on page 91

View chassis events

1. In vSphere Client, expand **Menu**, and then select **Hosts and Clusters**.
2. In the left pane, select an instance of vCenter.
3. In the right pane, click **Monitor** > **Tasks and Events** > **Events**.
4. To view more information, select a specific event.

   ⓘ **NOTE:** For a PowerEdge MX chassis with MCM configuration, the source of the event is displayed as lead chassis, however, the message details have the Service Tag of the member chassis for identification.

Related information

Configure events and alarms on page 90

View chassis alarms

1. In vSphere Client, expand **Menu**, and then select **Hosts and Clusters**.
2. In the left pane, select an instance of vCenter.
3. In the right pane, click **Monitor** > **Issues and Alarms** > **Triggered Alarms**.
4. In **Triggered Alarms**, click alarm name to view the alarm definition.

Related information

Configure events and alarms on page 90

View alarms and events setting

After 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. On the OMIVV home page, click **Settings** > **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 Configure events and alarms on page 90.

To view the event posting levels, see About events and alarms on page 89.

Related information

Configure events and alarms on page 90

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 9. 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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended 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
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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended 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 that a battery is in a predictive failure state	Warning	No action
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	Warning	No action

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended action
	exceeded its warning threshold		
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
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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended 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
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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended 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
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 **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	Warning	Remove and reinstall failed fans or install additional fans

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended action
	occurred, which requires 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 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 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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended action
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
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

Table 9. Virtualization events (continued)

Event name	Description	Severity	Recommended action
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

Data retrieval schedule

Schedule inventory job

To view the latest inventory data on OMIVV, you must schedule an inventory job to run periodically to ensure that inventory information of hosts or the chassis is up-to-date. Dell EMC recommends running the inventory job on a weekly- basis.

ⓘ **NOTE:** The chassis is managed in OMIVV context. There is no context of vCenter in chassis management. After scheduled host inventory is complete, the chassis inventory is triggered for all the chassis that are managed using OMIVV.

ⓘ **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. Select the **Enable Inventory Data Retrieval (Recommended)** check box.

   In PSC environment with multiple vCenter servers, if the schedule for individual vCenter is different and you select the **All Registered vCenters** option to update the inventory schedule, the inventory schedule settings page displays the default schedule.
2. Select the inventory data retrieval day and time, and click **APPLY**.

   ⓘ **NOTE:** In PSC environment with multiple vCenter servers, if you update the inventory schedule of **All Registered vCenters**, the update overrides the individual vCenter inventory schedule settings.

Schedule warranty retrieval jobs

1. Ensure that the inventory is run successfully on hosts and chassis.
2. To use the warranty features of OMIVV, you must have an Internet connection. If your environment requires proxy to reach Internet, ensure that you configure the proxy settings in the Admin portal.

Hardware warranty information is retrieved from Dell Online and displayed by OMIVV. Only the Service Tag is sent and not stored by Dell Online.

In PSC 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 credential 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. Select the **Enable Inventory Data Retrieval (Recommended)** check box.

   In PSC environment with multiple vCenter servers, if the schedule for individual vCenter is different and you select the **All Registered vCenters** option to update the warranty schedule, the warranty schedule settings page displays the default schedule.
2. Select the warranty data retrieval day and time, and click **APPLY**.

   ⓘ **NOTE:** In PSC environment with multiple vCenter servers, if you update the warranty schedule of **All Registered vCenters**, the update overrides the individual vCenter warranty schedule settings.

14

Chassis Management

View Dell EMC chassis information

You can view the chassis information that is discovered and inventoried using OMIVV. Dell EMC chassis lists all the Chassis that is managed by OMIVV.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The following information is displayed:
   - **Name**—Displays an IP address link for each Dell EMC chassis.
   - **IP Address/FQDN**—Displays the vCenter IP address or FQDN.
   - **Service Tag**—Displays the Service Tag of the chassis.
   - **Chassis URL**—Displays the chassis URL.
   - **Model**—Displays the model name.
   - **Role**—Applicable only for MX chassis. Displays the role of the chassis (Lead or Member).
   - **Last Inventory**—Displays the last inventory information.
   - **Available Slots**—Displays the available slots in chassis.
   - **Profile Name**—Displays the chassis credential profile name in which the chassis is associated.
   - **Location**—Displays the location of the chassis.

   If you do not run the inventory, the **Name**, **Last Inventory**, **Available Slots**, **Profile Name**, **Location** , and chassis inventory information are not displayed.

   NOTE: For a PowerEdge 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 or chassis role is changed, Dell EMC recommends removing the existing lead chassis and adds the new lead chassis IP again, and then associate to the chassis credential profile.
2. Select a chassis to view firmware, license type, and warranty-related information.
   If you do not run the inventory, the **Name**, **Firmware**, **License Type**, and **Warranty** information are not displayed.

View chassis inventory information

1. On the **Dell EMC Chassis** page, select a chassis or click Service Tag.
2. In the **Chassis Information** section, click **VIEW**.
   The **Overview** page displays the health of the chassis, the active errors, the component level health status of the chassis, hardware overview, and chassis relation (only for MX chassis).

   NOTE: It may take up to one minute to display the information such as chassis health and active errors because the OMIVV gets live information from the chassis devices.

   NOTE: For M1000e version 4.3 and earlier, the active errors are not displayed.

   The main pane displays the overall health of a chassis. The valid health indicators are **Healthy**, **Warning**, **Critical**, and **Unknown**. 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.

   The overall health indicates the health that is based on the chassis with the least health parameter. For example, if there are five healthy signs and one warning sign, the overall health is shown as warning.

Viewing hardware inventory information for chassis

You can view information about the hardware inventory for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Hardware**.

Table 10. Hardware inventory information

Hardware inventory: Component	Navigation through OMIVV	Information
Fans	● On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. ● On the **Overview** page, in the left pane, select **Hardware**. ● In the right pane, expand **Fans**. **OR** ● On the **Overview** page, click **Fans**.	Information about fans: ● Name ● Present ● Identifier (applicable only for MX chassis) ● Power State ● Reading (RPM) ● Warning Threshold (not applicable for MX chassis) ● Critical Threshold (not applicable for MX chassis) ○ Minimum ○ Maximum ● Pulse Width Modulation (Only for MX chassis) ⓘ **NOTE:** In a PowerEdge 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	● On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. ● On the **Overview** page, in the left pane, select **Hardware**. ● In the right pane, expand **Power Supplies**. **OR** ● On the **Overview** page, click **Power Supplies**.	Information about power supplies: ● Name ● Capacity ● Present ● Power state ● Input Voltage (Only for PowerEdge MX chassis).
Temperature Sensors	● On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. ● On the **Overview** page, in the left pane, select **Hardware**. ● In the right pane, expand **Temperature Sensors**. **OR** ● On the **Overview** page, click **Temperature Sensors**.	Information about temperature sensors: ● Location ● Reading ● Warning threshold ○ Maximum ○ Minimum ● Critical threshold ○ Maximum ○ Minimum ⓘ **NOTE:** For a PowerEdge M1000e chassis, information about chassis temperature is displayed. For other chassis,

Table 10. Hardware inventory information (continued)

Hardware inventory: Component	Navigation through OMIVV	Information
		information about the temperature sensors is displayed for chassis and associated modular servers.
I/O Modules	- On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. - On the **Overview** page, in the left pane, select **Hardware**. - In the right pane, expand **I/O Modules**. **OR** - On the **Overview** page, click **I/O Modules**.	Information about I/O modules: - Slot/Location - Present - Name - Fabric - Service Tag - Power Status - Role - Firmware version - Hardware version - IP address - Subnet mask - Gateway - MAC address - DHCP enabled
Fabric (Only for PowerEdge MX chassis)	- On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. - On the **Overview** page, in the left pane, select **Hardware**. - In the right pane, expand **Fabric**. **OR** - On the **Overview** page, click **Fabric**.	Information about fabric components: - Health - Fabric - Description - Switch Count - Compute Count - Uplink Count To view the switches that are associated with the fabric, select a fabric component and the following information is displayed in the lower grid: - Switch - Chassis - Slot - Chassis Role - Switch Model
PCIe	- On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. - On the **Overview** page, in the left pane, select **Hardware**. - In the right pane, expand **PCIe**. **OR** - On the **Overview** page, click **PCIe**.	Information about PCIe: - PCIe slot ○ Slot ○ Name ○ Power status ○ Fabric - Server slot ○ Name ○ Number - Slot type - Server mapping - Assignment status - Allocated slot power - PCI ID - Vendor ID

Table 10. Hardware inventory information (continued)

Hardware inventory: Component	Navigation through OMIVV	Information
		ⓘ **NOTE:** PCIe information is not applicable for M1000e chassis.
iKVM—Only for PowerEdge M1000e	● On the **Dell EMC Chassis** page, click **Chassis** > **Chassis List**, click the Service Tag link. ● On the **Overview** page, in the left pane, select **Hardware**.In the right pane, expand **iKVM**. **OR** ● On the **Overview** page, click **iKVM**.	Information about iKVM: ● iKVM Name ● Present ● Firmware version ● Front Panel USB/Video enabled ● Allow access to CMC CLI. ⓘ **NOTE:** The iKVM tab is displayed only if the chassis contains iKVM module.

View firmware inventory information

You can view the firmware-related information for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Firmware**.

   The following information about firmware is displayed:

   - Component
   - Current Version

   On this page, you can also launch OpenManage Enterprise Modular and CMC.

View management controller information

You can view the management controller-related information for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Management Controller**.

   The following information about Management Controller is displayed:

   - General
     - Name
     - Firmware Version
     - Last Update Time
     - Chassis Location
     - Hardware Version
   - Common Network
     - DNS Domain Name
     - Use DHCP for DNS
     - MAC Address

    - Redundancy Mode
    - Hardware Version
- IPv4 Information
    - IPv4 Enabled
    - DHCP Enabled
    - IP Address
    - Subnet Mask
    - Gateway
    - Preferred DNS Server
    - Alternate DNS Server
- IPv6 Information
    - IPv6 Enabled
    - DHCP Enabled
    - IP Address
    - Link Local Address
    - Gateway
    - Preferred DNS Server
    - Alternate DNS Server
- Local Access Configuration
    - Quick Sync Hardware Present
    - LCD Present
    - LED Present
    - KVM Enabled

> **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.

View storage inventory information

You can view the storage-related information for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Storage**.

   The following information about storage is displayed:

   - Virtual Disks
   - Physical Disks
   - Controllers
   - Enclosures
   - Hot Spares

   For MX chassis, the following information is displayed:

   - Slot Number
   - Slot Name
   - Model
   - Service Tag
   - Firmware version
   - Asset Tag
   - Power State
   - Assignment Mode

   For MX chassis, if you want to view information about drives, click storage sled. The following drive information is displayed in the lower pane:

- Health
- State
- Slot
- Slot Assignment
- Disk Name
- Capacity
- Bus protocol
- Media

If a disk in the PowerEdge MX chassis is unassigned, its slot assignment is shown as **NA**.

For M1000e chassis, if you have a storage module, the following storage details are displayed in a grid view without any additional information:

- Name
- Model
- Service Tag
- IP Address (Link to storage)
- Fabric
- Group Name
- Group IP Address (link to storage group).

ⓘ **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, additional information is displayed for each highlighted item.

View warranty information

You can view the warranty-related information for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Warranty**.

   Information about warranty:

   - Provider
   - Description
   - Status
   - Entitlement Type
   - Start Date
   - End Date
   - Days Left
   - Last Updated

   ⓘ **NOTE:** To view warranty status, ensure that you run a warranty job. See Schedule warranty retrieval jobs on page 99.

View related host for chassis

You can view information about the related host for the selected chassis.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.
3. On the **Overview** page, click **Related Hosts**.
   The following information about the associated host is displayed:

- Hostname
- Service Tag
- Model
- iDRAC IP
- Location
- Slot
- Last Inventory

4. To view more information about host, select a host.

View related chassis information

The **Chassis Relation** section shows the relationship between chassis in an MX chassis that is deployed in the MCM mode.

ⓘ **NOTE:** Related chassis information is applicable only for a PowerEdge MX chassis that is configured in an MCM group.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List**.
   The **Dell EMC Chassis** page is displayed.
2. Select a chassis, click the Service Tag link.
   The **Overview** page is displayed.

   On the **Overview** page, the **Chassis Relation** section displays all the associated chassis information for lead and member chassis.

Manage PowerEdge MX 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 for PowerEdge MX7000 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 a host credential 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 host credential profile, see Create host credential profile on page 35.
2. **Managing the servers using a chassis credential profile**: If you choose to manage your hosts using the chassis credential profile, OMIVV features such as, inventory, monitoring, firmware, and driver updates are supported. For more information about managing chassis and host using the chassis credential profile, see Create chassis credential profile on page 40.

ⓘ **NOTE:** OMIVV does not support managing the PowerEdge MX chassis with backup lead configuration.

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

- iDRAC Lockdown mode
- Ability to use this server as a reference server to capture System Profile
- OS deployment
- Getting or updating CSIOR status
- Server configuration compliance
- Few inventory-related information

ⓘ **NOTE:** The hosts with a public IPv4 iDRAC IP can also be managed using the chassis credential profile. However, it is not recommended because 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 host credential 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 credential 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 Add PowerEdge MX Chassis on page 107.

2. Create a chassis credential profile and associate the hosts.

   For more information about creating a chassis credential profile, see Create chassis credential profile on page 40.

3. View jobs for both chassis and host that is managed using the chassis credential profile.
4. View chassis and host inventory.

   For more information about host and chassis inventory, see View host inventory job on page 74 and View chassis inventory job on page 75.

5. Perform firmware update on hosts that are managed using chassis.

   For more information about firmware update, see Firmware update on page 121.

   ⓘ **NOTE:** Bare-metal workflow is not supported when the hosts are managed using chassis.

Add PowerEdge MX Chassis

A host with valid IPv4 iDRAC IP can be added to host credential 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 credential profile to manage the chassis and its associated hosts.

To add an MX chassis manually, do the following:

1. On the **OMIVV** home page, click **Hosts & Chassis** > **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 credential profile by creating a chassis credential profile. For more information about creating a chassis credential profile, see Create chassis credential profile on page 40.

ⓘ **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 credential profile.

ⓘ **NOTE:** The test connection fails, if the hosts are not present in the registered vCenters that are associated to the added MX chassis.

ⓘ **NOTE:** For a PowerEdge MX chassis configured in an MCM configuration, the lead and member must have same credentials.

MX chassis firmware update

Before scheduling the firmware update, ensure that the following conditions are met in the environment:

- Ensure that the MX chassis is part of chassis credential profile and successfully inventoried.
- If any of its hosts are undergoing firmware updates, chassis firmware cannot be updated.

ⓘ **NOTE:** By using the MX chassis firmware update feature, you can update only management module firmware.

ⓘ **NOTE:** MX chassis firmware update feature is only supported on medium, large, and extra large deployment modes.

1. On the OMIVV home page, click **Hosts & Chassis** > **Chassis** > **Chassis List** > **MX CHASSIS FIRMWARE UPDATE**.
2. On the **Chassis Firmware Update** page of the wizard, read the instructions, and then click **GET STARTED**.
3. From the **MX Chassis List**, select one or more MX chassis, and then click **NEXT**.

   The chassis is not displayed if any one of the following conditions is not met in the environment:

   - Chassis firmware update is in progress from OMIVV.
   - Chassis credential profile is not created for the chassis.
   - The inventory is not successful for the chassis.

   For the PowerEdge MX chassis with MCM configuration, you can select only the lead chassis. The member chassis is selected automatically.

4. On the **Select Update Source** page, do the following:
   a. Select an appropriate firmware repository profile from the drop-down menu.
   b. Based on the chassis and firmware repository profile you have selected, select the appropriate bundles from the identified system category.
5. On the **Select Firmware Components** page, select the firmware components that require an update, and then click **NEXT**.

   The components which have lower version than the available version in the catalog, or it is in the same level (Up-to-Date) cannot be selected. To select the components that are listed in downgrade state, click **Allow Firmware downgrade**.

   In a PowerEdge MX chassis associated with an MCM configuration, the firmware version can be downgraded even if the **Allow Firmware Downgrade** check box is not selected.

   You cannot select only member chassis for update or downgrade. Selecting the lead chassis automatically selects the member chassis.

   To select all the firmware components across all the pages, click ☑.

   To clear all the firmware components across all the pages, click X.

6. On the **Schedule Job** page, do the following:
   a. Enter the firmware update job name and description. The description is an optional field.

      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.
   b. Select an appropriate schedule option to apply the updates.
7. On the **Review Summary** page, review the firmware update details, and then click **FINISH**.

Table 11. Total number of concurrent MX chassis firmware updates for each deployment mode

Deployment Mode	Number of concurrent chassis firmware updates
Small	0
Medium	1
Large	2
Extra Large	2

15

Host Management

View OMIVV hosts

You can view all the OMIVV-managed hosts on the **OMIVV Hosts** page.

1. On the OMIVV home page, click **Hosts & Chassis** > **Hosts**.
2. On the **OMIVV Hosts** tab, view the following information:
   - **Host Name**—displays the IP address of the host. To view the host information, select a host.
   - **vCenter**—displays vCenter IP address of the host.
   - **Cluster**—displays the cluster name, if the Dell EMC host is in a cluster.
   - **Host Credential Profile**—displays the name of the host credential profile.

Monitor single host

The OMIVV enables you to view detailed information of a single host. You can view all the OMIVV hosts on the **Hosts and Clusters** page. To view more information, select a specific OMIVV-managed host, and then go to **Monitor** > **OMIVV Host Information**.

Viewing host summary information

You can view the host summary details for an individual host on the **Summary** page, where various portlets are displayed. Two of the portlets are applicable for OMIVV. 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. On the OMIVV home page, expand **Menu**, and then select **Hosts and Clusters**.
2. In the left pane, select the specific host.
3. In the right-pane, Click **Summary**.
4. Scroll down to view the OMIVV Server Management portlet.

   You can view the following information in the **OMIVV Host Information** and **OMIVV Host Health** section:

Table 12. OMIVV Host Information

Information	Description
Service Tag	Displays the Service Tag of the server. Use this ID when you call for support.
Model Name	Displays the model name of the server.
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 PowerEdge servers that support Fault Resilient Memory (FRM) option, running ESXi 5.5 or later version. The four different values of BIOS attribute are:

Table 12. OMIVV Host Information (continued)

Information	Description
	- 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. - 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. - Enabled and Not Protected: This value indicates that it supports the system with operating system version lesser than ESXi 5.5. - 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. - 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 iDRAC 8 and later servers. A closed lock represents the iDRAC Lockdown Mode is turned on whereas an opened lock represents the iDRAC Lockdown Mode is turned off.
Identification	Displays the following: - Hostname—Displays name of the OMIVV-managed host - Power State—Displays if power is ON or OFF. - iDRAC IP—Displays the iDRAC IP address - Management IP—Displays the management IP address - Host Credential Profile—Displays the host credential profile name for this host - Model—Displays the Dell EMC server model - Service Tag—Displays the Service tag for the server. - Asset Tag—Displays the Asset tag - Warranty Days Left—Displays the days left for the warranty - Last Inventory Scan—Displays the date and time of the last inventory scan
Hypervisor & Firmware	Displays the following: - Hypervisor—Displays the Hypervisor version - BIOS Version—Displays the BIOS version - Remote Access Card Version—Displays the remote access card version
Management Consoles	Displays a link to launch the Remote Access Console (iDRAC).
Host Actions	To blink at various time intervals, set up the physical server to blink at various time intervals. See Set up blink indicator light on page 130.

Table 13. 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,

Table 13. OMIVV host health

Information	Description
	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 that is based on the chassis with the least health parameter. The options include: ● Healthy (green check mark)—component operating normally ● Warning (yellow triangle with exclamation point)—component has a noncritical error. ● Critical (red X)—component has a critical failure. ● 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 is not available for hosts with cabled PSU or for modular servers.

View OMIVV host information

You can view the hardware, storage, firmware, power monitoring, warranty, and system event log information about all the OMIVV-managed hosts on the **OMIVV Host Information** page.

1. On the OMIVV home page, expand **Menu**, and then select **Hosts and Clusters**.
2. In the left pane, select a host, and then click **Monitor** > **OMIVV Host Information**.

View hardware information of a host

Table 14. Hardware information for a single host

Hardware: *Component*	Information
FRU	● **Part Name**—displays the FRU part name. ● **Part Number**—displays the FRU part number. ● **Manufacturer**—displays the name of the manufacturer. ● **Serial Number**—displays the serial number of the manufacturer. ● **Manufacture Date**—displays the manufacture date.
Processors	● **Socket**—displays the slot number. ● **Speed**—displays the current speed. ● **Brand**—displays the processor brand. ● **Version**—displays the processor version. ● **Cores**—displays the number of cores in this processor.
Power Supplies	● **Type**—displays the type of power supply. The power supply types include: ○ UNKNOWN ○ LINEAR ○ SWITCHING ○ BATTERY ○ UPS

Table 14. Hardware information for a single host (continued)

Hardware: *Component*	Information
	○ CONVERTER ○ REGULATOR ○ AC ○ DC ○ VRM ● **Location**—displays the location of the power supply, such as slot 1. ● **Output (Watts)**—displays the power in watts.
Memory	● **Memory Slots**—displays the Used, Total, and Available memory count. ● **Memory Capacity**—displays the Installed Memory, Total Memory Capacity, and Available Memory. ● **Slot**—displays the DIMM slot. ● **Size**—displays the memory size. ● **Type**—displays the memory type.
NICs	● **Total**—displays the total count of available network interface cards. ● **Name**—displays the NIC name. ● **Manufacturer**—displays only the manufacturer name. ● **MAC Address**—displays the NIC MAC address.
PCI Slots	● **PCI Slots**—displays the Used, Total, and Available PCI slots. ● **Slot**—displays the slot. ● **Manufacturer**—displays the manufacturer name of the PCI slot. ● **Description**—displays the description of the PCI device. ● **Type**—displays the PCI slot type. ● **Width**—displays the data bus width, if available.
Remote Access Card	● **IP Address**—display the IP address for the remote access card. If you are managing hosts using unified IP address, the iDRAC IP is not displayed in this section. ● **MAC Address**—displays the MAC address for the remote access card. ● **RAC Type**—displays the type of the remote access card. ● **URL**—displays the live URL for the iDRAC associated with this host.

View storage information of a host

You can view the count of Virtual Disks, Controllers, Enclosures, and associated Physical Disks with the Global Hot Spares, and Dedicated Hot Spare. To view more information about each of the storage components, from the **View** drop-down menu, select the specific component.

For hosts managed using chassis, the complete storage information that is Controller, Enclosures, Global Hot Spare, and Dedicated Hot Spare are not displayed.

NOTE: When the hosts are managed by using chassis profile, if you click **Storage**, and then select the following from the **View** drop-down menu:

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

Table 15. Storage details for a single host

Information	Description
Virtual Disks	● **Name**—displays the name of the virtual drive. ● **Device FQDD**—displays the FQDD. ● **Physical Disk**—displays on which physical disk the virtual drive is located. ● **Capacity**—displays the capacity of the virtual drive. ● **Layout**—displays the layout type of the virtual storage, which means the type of RAID that was configured for this virtual drive. ● **Media Type**—displays either SSD or HDD. To view information such as Stripe Size, Bus Protocol, and Cache Policy, select a virtual disk. ● **Controller ID**—displays the controller ID. ● **Device ID**—displays the device ID. ● **Stripe Size**—displays the stripe size, which is the amount of space that each stripe consumes on a single disk. ● **Bus Protocol**—displays the technology that the physical disks in the virtual drive are using. The possible values are: ○ SCSI ○ SAS ○ SATA ● **Default Read Policy**—displays the default read policy that is supported by the controller. The options include: ○ Read-Ahead ○ No-Read-Ahead ○ Adaptive Read-Ahead ○ Read Cache Enabled ○ Read Cache Disabled ● **Default Write Policy**—displays the default write policy that is supported by the controller. The options include: ○ Write-Back ○ Force Write Back ○ Write Back Enabled ○ Write-Through ○ Write Cache Enabled Protected ○ Write Cache Disabled ● **Cache Policy**—displays if cache policy is enabled.
Physical Disks When you select this option from the **View** drop-down menu, the **Filter** drop-down list is displayed. The following options are available in the filter: ● **All Physical Disks** ● **Global Hot Spares** ● **Dedicated Hot Spares** ● The last option displays custom name of the virtual drives.	● **Name**—displays the name of the physical disk. ● **Device FQDD**—displays the device FQDD. ● **Capacity**—displays the physical disk capacity. ● **Disk Status**—displays physical disk status. The options include: ○ ONLINE ○ READY ○ DEGRADED ○ FAILED ○ OFFLINE ○ REBUILDING ○ INCOMPATIBLE ○ REMOVED ○ CLEARED ○ SMART ALERT DETECTED ○ UNKNOWN ○ FOREIGN

Table 15. Storage details for a single host (continued)

Information	Description
	○ UNSUPPORTED ● **Configured**—displays whether the disk is configured. ● **Hot Spare Type**(Not applicable for PCIe)—shows the hot spare type. The options include: ○ No—there is no hot spare. ○ Global—an unused backup disk that is part of the disk group ○ 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. ● **Virtual Disk**—displays the name of the virtual drive. ● **Bus Protocol**—displays the bus protocol. ● **Controller ID**—displays the controller ID. ● **Media Type**—displays either SSD or HDD. ● **Remaining Rated Write Endurance**—displays the SSD remaining write endurance. ● **Connector ID**—displays the connector ID. ● **Enclosure ID**—displays the enclosure ID. ● **Device ID**—displays the device ID. ● **Model**—displays the model number of the physical storage disk. ● **Part Number**—displays the storage part number. ● **Serial Number**—displays the storage serial number. ● **Vendor**—displays the storage vendor name.
Controllers	● **Controller ID**—displays the controller ID. ● **Name**—displays the name of the controller. ● **Device FQDD**—displays the FQDD of the device. ● **Firmware Version**—displays the firmware version. ● **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. ● **Driver Version**—displays the driver version. ● **Patrol Read State**—displays the Patrol Read State. ● **Cache Size**—displays the cache size. ⓘ **NOTE:** This section displays the chipset controller information. This is not displayed in the storage controller section of iDRAC UI, but you can view this information about the inventory page of iDRAC.
Enclosures	● **Controller ID**—displays the controller ID. ● **Connector ID**—displays the connector ID. ● **Enclosure ID**—displays the enclosure ID. ● **Name**—displays the name of the enclosure. ● **Device FQDD**—displays the device FQDD. ● **Service Tag**—displays the service tag.

View firmware information of a single host

The following firmware-related information is displayed:

- **Name**—displays the name of all the firmware on this host.
- **Type**—displays the type of firmware.
- **Version**—displays the version of all the firmware on this host.
- **Installation Date**—displays the installation date.

ⓘ **NOTE:** When the hosts are managed using the chassis credential profile, the firmware inventory data show few extra components such as Life Cycle Controller and Software RAID.

You can launch firmware update and configure system lockdown mode wizards from this page.

View power monitoring information of a single host

You can view the information such as general information, thresholds, reserve power capacity, and energy statistics.

- **General Information**—displays the Power Budget and Current Profile name.
- **Threshold**—displays the Warning and Failure thresholds in watts.
- **Reserve Power Capacity**—displays the Instant and Peak reserve power capacity in watts.

Energy Statistics

- **Type**—displays the energy statistics type.
- **Measurement Start Time (Host Time)**—displays the date and time when the host began to consume power.
- **Measurement Finish Time (Host Time)**—displays the date and time when the host stopped to consume power.
- ⓘ **NOTE:** The host time, as used here, means the local time where the host is located.

  Reading—displays the average value of readings over a one-minute time period.
- **Peak Time (Host Time)**—displays the date and time of the host peak amps.
- **Peak Reading**—displays the System Peak Power statistic, which is the peak power that is consumed by the system (in watts).

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

ⓘ **NOTE:** For hosts managed using chassis, complete power monitoring information is not displayed.

View warranty information of a single host

To view a warranty status, ensure that you run a warranty job. See Schedule warranty retrieval jobs on page 99. 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.
- **Description**—displays a description.
- **Start Date**—displays the start date of the warranty.
- **End Date**—displays the end date of the warranty.
- **Days Left**—displays the days left on the warranty.
- **Last Updated**—the last time the warranty was updated.

View system event log information of a single host

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

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

  The severity levels are defined as:

  - Info
  - Warning
  - Error
- **Time (Server Time)**—Indicates the time and date when the event occurred.

To clear all the System Event Logs, click **CLEAR LOG**. A message is displayed indicating that the log data cannot be recovered after log has been cleared.

Monitor hosts on clusters and data centers

The OMIVV enables you to view detailed information about all hosts in a data center or cluster.

View OMIVV data center and cluster information

View overview of data center and cluster

You can view the information such as data center or cluster information, system lockdown mode, hardware resources, and warranty information. To view the information about this page, ensure that inventory is completed successfully. The OMIVV data center and cluster views directly report data from iDRAC.

1. On the OMIVV home page, expand **Menu**, and then select **Hosts and Clusters**.
2. In the left pane, select a data center or cluster, and then click **Monitor** > **OMIVV Cluster or Datacenter Information**.
3. To view more information, select a specific host.

   The information such as iDRAC IP, Chassis URL, CPUs, and Memory are displayed in the lower-most horizontal pane of the page.

Table 16. Overview of data centers and clusters

Information	Description
Datacenter/Cluster Information	Displays the following: ● Datacenter/cluster name ● Number of managed hosts ● Total energy consumption
System Lockdown Mode	Displays the status of the iDRAC Lockdown Mode. The iDRAC Lockdown Mode statuses of the total number of hosts are displayed as follows: ● Turned On ● Turned Off ● Not Applicable (Only for 14th generation servers)
Hardware Resources	Displays the following: ● Total Processors ● Total Memory ● Virtual Disk Capacity
Warranty Summary	Displays the warranty status for the selected host. The status options include: ● Expired warranty ● Active warranty ● Unknown warranty
Host	Displays the hostname
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 16. Overview of data centers and clusters (continued)

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. For all PowerEdge servers earlier than 14th generation, the System Lockdown Mode displayed as **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 modular 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
Host Credential Profile	Displays the name of the host credential profile
Remote Access Card Version	Displays the remote access card version
BIOS Firmware Version	Displays the BIOS firmware version

View hardware information of a data center and cluster

Table 17. Hardware information for data centers and clusters

Hardware: *Component*	Information
Hardware: FRU	● **Host**—displays the hostname. ● **Service Tag**—displays the service tag of the host. ● **Part Name**—displays the FRU part name. ● **Part Number**—displays the FRU part number. ● **Manufacturer**—displays the name of the manufacturer . ● **Serial Number**—displays the serial number of the manufacturer. ● **Manufacture Date**—displays the manufacture date.
Hardware: Processor	● **Host**—displays the hostname. ● **Service Tag**—displays the service tag of the host. ● **Socket**—displays the slot number. ● **Speed**—displays the current speed. ● **Brand**—displays the processor brand. ● **Version**—displays the processor version. ● **Cores**—displays the number of cores in this processor.
Hardware: Power Supply	● **Host**—displays the hostname. ● **Service Tag**—displays the service tag of the host. ● **Type**—displays the type of power supply. The power supply types include: ○ UNKNOWN ○ LINEAR ○ SWITCHING ○ BATTERY

Table 17. Hardware information for data centers and clusters (continued)

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

View storage information of a data center and cluster

Table 18. Storage details for a data center and cluster

Storage: disks	Description
Physical Disk	● **Host**—displays the hostname. ● **Service Tag**—displays the service tag of the host. ● **Capacity**—displays the physical disk capacity. ● **Disk Status**—displays physical disk status. The options include: ○ ONLINE ○ READY ○ DEGRADED ○ FAILED ○ OFFLINE ○ REBUILDING ○ INCOMPATIBLE ○ REMOVED ○ CLEARED ○ SMART ALERT DETECTION ○ UNKNOWN ○ FOREIGN ○ UNSUPPORTED **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` ● **Model Number**—displays the model number of the physical storage disk. ● **Last Inventory**—displays the day, month, and time of the last inventory that was run. ● **Status**—displays the host status. ● **Controller ID**—displays the controller ID. ● **Connector ID**—displays the connector ID. ● **Enclosure ID**—displays the enclosure ID. ● **Device ID**—displays the device ID. ● **Bus Protocol**—displays the bus protocol. ● **Remaining Rated Write Endurance**—displays the SSD remaining write endurance. ● **Hot Spare Type**(Not applicable for PCIe)—shows the hot spare type. The options include: ○ No—there is no hot spare. ○ Global—unused backup disk that is part of the disk group ○ Dedicated—unused backup disk that is assigned to a single virtual drive. When a physical disk in the virtual drive fails, the hot spare is enabled to replace the failed physical disk without interrupting the system or requiring your intervention ● **Part Number**—displays the storage part number. ● **Serial Number**—displays the storage serial number. ● **Vendor Name**—displays the storage vendor name.
Virtual Disk	● **Host**—displays the name of the host. ● **Service Tag**—displays the service tag of the host. ● **Name**—displays the name of the virtual drive. ● **Physical Disk**—displays on which physical disk the virtual drive is located. ● **Capacity**—displays the capacity of the virtual drive. ● **Layout**—displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual drive. ● **Last Inventory**—displays the day, date, and time the inventory was last run.

Table 18. Storage details for a data center and cluster (continued)

Storage: disks	Description
	- **Controller ID**—displays the controller ID. - **Device ID**—displays the device ID. - **Media Type**—displays either SSD or HDD. - **Bus Protocol**—displays the technology that the physical disks in the virtual drive are using. The possible values are: ○ SCSI ○ SAS ○ SATA ○ PCIe - **Stripe Size**—displays the stripe size, which provides the amount of space that each stripe consumes on a single disk. - Default Read Policy—displays the default read policy that is supported by the controller. The options include: ○ Read-Ahead ○ No-Read-Ahead ○ Adaptive Read-Ahead ○ Read Cache Enabled ○ Read Cache Disabled - **Default Write Policy**—displays the default write policy that is supported by the controller. The options include: ○ Write-Back ○ Force Write Back ○ Write Back Enabled ○ Write-Through ○ Write Cache Enabled Protected ○ Write Cache Disabled - **Disk Cache Policy**—displays the default cache policy that is supported by the controller. The options include: ○ Enabled—cache I/O ○ Disabled—direct I/O

View firmware information of a data center and cluster

The following information about each firmware component is displayed:

- **Host**—displays the name of the host.
- **Service Tag**—displays the service tag of the host.
- **Name**—displays the name of all the firmware on this host.
- **Version**—displays the version of all the firmware on this host.

View power monitoring information of a data center and cluster

- **Host**—displays the name of the host.
- **Service Tag**—displays the service tag of the host.
- **Current Profile**—displays power profile to maximize performance of your system and conserve energy.
- **Energy Consumption**—displays the energy consumption of the host.
- **Peak Reserve Capacity**—displays the peak power reserve capacity.
- **Power Budget**—displays the power cap for this host.
- **Warning Threshold**—displays your system's configure maximum value for temperature probe warning threshold.
- **Failure Threshold**—displays your system's configure maximum value for temperature probe failure threshold.
- **Instant Reserve Capacity**—displays the host instantaneous headroom capacity.
- **Energy Consumption Start Date**—displays the date and time when the host began to consume power
- **Energy Consumption End Date**—displays the date and time when the host stopped to consume power

- **System Peak Power**—displays the host peak power.
- **System Peak Power Start Date**—displays the date and time when the host peak power started
- **System Peak Power End Date**—displays the date and time when the host peak power ended
- **System Peak Amps**—displays the hosts peak amps.
- **System Peak Amps Start Date**—displays the starting date and time of the host peak amps.
- **System Peak Amps End Date**—displays the end date and time of the host peak amps.

NOTE: Time that is shown for Power Monitoring inventory of the hosts is incorrect when viewed from data center and cluster level. See the host level inventory for correct details.

View warranty information of a data center and cluster

To view a warranty status, ensure to run a warranty job. See Schedule warranty retrieval jobs on page 99. The **Warranty Summary** page lets you 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.

- **Warranty Summary**—the host warranty summary is displayed using icons to visually show the number of hosts in each status category.
- **Host**—displays the hostname.
- **Service Tag**—displays the service tag of the host.
- **Description**—displays a description.
- **Warranty Status**—displays the warranty status of the host. Status options include:
    - Active—the host is under warranty, and has not exceeded any threshold.
    - Warning—the host is Active, but exceeded the warning threshold.
    - Critical—same as warning, but for a critical threshold
    - Expired—the warranty has expired for this host.
    - 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.
- **Days Left**—displays the amount of days left for the warranty.

Firmware update

The OMIVV 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.

NOTE: In a multi-appliance environment, to perform firmware update on cluster or host, ensure that the appliance registered with target vCenter is loaded.

The following are the two methods to perform the firmware updates:

- Single DUP—performs firmware update for iDRAC and BIOS by pointing directly to the DUP location (either CIFS or NFS). The single DUP method can be used only at the host level.
- Repository Profiles—performs firmware and driver updates. The method can be used at both host level and cluster level.

    The following are the repository profiles that are used for firmware and driver updates:

    - Firmware Repository—A repository profile that uses firmware catalog to get the firmware information.

        The following are the two types of firmware repository:

        - User-created firmware repository
        - Factory-created firmware repository: The following are the two types of factory created catalogs: Factory-created catalogs are not applicable for vSAN cluster firmware update and baselining.
            - Dell Default Catalog: A factory-created firmware repository profile that uses the Dell EMC Online catalog to get the latest firmware information. If the appliance does not have an Internet connection, modify this repository to point to a local CIFS or NFS or HTTP or HTTPs based shares.
            - Validated MX Stack Catalog: A factory-created firmware repository profile that uses the Dell EMC online catalog to get the validated firmware information for MX chassis and its corresponding sleds.

    - Driver repository—A repository profile contains offline bundles that can be used to update the driver for vSAN clusters.

The Firmware Update Wizard always checks for the minimum firmware levels for iDRAC and BIOS 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 and BIOS. Once iDRAC and BIOS firmware versions meet the minimum requirements, the firmware update process enables updates for all firmware versions including iDRAC, RAID Controller, NIC, BIOS, and so on.

Related tasks

Update firmware and driver on vSAN host on page 122
Update firmware and driver on vSAN cluster on page 124
Update firmware on vSphere host on page 126
Update firmware on vSphere cluster on page 127

Update firmware and driver on vSAN host

Before scheduling the firmware update on vSAN hosts (hosts in vSAN enabled cluster), ensure that the following conditions are met in the environment:

- Ensure that host is compliant (CSIOR enabled and host must have supported ESXi version), associated with a host credential profile, and successfully inventoried.
- The following prerequisites are checked before scheduling the firmware update:
    - DRS is enabled.
    - Host is not already in maintenance mode.
    - vSAN data objects are healthy.

    To skip the prerequisites, clear the **Check Prerequisites** check box on the **Schedule Updates** page.
- For storage controller, HDD, and SSD components, the selected drivers and firmware versions in the selected repositories are compliant as per the VMware vSAN guidelines based on the vSAN version.
- For drivers, OMIVV supports only the offline bundles that are listed in the VMware Hardware Compatibility List.
- The cluster satisfies the vSAN requirements for the selected data migration option. If the vSAN cluster does not meet the requirements for the selected data migration option, the update times out.
- Dell EMC recommends selecting the baselined (Cluster Profile) firmware or driver repository.
- Ensure that there are no active firmware update jobs for any hosts under the cluster that you are updating.
- Ensure that you specify the required time out value for the "Enter maintenance mode" job. If the wait time goes beyond the specified time, the update job fails. However, the components may get updated automatically when the host is rebooted.
- Rerun the inventory after enabling vSAN.

During the firmware update process, Dell EMC recommends not to delete or move the following:

- The host from vCenter for which the firmware update job is in progress.
- The host credential profile of the host for which the firmware update job is in progress.
- The repositories that are located in CIFS or NFS.

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.

1. To launch the firmware update wizard, on the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, and then perform either of the following actions:
    - Right-click a host, select **OMIVV Host Actions** > **Firmware Update**.
    - Select a host, in the right pane, select **Monitor** > **OMIVV Host Information** > **Firmware** > **Run Firmware Wizard**.
    - Select a host, in the right pane, select **Summary**, and then go to **OMIVV Host Information** > **Host Actions** > **Run Firmware Wizard**.
2. On the **Firmware Update Checklist** page, ensure that all the prerequisites are verified before scheduling the update, and then click **GET STARTED**.
3. On the **Update Source** page, select any one of the following:
    - **Repository Profiles**
    - **Single DUP**
4. To load a single firmware update from a file, select **Single DUP**.

a. A single DUP can reside on a CIFS or NFS share that is accessible by the OMIVV appliance: Enter the file location in one of the following formats, and then go to step 9.

   - NFS—`<host>:/<share_path/FileName.exe`
   - CIFS—`\\<host accessible share path>\<FileName>.exe`

   NOTE: Ensure that the file name for the single component DUP does not have any blank space.

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

5. If you select the **Repository Profiles** option, select the firmware and driver repository profiles.

   If the cluster profile is associated to the cluster in which the host is present, by default, the associated firmware, and driver repository profiles are selected.

   If you change the firmware or driver repository profiles, a message is displayed indicating that the selected repository profile is not associated to baseline and using a different repository may affect the baseline comparison.

   NOTE: If you have both driver and firmware repositories are associated with the cluster profile, it is recommenced to update both driver and firmware simultaneously.

   If you do not want to update firmware or driver, or firmware or driver is up-to-date, from the drop-down menu, select **No Repository selected**.
6. Based on the firmware repository profile you have selected, select an appropriate bundle, and then click **NEXT**. Only 64-bit bundles are supported.
7. On the **Select Driver Components** page, select the driver components that require an update, and then click **NEXT**. When you select a driver component for update, all the components in the package are selected.

   You can use the filter option to filter the data based on the specific column names.
8. On the **Select Firmware Components** page, select the firmware components that require an update, and then click **NEXT**.

   The count of the components that is based on criticality status such as Urgent, Recommended, Optional, and Downgrades are displayed.

   The components which have lower version than the available version in the catalog, or it is in the same level (Up-to-Date), or scheduled for an update cannot be selected. To select the components which have lower version than the available version, select the **Allow Firmware downgrade** check box.

   To select all the firmware components across all the pages, click ☰.

   To clear all the firmware components across all the pages, click X.
9. On the **Schedule Updates** page, enter the firmware update job name and description. The description is an optional field.

   The firmware update job name is mandatory. If you purge the firmware update job name, you can reuse the job name again.
10. Under the **Additional Settings** section, do the following:

    a. Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or time out. However, the components may get updated automatically when the host is restarted.

    b. From the **Enter Maintenance Mode Option** drop-down menu, select an appropriate data migration option. For more information about the data migration option, see the VMware documentation.

    NOTE: Enter maintenance mode task fails if the cluster configuration does not support full data migration or the storage capacity is insufficient.

    By default, the following options are selected:

    - **Exit maintenance mode after firmware update completes**—If you disable this option, host remains in maintenance mode.
    - **Move powered-off and suspended virtual machines to other hosts in cluster**—Disabling this option disconnects VM until the host device is online.

    c. If you have issues while updating the firmware, select the **Delete Job Queue and Reset iDRAC** check box. 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.

    For hosts managed using chassis credential profile, delete job queue is not supported.

    By default, the **Check Prerequisites** option is selected.
11. Under the **Update Schedule** section, select any one of the following options:

    - **Update Now**

- **Schedule Update**
- **Apply Updates on Next Reboot**

12. On the **Review Summary** page, review the firmware update information, and then click **FINISH**.
    The firmware update jobs can take up to several hours depending on the components and number of servers selected. You can view the status of the jobs on the **Jobs** page.

    After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode that is based on an option that is selected in the **Schedule Updates** page.

Related information

Firmware update on page 121

Update firmware and driver on vSAN cluster

Before scheduling the firmware update, ensure that the following conditions are met in the environment:

- Ensure that host is compliant (CSIOR enabled and host must have supported ESXi version), associated with a host credential profile, and successfully inventoried. If the host is not listed, run the management compliance wizard for hosts from OMIVV and then use the firmware update wizard.
- The following prerequisites are checked before scheduling the firmware update:
  - DRS is enabled.
  - Host is not already in maintenance mode.
  - vSAN data objects are healthy.
- For storage controller, HDD, and SSD components, ensure that the selected drivers and firmware versions in the selected repositories are compliant as per the VMware vSAN guidelines based on the vSAN version.
- For drivers, OMIVV supports only the offline bundles that are listed in the VMware Hardware Compatibility List.
- The cluster satisfies the vSAN requirements for the selected data migration option. If the vSAN cluster does not meet the requirements for the selected data migration option, the update will time out.
- Dell EMC recommends selecting the baselined (Cluster Profile) Firmware or Driver repository.
- Ensure that there are no active firmware update jobs for any hosts under the cluster that you are updating.
- Ensure that you specify the required time out value for the "Enter maintenance mode" job. If the wait time goes beyond the specified time, the update job fails. However, the components may get updated automatically when the host is rebooted.
- Ensure that you rerun the inventory after enabling vSAN.

During the firmware update process, Dell EMC recommends not to delete or move the following:

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

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

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.

1. To launch the firmware update wizard, on the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, and then perform either of the following actions:
   - Right-click a cluster, select **OMIVV Cluster Actions** > **Firmware Update**.
   - Select a cluster, in the right pane, select **Monitor** > **OMIVV Cluster Information** > **Firmware** > **Run Firmware Wizard**.
2. On the **Firmware Update Checklist** page, ensure that all the prerequisites are verified before scheduling the update, and then click **GET STARTED**.
3. On the **Update Source** page, select the firmware and driver repository profiles.

   If the cluster profile is associated to the cluster in which the host is present, by default, the associated firmware, and driver repository profiles are selected.

   If you change the firmware or driver repository profiles, a message is displayed indicating that the selected repository profile is not associated to baseline and using a different repository may affect the baseline comparison.

   ⓘ **NOTE:** If you have both driver and firmware repositories are associated with the cluster profile, it is recommenced to update both driver and firmware simultaneously.

If you do not want to update firmware or driver, or firmware or driver is up-to-date, from the drop-down menu, select **No Repository selected**.

4. Based on the firmware repository profile you have selected, select an appropriate bundle, and then click **NEXT**. Only 64-bit bundles are supported.

   NOTE: Only one bundle can be selected for OEM (debranded) servers even if they are of different models. Even if the bundle is not applicable for one or more of the OEM servers, the components page of the firmware update wizard lists each OEM server or firmware component pair. If the firmware update fails for a given firmware component pair, retry with the alternate bundle displayed for the OEM server.

5. On the **Select Driver Components** page, select the driver components that require an update, and then click **NEXT**. When you select a driver component for update, all the components in the package are selected.

   You can use the filter option to filter the data based on the specific column names.

6. On the **Select Firmware Components** page, select the firmware components that require an update, and then click **NEXT**.

   The count of the components that is based on criticality status such as Urgent, Recommended, Optional, and Downgrades are displayed.

   You can use the filter option to filter the data based on the specific column names.

   The components which have lower version than the available version in the catalog, or it is in the same level (Up-to-Date), or scheduled for an update cannot be selected. To select the components which have lower version than the available version, select the **Allow Firmware downgrade** check box.

   To select all the firmware components across all the pages, click ☰.

   To clear all the firmware components across all the pages, click X.

7. On the **Schedule Updates** page, enter the firmware update job name and description. The description is an optional field.

   The firmware update job name is mandatory. If you purge the firmware update job name, you can reuse the job name again.

8. Under the **Additional Settings** section, do the following:

   a. Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is restarted.

   b. From the **Enter Maintenance Mode Option** drop-down menu, select an appropriate data migration option. For more information about the data migration option, see the VMware documentation.

      NOTE: Enter maintenance mode task fails if the cluster configuration does not support full data migration or the storage capacity is insufficient.

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

   c. If you have issues while updating the firmware, select the **Delete Job Queue and Reset iDRAC** check box. 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.

      For hosts managed using chassis credential profile, delete job queue is not supported.

9. Under the **Update Schedule** section, select any one of the following options:

   - **Update Now**
   - **Schedule Update**

10. On the **Review Summary** page, review the firmware update information, and then click **FINISH**.
    The firmware update jobs can take up to several hours depending on the components and number of servers selected. You can view the status of the jobs on the **Jobs** page.

    After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode that is based on an option that is selected in the **Schedule Updates** page.

Related information

Firmware update on page 121

Update firmware on vSphere host

Before scheduling the firmware update on vSphere hosts (ESXi only), ensure that the following conditions are met in the environment:

- Ensure that host is compliant (CSIOR enabled and host must have supported ESXi version), associated with a host credential profile, and successfully inventoried.
- The DRS is enabled.

  NOTE: For a stand host, the DRS check is not applicable.

  To skip the prerequisites check, clear the **Check Prerequisites** check box on the **Schedule Updates** page.

  NOTE: Driver update is not supported on vSphere cluster and host.

During the firmware update process, Dell EMC recommends not to delete or move the following:

- The host from vCenter for which the firmware update job is in progress.
- The host credential profile of the host for which the firmware update job is in progress.
- The repositories that are located in CIFS or NFS.

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.

1. To launch the firmware update wizard, on the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, and then perform either of the following actions:
   - Right-click a host, select **OMIVV Host Actions** > **Firmware Update**.
   - Select a host, in the right pane, select **Monitor** > **OMIVV Host Information** > **Firmware** > **Run Firmware Wizard**.
   - Select a host, in the right pane, select **Summary**, and then go to **OMIVV Host Information** > **Host Actions** > **Run Firmware Wizard**.
2. On the **Firmware Update Checklist** page, ensure that all the prerequisites are verified before scheduling the update, and then click **GET STARTED**.
3. On the **Update Source** page, select any one of the following:
   - **Repository Profiles**
   - **Single DUP**
4. To load a single firmware update from a file, select **Single DUP**.
   a. A single DUP can reside on a CIFS or NFS share that is accessible by the OMIVV appliance. Enter the File Location in one of the following formats, and then go to step 8.
      - NFS—`<host>:/<share_path/FileName.exe`
      - CIFS—`\\<host accessible share path>\<FileName>.exe`

      NOTE: Ensure that the file name for the single component DUP does not have any blank space.

      For CIFS share, OMIVV prompts you to enter the username and password that can access the share drive.
5. If you select the **Repository Profiles** option, select the firmware repository profile.

   If the cluster profile is associated to the cluster in which the host is present, by default, the associated firmware repository is selected. Else, **Dell Default Catalog** is selected.

   If you change the firmware repository profile, a message is displayed indicating that the selected repository profile is not associated to baseline and using a different repository may affect the baseline comparison.
6. Based on the firmware repository profile you have selected, select an appropriate bundle, and then click **NEXT**. Only 64-bit bundles are supported.
7. On the **Select Firmware Components** page, select the firmware components that require an update, and then click **NEXT**.

   The count of the components that is based on criticality status such as Urgent, Recommended, Optional, and Downgrades are displayed.

   You can use the filter option to filter the data based on the specific column names.

   The components which have lower version than the available version in the catalog, or it is in the same level (Up-to-Date), or scheduled for an update cannot be selected. To select the components which have lower version than the available version, select the **Allow Firmware downgrade** box.

   To select all the firmware components across all the pages, click ☰.

To clear all the firmware components across all the pages, click X.

8. On the **Schedule Updates** page, enter the firmware update job name and description. The description is an optional field.

   The firmware update job name is mandatory. If you purge the firmware update job name, you can reuse the job name again.
9. Under the **Additional Settings** section, do the following:
   a. Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is restarted.

      By default, the following options are selected:

      - **Exit maintenance mode after firmware update completes**—If you disable this option, host remains in maintenance mode.
      - **Move powered-off and suspended virtual machines to other hosts in cluster**—Disabling this option disconnects VM until the host device is online.

   b. If you have issues while updating the firmware, select the **Delete Job Queue and Reset iDRAC** check box. 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.

      For hosts managed using chassis credential profile, delete job queue is not supported.

      By default, the **Check Prerequisites** option is selected.
10. Under the **Update Schedule** section, select any one of the following options:
    - **Update Now**
    - **Schedule Update**
    - **Apply Updates on Next Reboot**
    - **Apply Updates, and Force Reboot without enetring Maintenance mode**
11. On the **Review Summary** page, review the firmware update information, and then click **FINISH**.
    The firmware update jobs can take up to several hours depending on the components and number of servers selected. You can view the status of the jobs on the **Jobs** page.

    After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode that is based on an option that is selected in the **Schedule Updates** page.

Related information

Firmware update on page 121

Update firmware on vSphere cluster

Before scheduling the firmware update, ensure that the following conditions are met in the environment:

- Ensure that host is compliant (CSIOR enabled and host must have supported ESXi version), associated with a host credential profile, and successfully inventoried. If the host is not listed, run the management compliance wizard for hosts from OMIVV and then use the firmware update wizard.
- The DRS is enabled.
- Ensure that there are no active firmware update jobs for any hosts under the cluster that you are updating.
- Ensure that you specify the required time out value for the "Enter maintenance mode" job. If the wait time goes beyond the specified time, the update job fails. However, the components may get updated automatically when the host is rebooted.

NOTE: Driver update is not supported on vSphere cluster and host.

During the firmware update process, Dell EMC recommends not to delete or move the following:

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

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

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.

1. To launch the firmware update wizard, on the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, and then perform either of the following actions:
   - Right-click a cluster, select **OMIVV Cluster Actions** > **Firmware Update**.
   - Select a cluster, in the right pane, select **Monitor** > **OMIVV Cluster Information** > **Firmware** > **Run Firmware Wizard**.
2. On the **Firmware Update Checklist** page, ensure that all the prerequisites are verified before scheduling the update, and then click **GET STARTED**.
3. On the **Update Source** page, If the cluster profile is associated to the cluster in which the host is present, by default, the associated firmware repository is selected. Else, **Dell Default Catalog** is selected.

   If you change the firmware repository profile, a message is displayed indicating that the selected repository profile is not associated to baseline and using a different repository may affect the baseline comparison.
4. Based on the firmware repository profile you have selected, select an appropriate bundle, and then click **NEXT**. Only 64-bit bundles are supported.

   > **NOTE:** Only one bundle can be selected for OEM (debranded) servers even if they are of different models. Even if the bundle is not applicable for one or more of the OEM servers, the components page of the firmware update wizard lists each OEM server or firmware component pair. If the firmware update fails for a given firmware component pair, retry with the alternate bundle displayed for the OEM server.
5. On the **Select Firmware Components** page, select the firmware components that require an update, and then click **NEXT**.

   The count of the components that is based on criticality status such as Urgent, Recommended, Optional, and Downgrades are displayed.

   The components which have lower version than the available version in the catalog, or it is in the same level (Up-to-Date), or scheduled for an update cannot be selected. To select the components which have lower version than the available version, select the **Allow Firmware downgrade** check box.

   You can use the filter option to filter the data based on the specific column names.

   To select all the firmware components across all the pages, click ✓☰.

   To clear all the firmware components across all the pages, click ✕.
6. On the **Schedule Updates** page, enter the firmware update job name and description. The description is an optional field.

   The firmware update job name is mandatory. If you purge the firmware update job name, you can reuse the job name again.
7. Under the **Additional Settings** section, do the following:
   a. Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is restarted.

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

   b. If you have issues while updating the firmware, select the **Delete Job Queue and Reset iDRAC** check box. 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.

      For hosts managed using chassis credential profile, delete job queue is not supported.
8. Under the **Update Schedule** section, select any one of the following options:
   - **Update Now**
   - **Schedule Update**
9. On the **Review Summary** page, review the firmware update information, and then click **FINISH**.
   The firmware update jobs can take up to several hours depending on the components and number of servers selected. You can view the status of the jobs on the **Jobs** page.

   After firmware update task is complete, the inventory runs automatically on the selected hosts and hosts exit automatically from maintenance mode that is based on an option that is selected in the **Schedule Updates** page.

Related information

Firmware update on page 121

Update same firmware component type

The following are the key points to remember when updating firmware components of same type:

- If multiple components of the same type with same versions are present in the server, only one version of the component is displayed on the **Select Firmware Components** page. The update will be applied to all the components and the drift details are displayed for only one version of the component.

  For example,

  ### Table 19. Example for multiple components with same type present in server

Component	Current version	Available version
HDD1	V1	V3
HDD2	V1	V3
HDD3	V1	V3

  In this case, the **Select Firmware Components** page displays the following:

  ### Table 20. Example for multiple components of the same version present in server

Component	Current version	Available version
HDD1	V1	V3

- If multiple components of the same type with different versions are present in the server, a single component will be displayed for each unique version. In this case, if you select any one component, the update will be applied to all the components irrespective of their current firmware versions. The drift details are displayed for all the components irrespective of their current firmware versions.

  For example,

  ### Table 21. Example for multiple components with different version present in server

Component	Current version	Available version
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3

  In this case, the **Select Firmware Components** page displays the following:

  ### Table 22. Example for multiple components with different version present in server

Component	Current version	Available version
HDD1	V1	V3
HDD2	V2	V3

- If the catalog contains multiple available versions, it is recommended to select only one of the available version for a component type. The selected firmware is then applied to all applicable components irrespective of their current version.

  For example,

  ### Table 23. Example for multiple available version present in catalog

Component	Current version	Available version
HDD1	V1	V3
HDD2	V2	V3
HDD3	V2	V3
HDD1	V1	V4
HDD2	V2	V4

Table 23. Example for multiple available version present in catalog (continued)

Component	Current version	Available version
HDD3	V2	V4

In this case, the **Select Firmware Components** page displays the following:

Table 24. Example for multiple available version present in catalog

Component	Current version	Available version
HDD1	V1	V3
HDD2	V2	V3
HDD1	V1	V4
HDD2	V2	V4

Set up 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. To launch the **Blink Server LED Indicator** wizard, perform either of the following actions:
   a. On the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, right-click a host or cluster, and then go to **Summary** > **OMIVV Host Information** > **Host Actions** > **Blink Server LED Indicator**.
   b. Right-click a host, go to **All OpenManage Integration Actions** > **Blink Server LED Indicator**.
2. In the right pane, click Summary, and then go to **OMIVV Host Information** > **Hosts Action** > **Blink Server LED Indicator.**
   The **Blink Server LED Indicator** dialog box is displayed.
3. Select any one of the following:
   a. To turn on the server LED indicator and set the time period, click **On**.
   b. To turn off the server LED indicator, click **Off**.

Configure System Lockdown Mode

The System Lockdown Mode setting is available in iDRAC for 14th generation PowerEdge servers with an Enterprise license. When you turn on the System Lockdown Mode, lock the system configuration including firmware updates. The System Lockdown Mode 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 using chassis credential 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 has limitations:

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

1. To launch the Configure System Lockdown Mode wizard, perform either of the following actions:
   a. On the OMIVV home page, expand **Menu**, select **Hosts and Clusters**, right-click a host or cluster, and then go to **Summary** > **OMIVV Host Information** > **Host Actions** > **Configure System Lockdown Mode**.
   b. Right-click a host or cluster, go to **All OpenManage Integration Actions** > **Configure System Lockdown Mode**.
   c. Select a host or cluster, got to **Monitor** > **OMIVV Host or Cluster Information** > **Firmware** > **Configure System Lockdown Mode**.
2. For cluster level, enter the System Lockdown Mode job name and description. The description is an optional field.
3. To enable the System Lockdown Mode, click **Turn On**. This option restricts changes to the System configurations (including firmware and BIOS version) in the system.

4. To disable the System Lockdown Mode, click **Turn Off**. This option enables changes to the System configurations (including firmware and BIOS version) in the system.

   If you try to configure the System Lockdown Mode for 13th and earlier generation of PowerEdge servers, you are prompted with a message that this feature is not supported on this platform.
5. Click **OK**.
   A job is successfully created for the configuring System Lockdown Mode. To check the job status, go to **Jobs** > **System Lockdown Mode**. For more information about System Lockdown Mode job, see System Lockdown Mode jobs on page 73.

16

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.

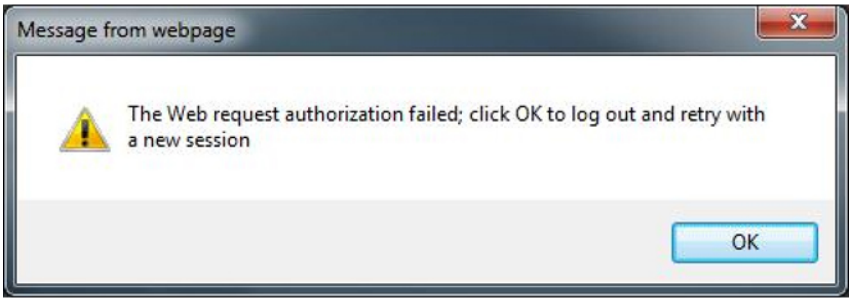
By default, users in the Administrators group have all the privileges. The Administrators can use all the functions of the OpenManage Integration for VMware vCenter within VMware vSphere web client. If you want a user with necessary privileges to manage the product, do the following:

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.

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 certificate of the vCenter server 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 1. 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 25. 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 that are 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 that is 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

17

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 151

Frequently Asked Questions-FAQ

This section contains some common questions and solutions.

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 and later

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 and later

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 go to **Troubleshooting Options**.
3. In **Troubleshooting Options**, go 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 Create host credential profile on page 35 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 and later

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. For more information, see 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.

Version Affected: 3.0 and later, vCenter 6.0 and later

Replacing the certificates on vCenter Windows installation

For more information, see https://kb.vmware.com/s/article/2121689.

Replacing the certificates on the vCenter server appliance

For more information, see https://kb.vmware.com/s/article/2121689.

Retrieving the old certificate from Managed Object Browser-MOB

For more information, see https://kb.vmware.com/s/article/2121701.

Extracting thumbprint from the old certificate

For more information, see https://kb.vmware.com/s/article/2121701.

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.

What should I do when a web communication error in the vCenter HTML-5 Client opens after changing the DNS settings in OMIVV

If you see any kind of web communication error in the vCenter HTML-5 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.

Installation date be displays as 12-31-1969 for some of the firmware on the firmware page

In web client, the installation date be displays 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

I am not seeing OpenManage Integration icon in HTML-5 Client even if registration of plug-in to vCenter was successful

OpenManage Integration icon is not displayed in the vSphere client unless the vSphere client services are restarted. When you register the OpenManage Integration for VMware vCenter appliance, the appliance is registered with the vSphere 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 be display in the vSphere Client. This is due to a caching issue from VMware. To clear the issue, ensure that you restart the Sphere Client service on the vCenter Server. Then the plug-in is displayed in the UI.

Resolution: Restart the vSphere client services on the vCenter server.

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

Running firmware update may display an error message, The firmware repository file does not exist or is invalid.

While running the Firmware Update wizard, at cluster level, an error message may be displayed: **The firmware repository file does not exist or is invalid**. This may be due to a daily background process that was unable to download and cache the catalog file from the repository. This occurs if the catalog file is not reachable at the time the background process runs.

Resolution: After resolving any catalog connectivity issues that may exist, you can reinitiate the background process by changing the firmware repository location, and then setting it back to the original location. Allow about five minutes for the background process to complete. Ensure that there is no @ character present in the credential that is provided for the CIFS. Also, ensure that the DUP file exists in the share location.

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 EMC PowerEdge 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 iDRAC with 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:** 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 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, see the User's Guide for Dell EMC 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 EMC 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

Use the following port settings for OMIVV:

Table 26. 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.
80/443	HTTP/ HTTPS	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 operating system deployment flow for post installation scripts to communicate with the OMIVV appliance.
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 vSphere Client and Dell Admin portal.
443	WSMAN	TCP	128-bit	In/Out	OMIVV appliance to or from iDRAC	iDRAC communication	iDRAC and CMC or OME-Modular 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.

Table 26. Virtual appliance (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
4433	HTTPS	TCP	128-bit	In	iDRAC to OMIVV appliance	Auto Discovery	Provisioning server that is 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 operating system deployment flows.
4001 to 4004	NFS	UDP/ TCP	None	In/Out	OMIVV appliance to NFS	Public Share	These ports must be kept open to run the statd, quotd, lockd, and mountd services by the V2 and V3 protocols of the NFS server.
11620	SNMP Agent	UDP	None	In	iDRAC to OMIVV appliance	SNMP Agent (server)	Port used to receive the standard SNMP alerts by using UDP: 162. Data from iDRAC and CMC or OME-Modular are received 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 27. 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 that are sent from ESXi. This port have to open from ESXi.
443	WSMAN	TCP	128-bit	In	OMIVV appliance to ESXi	iDRAC 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.

Table 28. Managed nodes (iDRAC or CMC or OME-Modular)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
443	WSMAN /HTTPS, REST/ HTTPS	TCP	128-bit	In	OMIVV appliance to iDRAC or CMC or OME-Modular	iDRAC communication	Used to provide information to the management station and communicate to MX chassis by using REST or HTTPS protocols. This port has to open from iDRAC and CMC or OME-Modular.
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

Table 28. Managed nodes (iDRAC or CMC or OME-Modular) (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
							appliance. That is used for operating system deployment and firmware update. To access the iDRAC configurations from the OMIVV. Used in deployment flow.
4001 to 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 operating system deployment and firmware update. 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 system profile that has same user with new changed credentials in iDRAC user list

The password of the user who is used from discovery is not changed to the new credential if only System Profile (Configuration of the hardware) is selected for deployment. This is done intentionally so that the plug-in can 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.

Can OMIVV support ESXi with lockdown mode enabled

Yes, lockdown mode is supported in this Release on hosts ESXi 6.0 and later.

When I tried to use lockdown mode, it fails

When I added a host to the host credential 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.

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 accessible by the virtual appliance.
3. Ensure that you select the management NICs based on the network connectivity to the OMIVV.
4. 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.
5. Ensure that at least one Virtual Disk, or IDSDM, or BOSS is seen by the system.

Auto discovered systems are displayed without model information in Deployment wizard

This usually indicates that the firmware version that is 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 can 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 OMIVV 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. Click **Home** > **Content** > **HealthUpdateManager**.
8. Click **QueryProviderList** > **Invoke method**.
9. Copy the provider ID string value and close the window.
10. Click **UnregisterHealthUpdateProvider** and enter the copied provider ID string value.
11. Click **Invoke Method**.
12. In the vSphere Client, turn off OMIVV and delete it. The key to unregister must be for the vSphere 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. Scroll down the page to enter the encryption password.

What should I do as firmware update failed

Check the OMIVV 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, 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 that you entered.

Performance during host credential 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:
   - iDRAC7: Select **iDRAC settings** > **Users tab**.
   - iDRAC8: Select **iDRAC settings** > **Users tab**.
   - iDRAC9: Select **iDRAC settings** > **Users tab**.

   For iDRAC 7 and 8:

   a. To edit the settings, in the User ID column, click the link for the admin (root) user.
   b. Click **Configure User**, and then click **Next**.
   c. In the **User Configuration** page for the selected user, select the check box next to Enable user, and then click **Apply**.

   For iDRAC9:

   a. Select the **root** user and click **Enable**.

Does OMIVV support VMware vCenter server appliance

Yes, OMIVV supports the VMware vCenter Server appliance since v2.1.

A server may show as non-compliant with CSIOR status, "Unknown"

Resolution: An unknown CSIOR state indicates a non-responsive iDRAC on the host. A manual iDRAC reset on the host fixes this issue.

Version Affected: All

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. Even if the host is removed from the vCenter tree, the host is displayed under the chassis until the next chassis inventory is run.

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 OMIVV GUI, in the **Settings** tab, manually change the **Events and Alarms** settings.

OS deployment fails when NPAR is enabled on a target node and disabled in System Profile

OS 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 using System Profile during deployment, ensure that you select only the first partition for management network in the deployment wizard.

Version Affected: 4.1 and later

Available OMIVV 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 and later bare-metal server

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 deployment, system profile apply fails due to iDRAC error

During deployment, OMIVV attempts to create configuration update job in iDRAC. However, the job creation may fail sometimes and displays a message indicating that a Configuration job is already created.

Resolution: Clear the stale entries and retry the deployment. Log in to iDRAC to clear the jobs.

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 have 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 that are created from one modular server cannot be applied on other modular servers in the same FX chassis because of NIC level restrictions.

Version Affected: 4.1 and later.

Resolution: System profile that is 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.

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 and later

When creating a host credential 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 and later

Dell EMC 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 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

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

After registration of vCenter, the Dell EMC logo of OMIVV is not displayed on the home page of VMware

Description: The Dell EMC logo of OMIVV may not be displayed on the **Home** page of VMware because soon after completion of registration, VMware vCenter will be validating the plugin.

Resolution: Perform the following:

1. Refresh the browser, or clear the browser cache, or restart the client services for vSphere Client (HTML-5).
2. Log out from vSphere WebClient and then log in again.

Version Affected: 5.0

Non-compliant 11G PowerEdge servers are retained in OMIVV inventory after backup and restore

After performing the backup and restore operation in OMIVV, the non-compliant and non-inventoried 11G hosts are still associated to the Host Credential Profile. However, if you try to fix the configuration compliance and run a fresh inventory, the job fails on the unsupported 11G servers.

Resolution: 11G servers are not supported with OMIVV 5.0. Manually remove the unsupported 11G hosts from the host credential profile.

Version Affected: 5.0

Unable to launch vCenter from flex client after upgrading the OMIVV appliance

Resolution: See VMware KB article for resolution: https://kb.vmware.com/s/article/54751.

Version affected: 5.0

When adding or removing network adapters to OMIVV, the existing NICs disappear from the OMIVV console

Sometimes, when you add or remove a network adapter to the OMIVV appliance by using the vSphere WebClient, the existing NICs disappear from the OMIVV console.

Workaround: Perform any one of the following tasks:

1. a. Remove all the work adapters from the terminal console utility.
   b. Shut down the appliance
   c. Remove the network adapters from the appliance.
   d. Reboot the OMIVV appliance.
   e. Shut down the appliance
   f. Add the required network adapter (s) and complete the network adapters configuration.

g. Reboot the appliance.

2. a. Back up OMIVV from Admin Portal

   b. Create an OMIVV appliance.

   c. Shut down the appliance

   d. Add the required network adapter (s) and complete the network adapters configuration.

   e. Reboot the appliance.

   f. Restore the latest backed up data.

Version Affected: OMIVV 5.0

After adding or removing the second NIC, the Network Configuration page shows three NICs

After you add or remove a NIC from the OMIVV appliance using the vSphere client, once you boot the OMIVV appliance and log in to the OMIVV terminal console, sometimes the **Network Configuration** page shows inconsistent number of NICs.

Resolution: Use the MAC address to compare and configure the correct NIC and use the **–** button to remove the extra NICs.

Version Affected: 5.0

A server with Unknown status in the earlier version is not listed on the Bare-metal Servers page after backing up and restoring to a latest OMIVV version

After restoring a backup from earlier versions, unsupported servers (11G and earlier) are removed from the bare-metal inventory. Servers whose generation has not been determined by the earlier version before the backup will also be removed.

Resolution: Rediscover the server. If the missing server is supported, then it is listed in the bare-metal inventory.

Version Affected: 5.0

After OS deployment, OMIVV failed to add ESXi host to vCenter or failed to add Host Profile or Enter Maintenance Mode is failed for host

After OS deployment, OMIVV queries vCenter to perform the host actions (Add host, Add Host Profile, or Enter Maintenance Mode). If the query does not receive a response within two minutes, the specific action on vCenter is timed out, and a message is displayed in the task history indicating that the communication failure. However, at times, the vCenter query operations are successful.

Resolution: Take the host IP from the task history and add manually.

When performing backup and restore, error message displayed is not informative in admin portal if the invalid username is entered

When the username entered during backup and restore has special characters (@, %) appended at the beginning, the authentication fails with a message that is not informative.

Workaround: Retry with the correct username and password.

Version affected: 4.1 and later.

iDRAC license status is displayed as compliant on the management compliance page when the iDRAC IP is not reachable

After performing periodic inventory, if iDRAC not reachable, iDRAC License status is displayed as compliant on the management compliance page.

Resolution: Ensure that the iDRAC is reachable and run the inventory again to get the right iDRAC license details.

ESXi host is either disconnected or not responding state after successful OS deployment using OMIVV.

ESXi host fails to send heartbeat packets to vCenter because its DNS is not properly configured to lookup FQDN of the vCenter.

Resolution: Perform the following tasks:

1. Remove the ESXi host from the vCenter inventory.
2. Add the host in vCenter using the **Add host** wizard.
3. Create a host credential profile and run the inventory.

Deployment job times out when network interface card (NIC) of OMIVV is not connected to the ESXi host network

OS deployment has dependency on the selection of NIC. If the correct NIC is not selected, then OSD job times out.

Resolution: Select appropriate 'Appliance NIC connected to Host ' from Configure Host Settings page of Deployment wizard . This is needed by OMIVV to reach ESXi network during OS installation process.

Warranty job is not running for certain hosts

In a PSC environment with multiple vCenters, if you add a host using FQDN to one vCenter and IP to another vCenter, warranty job runs only for one host instance.

Resolution: Remove the disconnected host instance from the host credential profile and run the inventory and warranty job.

Version Affected: 5.0

Management compliance page shows that incorrect credential profile name for hosts managed using chassis credential profile

For hosts managed using chassis credential profile, the management compliance shows incorrect credential profile name instead of actual chassis credential profile name.

Resolution: There is no impact on any OMIVV functionality.

Version Affected: 5.0

Proactive HA initialization is not happening after performing backup and restore

When you restore OMIVV from the previous version that is registered with the vSphere Client, for Proactive HA enabled clusters the Dell Provider is disconnected.

Resolution: Disable and enable the Proactive HA for clusters.

Version Affected: 5.0

OMIVV page displays invalid session, or time out exception, or two million errors in Firefox browser

If the OMIVV page is idle for some time (5–10 minutes), the invalid session, or time out exception, or two million errors is displayed.

Resolution: Refresh the browser. `If the issue persists, log out and log in from vCenter.`

To see the correct data in OMIVV, ensure that you complete the task listed in resolution.

Version Affected: 5.0

The System profile configuration preview task fails for iDRAC new user addition

When you try to enable a new iDRAC user and perform configuration preview, preview result shows **Failure**.

Resolution: If you proceed with deployment, user gets added successfully even if it shows failure in the preview.

Version Affected: 5.0

Attribute is not applied after successful system profile RAID deployment

Changes to *RAIDccMode* and *RAIDinitOperation* values are not deployed on the target server though the deployment is successful.

Resolution: Use the iDRAC setup to apply the values.

Version Affected: 5.0

OMIVV lists the virtual IP of the lead when you try to add the member chassis in chassis credential profile

When the virtual IP is configured for MX chassis and if you try to add one of the member chassis to OMIVV, the virtual IP is displayed in chassis credential profile instead of the physical IP of the lead chassis.

Resolution: Perform the following:

1. Log in to the MX chassis.
2. Get the physical IP of the lead chassis.
3. Add the physical IP of the lead chassis to OMIVV using the **ADD MX CHASSIS** option.

Version Affected: 5.0

Chassis inventory fails in OMIVV after promoting backup lead as a lead

When the lead chassis of the MCM group is powered off or not functional, the backup lead gets promoted as the lead chassis. In this case, inventory of the lead and member chassis fails in OMIVV.

Resolution: Perform the following:

1. Make the previous lead chassis active and run the inventory from OMIVV.
2. Delete the chassis credential profile and all the chassis present in the group from OMIVV.
3. Add the new lead chassis to rediscover the group.

Version Affected: 5.0

In vCenter, recent tasks pane does not show the details column for some OMIVV task notifications

Resolution: To see the task notifications, in vCenter, go to **Task Console** of vCenter.

Version Affected: 5.0

Unable to see the failure details in OMIVV logs for failed MX chassis firmware update job

Resolution: Log in to OME-Modular and check the firmware update job status.

If the status shows **Success** in OME-Modular, OMIVV updates firmware details in the next chassis inventory.

Version Affected: 5.0

Host firmware update fails, if a canceled firmware update job of related chassis is present

If you cancel the firmware update job of a PowerEdge MX chassis, subsequent host firmware update job for hosts present in the same chassis is blocked.

Resolution: Purge the canceled chassis firmware update job to release the lock on the related hosts.

On the configuration preview page of the deployment wizard, an error message is displayed

If you clear the target server after performing the configuration preview operation, an error message is displayed—*You must select server for deployment*.

Resolution: Select the target on the configuration preview page to complete the wizard. Selection that is done on this page does not override the target that is selected on the **Select Server (s)** page.

Version Affected: 5.0

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
   ```

A

System specific attributes

iDRAC

Table 29. 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
Address	IPv4 Address	IPv4 Static Information
Net Mask	Net Mask	IPv4 Static Information
Gateway	Gateway	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 30. 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
IscsiDev1Con1TargetIp	Target IP Address	Connection 1 Settings

Table 30. System specific attributes for BIOS (continued)

Attribute Name	Display Attribute Name	Group Display Name
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 31. 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 32. 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
IscsiInitiatorChapPwd	CHAP Secret	iSCSI Initiator Parameters

Table 32. System specific attributes for CNA (continued)

Attribute Name	Display Attribute Name	Group Display Name
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 33. 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

B

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*

C

Customization attributes

Table 34. 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 Password	Only iDRAC enabled users will have " Password " link to enter the password.
PCIeSSD	PCIeSSDSecureErase	Always Disabled

D

Component vs. baseline version comparison matrix

Table 35. 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 attributes of the 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 is available in the associated baseline but the component or attribute is not available in host.	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 version matches with the associated baseline.	Compliant
	Available	Available	Firmware component version not matches with the associated baseline.	Non-compliant
	Not Available	Available	Firmware component version is not available in the associated baseline but the component is available in host. The comparison status is not calculated and ignored.	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 version matches with the associated baseline.	Compliant
	Available	Available	Driver component version not matches with the associated baseline.	Non-compliant

Table 35. Component vs. baseline version comparison matrix (continued)

Drift Type				
	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 is available in host.	Non-compliant
	Not available	Not available	The comparison status is not calculated and ignored.	Compliant