OpenManage Integration for VMware vCenter for Web Client

User's Guide Version 3.2

April 2017
Rev. A00

DELL EMC

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

NOTE: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction

VMware vCenter is the primary console used by IT administrators to manage and monitor VMware vSphere ESX/ESXi hosts. In a standard virtualized environment, VMware alerts and monitoring are used to prompt you to launch a separate console to resolve hardware issues. OpenManage Integration for VMware vCenter is a product that lets you manage VMware vCenter servers from within the VMware Web client and free you from being tied to a Windows system. Using OpenManage Integration for VMware vCenter, you have capabilities to manage and monitor Dell hardware within the virtualized environment, such as:

- Alerts and environmental monitoring: Detect key hardware faults and perform virtualization-aware actions (for example, migrate workloads or place host in maintenance mode).
- Single server monitoring and reporting: Monitoring and reporting capabilities of servers.
- Firmware updates: Update Dell hardware to the most recent version of BIOS and firmware.
- Enhanced deployment options: Create hardware profiles, hypervisor profiles, and deploy any combination of the two on bare-metal Dell PowerEdge servers, remotely and without PXE—using vCenter

Topics:

OpenManage Integration for VMware vCenter Features

You can use the OpenManage Integration for VMware vCenter to perform:

Inventory	Inventory key assets, perform configuration tasks, and provide cluster and datacenter views of Dell platforms.
Monitoring and Alerting	Detect key hardware faults and perform virtualization-aware actions (for example, migrate workloads or place host in maintenance mode). Provide additional intelligence (inventory, events, alarms) to diagnose server problems. Report at the datacenter and cluster view and export to CSV file.
Firmware Updates	Update Dell hardware to the most recent version of BIOS and firmware.
Deployment and Provisioning	Create hardware profiles, hypervisor profiles, and remotely deploy any combination of the two on bare-metal Dell PowerEdge servers using VMware vCenter, without using PXE.
Service Information	Retrieve warranty information from Dell online.
Security Role and Permissions	Integrate with standard vCenter authentication, rules, and permissions.

What's new in this release

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

- Support for Dell OpenManage Server Administrator (OMSA) version 8.5
- Support for VMware vCenter server version 6.0 U3
- Support for VMware ESXi version 6.0 U3
- Support for PowerEdge R830 platform
- Support for Non-Uniform Memory Access (NUMA) Fault Resilient Memory (FRM)

NOTE: The Auto discovery feature is not functional in this release. For more details about this, see OMIVV cannot act as a provisioning server during the auto discovery process on page 109

2

Understanding How to Configure or Edit the OpenManage Integration for VMware vCenter

After you complete the basic installation of the OMIVV, the **Initial Configuration Wizard** is displayed when you click the OMIVV icon. Use the **Initial Configuration Wizard** to configure the **Settings** on first launch. For subsequent instances use the **Settings** page. From the **Initial Configuration Wizard** you can create a connection profile, edit the settings of warranty, inventory, events and alarms. Although, using the **Initial Configuration Wizard** is the most common method used, you can also accomplish this task through the appliance's **OpenManage Integration → Manage → Settings** page in the OMIVV. For more information on the Initial Configuration Wizard, see, *OpenManage Integration for VMware vCenter User Guide* available at `dell.com/support/manuals`.

Configuration Tasks Using the Configuration Wizard

The **Initial Configuration Wizard** can be used to configure the following for one vCenter or for all registered vCenters:

NOTE: If you view a web communication error in the vCenter Web client while performing OMIVV related tasks after changing the DNS settings, perform the following:

- Clear the browser cache.
- Logout and login from the Web client.

1. vCenter Selection
2. Creating A New Connection Profile
3. Scheduling Inventory Jobs
4. Running A Warranty Retrieval Job
5. Configuring Events And Alarms

NOTE: You can also launch the Initial Configuration Wizard using the link **Start Initial Configuration Wizard** under **Basic Tasks** in the **Getting Started** page.

Topics:

Configuration Wizard Welcome Page

After you install the OMIVV, it must be configured.

1. In the **vSphere Web Client**, click **Home**, and then click **OpenManage Integration** Icon.
2. The first time you click the **OpenManage Integration** icon, it opens the **Configuration Wizard**. You can also access this wizard on the **OpenManage Integration** > **Getting Started** > **Start Initial Configuration Wizard** page.

vCenter Selection

Using the **vCenter Selection** page you can configure:

- A specific vCenter

- All available vCenters

1. In the **Initial Configuration Wizard**, click **Next** in the **Welcome** screen.
2. Select one vCenter or all vCenters from the **vCenters** drop-down list.

   Select an individual vCenter for those not configured yet or if you have added a new vCenter to your environment. The vCenter selection page allows you to select one or more vCenters to configure settings.
3. Click **Next** to proceed to the **Connection Profile** description page.

   NOTE: If you have multiple vCenter servers as a part of the same SSO and if you chose to configure a single vCenter server, the following steps must be repeated until you configure each vCenter.

Creating A New Connection Profile using the Initial Configuration Wizard

A connection profile stores the iDRAC and host credentials that the virtual appliance uses to communicate with Dell servers. Each Dell server must be associated with a connection profile to be managed by the OMIVV. You may assign multiple servers to a single connection profile. You can create the Connection Profile using the Configuration Wizard or from **OpenManage Integration for VMware vCenter** > **Settings**.

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

NOTE: Before using the Active Directory credentials with a connection profile, the Active Directory user's account must exist in Active Directory and the iDRAC and host must be configured for Active Directory based authentication.

NOTE: The Active Directory credential can be same for both iDRAC and the host or it can be set as separate active directory credentials. The user credential must have administrative privileges.

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

To create a new connection profile using the Configuration Wizard:

1. In the **Connection Profile Description** page, click **Next**.
2. In the **Name and Credentials** page, enter the **Connection Profile Name** and an optional **Connection Profile Description**.
3. In the **Name and Credentials** page, under **iDRAC Credentials**, do one of the following:

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

   - For iDRACs already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory**; otherwise skip down to configure the iDRAC credentials.
     - In **Active Directory User Name**, type the user name. Type the **username** in one of these formats: **domain/username** or **username@domain**. The user name is limited to 256 characters. See Microsoft Active Directory documentation for user name restrictions.
     - In **Active Directory Password**, type the password. The password is limited to 127 characters.
     - In **Verify Password**, type the password again.
     - Perform one of the following actions:
       - To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**.
       - To not store and perform the iDRAC certificate checking during all future connections, clear **Enable Certificate Check**.
   - To configure iDRAC credentials without Active Directory, do the following:
     - In **User Name**, type the user name. The user name is limited to 16 characters. See the iDRAC documentation for information about user name restrictions for your version of iDRAC.
     - In **Password**, type the password. The password is limited to 20 characters.
     - In **Verify Password**, type the password again.

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

4. In the **Host Root** area, do one of the following:
   - For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select **Use Active Directory** ; otherwise configure your **Host Credentials**.
     - In **Active Directory User Name**, type the user name. Type the **username** in one of these formats: **domain/username** or **username@domain**. The user name is limited to 256 characters.

       For host user name and domain restrictions, refer to the following:

       Host Username Requirements:
       a. Between 1 and 64 characters long
       b. No non-printable characters
       c. Invalid characters: " / \ [ ] : ; | = , + * ? < > @

       Host Domain Requirements:
       a. Between 1 and 64 characters long
       b. First character must be alphabetical
       c. Cannot contain a space
       d. Invalid characters: " / \ : | , * ? < > ~ ! @ # $ % ^ & ' ( ) { } _
     - In **Active Directory Password**, type the password. The password is limited to 127 characters.
     - In **Verify Password**, type the password again.
     - Perform one of the following actions:
       - To download and store the Host certificate and validate it during all future connections, select **Enable Certificate Check**.
       - To not store and perform the Host certificate check during all future connections, clear **Enable Certificate Check**.
   - To configure Host Credentials without Active Directory, do the following:
     - In **User Name**, the user name is root. This is the default **username** and you cannot change the username. However, if the Active directory is set, you can choose any Active directory user and not just root.
     - In **Password**, type the password. The password is limited to 127 characters.

       NOTE: The OMSA credentials are the same credentials used for ESXi hosts.
     - In **Verify Password**, type the password again.
     - Perform one of the following actions:
       - To download and store the Host certificate and validate it during all future connections, select **Enable Certificate Check**.
       - To not store and perform the Host certificate check during all future connections, clear **Enable Certificate Check**.

5. Click **Next**.
6. In the **Associated Hosts** page, select the hosts for the connection profile and click **OK**.
7. To test the connection profile, select one or more hosts and click **Test Connection**.

   NOTE: This step is optional. This is used to check whether the Host and iDRAC credentials are correct or not.

8. To complete the profile, click **Next**.

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

Scheduling Inventory Jobs [Wizard]

You can configure inventory schedule using the Configuration Wizard or OpenManage Integration under **OpenManage Integration** > **Manage** > **Settings**.

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

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

To schedule an inventory job:

1. In the **Configuration Wizard**, in the **Inventory Schedule** window, select **Enable Inventory Data Retrieval** if it is not enabled.

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

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

Running A Warranty Retrieval Job [Wizard]

The warranty retrieval job configuration is from setting option in the OMIVV. In addition, you can also run or schedule warranty retrieval job from **Job Queue**->**Warranty**. Scheduled jobs are listed in the Job queue. In an SSO environment having multiple vCenters, the chassis warranty runs automatically with every vCenter when the warranty for any vCenter is run. Warranty is not automatically run if it is added to chassis profile.

To run a warranty retrieval job:

1. In the **Configuration Wizard**, in the **Warranty Schedule** window, select **Enable Warranty Data Retrieval** to enable you to schedule the warranty.
2. Under **Warranty Data Retrieval Schedule**, do the following:
   a. Select the check box next to each day of the week that you want to run the warranty.
   b. In the text box, enter the time in HH:MM format.

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

Configuring Events And Alarms [Wizard]

You can configure events and alarms using the **Configuration Wizard** or from the **Settings** option for **Events and Alarms**. To receive the events from the servers, OMIVV is configured as the trap destination. For 12th generation hosts and later, the SNMP trap destination must be set in iDRAC. For hosts prior to 12th generation, trap generation must be set in OMSA.

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

To configure events and alarms:

1. In the **Initial Configuration Wizard**, under **Event Posting Levels**, select one of the following:
   - Do not post any events — Block hardware events.
   - Post All Events — Post all hardware events.
   - Post only Critical and Warning Events — Post only critical or warning level hardware events.
   - Post only Virtualization-Related Critical and Warning Events — Post only virtualization-related critical and warning events; this is the default event posting level.
2. To enable all hardware alarms and events, select the **Enable Alarms for Dell Hosts** check box.

   NOTE: Dell hosts that have alarms enabled respond to some specific critical events by entering maintenance mode.
3. A dialog box **Enabling Dell Alarm Warning** is displayed, click **Continue** to accept the change, or click **Cancel**.

   NOTE: You must complete this step only if **Enable Alarms For Dell Hosts** is selected.

   NOTE: After restoring the appliance the **Events and Alarms** settings are not enabled even if the Graphic User Interface shows it as enabled. You must enable the **Events and Alarms** settings again from the **Settings** page.
4. Click **Apply**.

3

About VMware vCenter Web Client Navigation

Navigating around VMware vCenter is easy. When you log in to VMware vCenter and land on the home page and Home Tab, the **OpenManage Integration** icon is located in the main content area under the Administration group. Use the **OpenManage Integration** icon to navigate to the OpenManage Integration for VMware vCenter tab. The Dell group is displayed in the Navigator Area.

VMware vCenter layout has the following three main sections:

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

Topics:

Navigating to the OpenManage Integration for VMware vCenter Inside the VMware vCenter

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

1. Log in to VMware vCenter.
2. In VMware vCenter home page, click the **OpenManage Integration** icon.
   From here you can manage OpenManage Integration for VMware vCenter connection profiles, product settings, monitor inventory and warranty jobs, view the summary page and much more from the tabs in the main content area.
3. To monitor hosts, datacenters, and clusters, in the left-side Navigator, under Inventory Lists, select the host, datacenter or cluster you want to investigate and then on the Object tab, click the object you want.

Understanding Icon Buttons

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

Table 1. Icon buttons defined.

Icon Button	Definition
	Use this plus-sign icon to add or create something new.

Table 1. Icon buttons defined. (continued)

Icon Button	Definition
	Use this add server icon to add a server to a connection profile, datacenter, and cluster,
	Use this icon to abort a job.
	Use this icon to collapse a list.
	Use this icon to expand a list.
	Use this icon to delete an object.
	Use this icon to change a schedule.
	Use this pencil icon to edit.
	Use this broom icon to purge a job.
	Use this icon to export a file.

Locating the Software Version

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

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

Refreshing the Screen Content

Refresh the screen at anytime using the VMware vCenter Refresh icon.

1. Select a page that you want to refresh.
2. In the VMware vCenter title bar, click the **Refresh** button.
   The Refresh icon is left of the Search area and looks like a clockwise arrow.

Viewing the OpenManage Integration for VMware vCenter Licensing Tab

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

The page under **Licensing** displays:

- Buy License

This page under **License Management** has links to

- Product Licensing Portal (Digital Locker)
- iDRAC Licensing Portal
- Administration Console
- Buy License

In the OpenManage Integration for VMware vCenter, on the Licensing tab, view the following:

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.

Opening Online Help

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

1. In OpenManage Integration for VMware vCenter. Do one of the following:
   - In the Help and Support, under **Product Help**, click **OpenManage Integration for VMware vCenter Help**.
2. Use the left-pane table of contents or search to find the topic of your choice.
3. When finished with Help, in the upper right-hand corner, Close the window or tab. if a browser is opened, the online help contents are displayed in the browser window. If you want to close the online help, click on the **X** which is on the top right corner of the browser window.

Finding Help and Support

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

Product Help	Provides the following links: • **OpenManage Integration for VMware vCenter Help** Provides a link to the product help, which is located inside the product. Use the table of contents or search to find the help you need. • About This link brings up the Version Information dialog box. You can find the product version here.
Dell Manuals	Provides live links to: • Server Manuals • OpenManage Integration for VMware vCenter Manuals
Administration Console	Provides a link to the Administration Console.
Additional Help and Support	Provides live links to: • iDRAC with Lifecycle Controller Manuals • Dell VMware Documentation • OpenManage Integration for VMware vCenter Product Page • Dell Help and Support Home

	• Dell TechCenter
Support Call Tips	Offers tips on how to contact Dell Support and route your calls correctly.
Troubleshooting Bundle	Provides a link to create and download the troubleshooting bundle. Provide or see this bundle when you contact technical support. For more information, see `Download a Troubleshooting Bundle`
Dell Recommends	Dell recommends Dell Repository Manager and you can find a link to it here. Use Dell Repository Manager to find and download all firmware updates available for your system.
iDRAC Reset	Provides a Reset iDRAC link to use when iDRAC is not responsive. This reset performs a normal iDRAC reboot.

Downloading a Troubleshooting Bundle

Use this information to assist in troubleshooting issues, or send to Technical Support.

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

Resetting iDRAC

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

NOTE: Dell recommends that you place the host in maintenance mode before resetting iDRAC. You can only apply this reset action on a host that is part of a connection profile that has been inventoried at least once. This reset action might not return the iDRAC to a usable state. In this case, a hard reset is required. Refer to your iDRAC documentation to learn more about a hard reset.

While iDRAC is rebooting, you might see:

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

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

1. In the OpenManage Integration for VMware vCenter, click the **Help and Support** tab.
2. Under iDRAC Reset, click **Reset iDRAC**.
3. On the iDRAC Reset dialog, under iDRAC Reset, type the host IP address/name.
4. To confirm that you understand the iDRAC reset process, select the **I understand iDRAC reset. Continue iDRAC reset**.
5. Click **Reset iDRAC**.

Launching the Administration Console

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

1. In the OpenManage Integration for VMware vCenter, on the Help and Support tab, under the Administration Console, click the link to the console.

2. In the Administration Console login, use the admin password to log in. You can perform the following operations in the Administration console:
   a. Register or unregister a vCenter, modify credentials, or update the certificate.
   b. Upload the license.
   c. View the summary about the number of vCenters registered and available, and about maximum host license, in use and available.
   d. Restart the virtual appliance.
   e. Update (upgrade to latest version).
   f. Generate troubleshooting bundle.
   g. Display the network settings (read only mode).
   h. Configure the HTTP Proxy Settings: this is used to connect to Dell server for appliance upgrade or for connectivity to http://downloads.dell.com/published/Pages/index.html.
   i. Configure NTP settings, which allow you to enable or disable NTP server, and configure preferred and secondary NTP server.
   j. Generate a certificate signing request (CSR), upload a certificate, or restore the default certificate for HTTPS Certificates.
   k. Configure global settings on how alerts are stored for all vCenter instances. You can configure the maximum numbers of alerts to be stored, numbers of days to retain them, and time out for duplicate alerts.
   l. Initiate Backup, or Restore.
   m. Configure backup location to a network share, and the encryption password for the backed-up files (along with test network connection).
   n. Schedule a recurring backup.

4

Profiles

The Credential Profiles tab let you manage and configure the Connection Profiles and the Chassis Profiles.

The Connection Profiles let you manage and configure connection profiles required to access the Dell servers. The Connection Profiles lets you manage and configure connection profiles that contain credentials used by the virtual appliance to communicate with Dell Servers. Associate each Dell server with only one connection profile for management by the OpenManage Integration for VMware vCenter. You may assign multiple servers to a single connection profile.

The Chassis Profiles let you manage and configure connection profiles that contain credentials used by the virtual appliance to communicate with Dell Chassis. Associate each discovered Chassis with one chassis profile for management by the OpenManage Integration for VMware vCenter. You may assign multiple chassis to a single chassis profile.

- Creating a Connection Profile
- Viewing Connection Profiles
- Editing a Connection Profile
- Refreshing a Connection Profile
- Deleting a Connection Profile
- Testing a Connection Profile

Topics:

Viewing Connection Profiles

A Connection Profile must be created and/or exist before it can be viewed.

After one or more connection profiles are created, those can be viewed on Connection Profile page. The OpenManage Integration for VMware vCenter uses the credentials given in the profiles to communicate with Dell hosts.

In OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Connection Profiles** you can view all the connection profiles you have created. The information you can view includes:

Profile Name	Displays the name of the connection profile.
Description	Displays a description, if provided.
vCenter	Displays the FQDN or Host Name or else IP address of the vCenter as per the context.
Associated Hosts	Displays the hosts associated with this connection profile. If more than one, use the expand icon to show all.
iDRAC Certificate Check	Shows whether the iDRAC Certificate Check is enabled or disabled.
Host Root Certificate Check	Shows whether the Host Root Certificate Check is enabled or disabled.
Date Created	Displays the create date.
Date Modified	Displays the Modify date.

Last Modified By	Displays user's details.

Creating A Connection Profile

You may associate multiple hosts to a single connection profile. Create a Connection Profile using the following steps:

NOTE: The vCenter hosts that display during this procedure have authenticated using the same Single Sign On (SSO). If you do not see a vCenter host, it may be on a different SSO or you may be using a VMware vCenter version less than version 5.1.

1. In the OpenManage Integration for VMware vCenter, in the left pane, on the **Manage** → **Profiles** → **Credential Profiles** → **Connection Profiles** tab, click on **+**.
2. In the **New Connection Profile** page, enter the following.
3. In the **Profile Name and Description** area, do the following:
   a. Under Profile, type the **Profile Name** and optional **Description**.
   b. Under Associated Hosts, select one or multiple hosts on which you want to associate with this connection profile. This option lets you create one connection profile for one or multiple hosts.
   c. Click **Next**.
   d. Under **iDRAC Credentials** page, do the following:
      - The iDRAC account requires administrative privileges for updating firmware, applying hardware profiles, and deploying hypervisor.
      - In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
      - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
      - In the **Verify Password** text box, type the password again
      - Perform the following actions:
        - To download and store the iDRAC certificate and validate it during all future connections, select the **Certificate Check** Enabled drop-down
        - To perform no check and not store the certificate, do not select the **Certificate Check**

   e. In the **Hosts Root** page, do the following:.
      - For hosts already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise skip down to configure your Host Credentials.

        In the **Active Directory User Name** text box, type the user name. Type the username in one of these formats: domain\username or username@domain. The user name is limited to 256 characters. Refer to Microsoft Active Directory documentation for user name restrictions.
      - In the **Active Directory Password** text box, type the password. The password is limited to 127 characters.
      - In the **Verify Password** text box, type the password again.
      - Perform one of the following actions:
        - To download and store the Host certificate and validate it during all future connections, select the box.
        - To perform no check and not store the Host certificate, do not select the **Enable Certificate Check** box.
      - To configure Host Credentials without Active Directory, do the following:
      - In the **User Name** text box, the user name is root. This is the default username and you cannot change the username
      - If the Active directory is set, you can choose any Active directory user not just root.
      - In the **Password** text box type the password. The password is limited to 127 characters.

        NOTE: The OMSA credentials are the same credentials as those used for ESXi hosts.
      - In the **Verify Password** text box, type the password again.
      - In the **Enable Certificate Check** check box, select one of the following:
      - To download and store the Host certificate and validate it during all future connections, select the **Enable Certificate Check** box.

- To perform no check and not store the Host certificate, do not select the **Enable Certificate Check** check box.

4. Click **Next**.
5. In the Associated Hosts page, select one or more hosts for the connection profile and click **OK**.
6. To test the connection profile, select one or more hosts and select the Test Connection button. This step is optional. This is used to check whether or not the Host and iDRAC credentials are correct.
7. To complete the profile, click **Next**. For servers that do not have either an iDRAC Express or Enterprise card, the iDRAC test connection result states Not Applicable for this system.

Editing a Connection Profile

After you have configured a connection profile, you can edit the profile name, description, associated hosts, and credentials.

NOTE: The vCenters that display during this procedure has authenticated using the same Single Sign On (SSO). If you do not see a vCenter host, it may be on a different SSO or you may be using a VMware vCenter version less than version 5.1.

NOTE: You are allowed to edit the connection profile irrespective of the license limit

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Connection Profiles** tab, select a connection profile.
2. Click the **Edit** icon.
3. In the Connection Profile window, on the Welcome tab, read the information and click **Next**.
4. In the Name and Credentials tab, do the following:
   a. Under Profile, type the **Profile Name** and optional **Description**.
   b. Under vCenter, view the associated hosts for this connection profile. See the note preceding about why you see the hosts displayed here.
   c. Under iDRAC Credentials, do the following:
      - The user name is root and this entry cannot be modified if you do not select the **Active Directory**. It is not compulsory that iDRAC user needs to use root credential, it can be any Administrator Privilege if the **Active directory** is set.
      - Domain\Username: Type the username in one of these formats: domain\username, or domain@username.
        - The following characters are allowed for the user name: / (forward slash), &, \ (backslash), . (period), " (quotation mark), @, % (percent) (127 character limit).
        - The domain can contain alphanumeric characters, - (dash), and . (period) only (254 character limit). The first and last characters for domain must be alphanumeric.
      - Password: Type your password.

        The following characters are not allowed for the password: / (forward slash), &, \ (backslash), . (period), " (quotation mark).
      - Verified password: Type your password again.
      - Enable Certificate Check: The default is a cleared check box. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**, or clear the **Enable Certificate Check** check box to perform no certificate check and not store the certificate.

        NOTE: You need to select **Enable** if you are using Active-Directory.
   d. Under Host Root, do the following:
      - Select the **Use Active Directory** check box to access all the consoles associated with the active directory.

        Username: The default username is **root** and cannot be modified. If the Use Active Directory is selected, you can use any active directory user name.
      - Password: Type your password.

        The following characters are not allowed for the password: / (forward slash), &, \ (backslash), . (period), " (quotation mark).
      - Verified password: Type your password again.

- Enable Certificate Check: The default is a cleared check box. To download and store the iDRAC certificate and validate it during all future connections, select **Enable Certificate Check**, or clear the **Enable Certificate Check** check box to perform no certificate check and not store the certificate.

  NOTE: You need to select **Enable** if you are using Active-Directory.

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

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

5. Click **Next**.
6. In the Select Hosts dialog box, select the hosts for this connection profile.
7. Click **OK**.
8. The Associated Host tab lets you test the iDRAC and Host Credentials on the selected servers. Do one of the following:
   - To begin the test, select the hosts to check and then click the **Test Connection** icon. The other options are inactive.

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

Refreshing A Connection Profile

In the OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Connection Profiles** tab, up in the VMware vSphere Web Client title bar, click the **Refresh** icon.

NOTE: After removing the host from vCenter, when you navigate to connection profile page, you will be prompted to remove the host from connection profile. Upon confirmation, the host will be removed from Connection Profile.

Deleting A Connection Profile

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Connection Profiles** tab, select the profiles to delete.
2. Click the **Delete** icon.
3. On the Delete Confirmation message, to remove the profile, click **Yes** , or click **No** to cancel the delete action.

Testing a Connection Profile

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Connection Profiles** tab, select a connection profile to test. This action may take several minutes to complete.
2. In the Test Connection Profile dialog, select the hosts you want to test and then click the **Test Connection** icon.
3. To abort all selected tests and cancel the testing, click **Abort All Tests**. In the Abort Tests dialog box, click **OK**.
4. To exit, click **Cancel**.

Creating A Chassis Profile

OMIVV can monitor all Dell Chassis associated with the Dell servers that are managed by OMIVV. Chassis profile is required to monitor the chassis. A chassis credential profile can be created to associate with a single or multiple chassis. The chassis profile is created using the following steps:

1. In the **OpenManage Integration for VMware vCenter**, select **Manage** > **Profiles** > **Credential Profiles** > **Chassis Profile**.
2. In the **Chassis Profiles** page, click on the **Plus (+)** icon to create a **New Chassis Profile**.
3. In the **Chassis Profile Wizard** page, do the following:

a. In the **Profile Name** text box, enter the profile name.
b. In the **Description** text box, enter an optional description.

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

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

5. Click **Next**.

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

   NOTE: Chassis will be discovered and available to be associated with the Chassis Profile only after the successful inventory run of any modular host present under that chassis.

6. To select either an individual chassis or multiple chassis, select the corresponding check boxes next to the **IP/Host Name** column.

   If the selected chassis is already a part of another profile then a warning message is displayed, stating that the selected chassis is associated with a profile.

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

7. Click **OK**.

   The **Associated Chassis** page is displayed.

8. Select the chassis and click on **Test Connection** Icon to test the chassis connectivity which verifies the credentials and the result is displayed in the **Test Result** column as **Pass** or **Fail**.
9. Click **Finish** to complete the profile.

   NOTE: You can also add or remove a chassis by clicking on the Plus Icon displayed on the top left corner of the **Associated Chassis** page.

Viewing Chassis Profiles

To view chassis profiles:

1. In the **OpenManage Integration for VMware vCenter**, select **Manage** > **Profiles** > **Credential Profiles** > **Chassis Profiles** window. The Chassis Profiles are displayed.
2. If multiple chassis are associated with the Chassis Profile, clicking the arrow icon displays all the associated chassis.
3. In the **Chassis View** page, you can view the Profile name, description, Chassis IP, service tag and the date you modified the chassis.
4. You can perform the following actions from the **Chassis View** Page.
   a. Add
   b. Edit
   c. Delete
   d. Test connectivity

Editing a Chassis Profile

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

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Profiles** > **Credential Profiles** > **Chassis Profiles** tab, select a chassis profile.
2. Click the **Edit** icon on the main menu which is displayed as a tilted `Pencil` icon.
3. The **Edit Chassis Profile** window is displayed.
4. In the **Chassis Profile** area, you can edit the **Profile Name** and optional **Description**.

5. Under the **Credentials** area, you can edit the **User Name**, **Password**, and **Verify Password** The password that you type in the **Verify Password** must be same as the one you entered in the **Password** field. The credentials entered must have administrator rights on the chassis.
6. Click **Apply**. The changes are saved.
7. The **Associated Chassis** tab lets you test the Chassis and Credentials on the selected chassis. Do one of the following:
   - To begin the test, select either one chassis or multiple chassis to check and then click the **Test Connection** icon. The **Test Result** column displays whether or not the test connection is successful.
   - You can add or delete either one or multiple chassis to a chassis profile by clicking on the **Plus** icon.

   NOTE: If the chassis are not inventoried, only the IP/host name and Service tag are displayed. The fields **Chassis Name** and **Model** are displayed once the chassis is inventoried.

Deleting Chassis Profiles

To delete Chassis profiles:

1. In the **OpenManage Integration**, select **Manage** > **Profiles** > **Credential Profile** > **Chassis Profiles** window.
2. Select a chassis profile that you want to delete and click the **Cross** (X) Icon. A warning message is displayed.
3. Click **Yes** to proceed with deletion or click **No** to cancel deletion.

   NOTE: If all the chassis associated to a Chassis profile have been deselected or moved to different profiles, a delete confirmation message will be displayed mentioning the chassis profile does not have any associated chassis and will be deleted. Click on OK to delete the chassis profile.

Testing a Chassis Profile

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

5

Job Queue

After the OpenManage Integration for VMware vCenter is configured, you can monitor the inventory, warranty jobs and firmware updates under the Monitor tab. Inventory and warranty are set up with the Configuration Wizard or from the Settings tab.

- Inventory History
- Warranty History

Topics:

Inventory History

Inventory Jobs are set up using the Settings tab or the Initial Configuration wizard. Use the Inventory History tab to view your inventory jobs. Tasks you can do from this tab include:

- Viewing Host Inventory
- Changing Inventory Job Schedules
- Running an Inventory Job Now
- Running a Chassis Inventory Job Now

Viewing Hosts Inventory

A successful completed inventory is required to gather the data. Once the inventory is complete, you can view the inventory results for the entire datacenter or for an individual host system. Columns are sortable in ascending and descending order.

If server data cannot be retrieved and displayed, there are several possible causes:

- The server is not associated with a connection profile, and therefore you cannot run an inventory job.
- An inventory job has not been run on the server to collect the data, and therefore there is nothing to display.
- The number of host licenses is exceeded, and you must have additional licenses available for the inventory task to complete.
- The server does not have the correct iDRAC license required for 12th and later generation of Dell PowerEdge servers and you must purchase the correct iDRAC licence.
- Credentials might be wrong
- Target might not be reachable

To view the host inventory details, do the following:

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue** > **Inventory History** > **Hosts Inventory**.
3. To view the server information on a selected vCenter, select a vCenter to display all associated host details.
4. Review the Host Inventory information.

vCenter Details	
vCenter	Displays vCenter Address.

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

Changing Inventory Job Schedules

To make sure there is up-to-date server information, you must run periodic inventories on Dell servers. Dell recommends running an inventory once a week. Inventories do not impact host performance. You can change inventory job schedule on the **Monitor** > **Job Queue** > **Inventory History** > **Hosts Inventory** page or from the **Initial Configuration Wizard**.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Inventory History** > **Hosts Inventory**.
2. Select a vCenter and then click the **Change Schedule** icon.
3. In the Inventory Data Retrieval dialog box, do the following:
   a. Under Inventory Data, select the **Enable Inventory Data Retrieval** check box.
   b. Under Inventory Data Retrieval Schedule, select the days of the week for your job.
   c. In the Inventory Data Retrieval Time text box, type the local time for this job.
   You may need to consider the time difference between job configuration time and job implementation time.
4. Click **Apply** to save the settings, **Clear** to reset the settings, and **Cancel** to abort the operation.

Running an Inventory Job Now

Run and triggers an Inventory task immediately for the selected VCenter triggers an Inventory task immediately for the selected VCenter.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Inventory History** > **Hosts Inventory**.
2. Click the **Run Now** button.
3. In the Success dialog box, click **Close**.

   NOTE: When you run a modular host inventory, corresponding chassis are discovered automatically.

   An inventory job is now in queue. Note that you cannot run an inventory for a single host. An inventory job starts it for all hosts.

Running a Chassis Inventory job now

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

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Inventory History** > **Chassis Inventory**.
2. The list of chassis and status that had inventory run in the last inventory execution will be shown.

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

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

Warranty History

Hardware warranty information is retrieved from Dell Online and displayed by the OpenManage Integration for VMware vCenter. Server's Service Tag is used to gather warranty information about the server. Warranty data retrieval jobs are set up using the Configuration Wizard. View your warranty job history on this tab. Tasks you can do on this tab include:

- Viewing Warranty History
- Modifying a Warranty Job Schedule
- Running a Warranty Job Now

Viewing Warranty History

A warranty job is a scheduled task to get warranty information from support.dell.com on all systems. Columns are sortable in ascending and descending order.

1. In the OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. Click **Job Queue** > **Warranty History.**
3. Expand Warranty History to display **Hosts Warranty** and **Chassis Warranty**.
4. Select either **Hosts Warranty** or **Chassis Warranty** to view your corresponding warranty job history information

vCenter History	
vCenters	Displays lists of vCenters.
Hosts Passed	Displays the number of vCenter Hosts that passed.
Last Warranty	Displays the last warranty job that was run.
Next Warranty	Displays the next warranty job that will run.
Modify Schedule button	Click to edit a warranty job schedule.
Run Now button	Click to run a warranty job.
Hosts History	
Host	Displays the host address.
Status	Displays the status. Options include: • Successful • Failed • In Progress • Scheduled
Duration (MM:SS)	Displays the duration of the warranty job in MM:SS.
Start Date and Time	Displays the date and time when the warranty job started.
End Date and Time	Displays the time the warranty job ended.
Chassis History	
Chassis IP	Displays the chassis IP address.

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

Modifying a Warranty Job Schedule

Warranty jobs are originally configured in the Initial Configuration Wizard. Later, you can modify a warranty job schedule on the **Monitor Tab** > **Job Queue** > **Warranty History** > **Hosts Warranty** page or from the **Manage Tab** > **Settings** page.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab, click **Warranty History**.
2. Click the **Change Schedule** icon.
3. In the Warranty Data Retrieval dialog box, do the following:
   a. Under Warranty Data, select the **Enable Warranty Data Retrieval** check box.
   b. Under Warranty Data Retrieval Schedule, select the days of the week for your job.
   c. In the Warranty Data Retrieval Time text boxes, type the local time for this job.
   You may need to calculate the time difference required to run this job at the proper time.
4. Click **Apply**.

Running a Hosts Warranty Job Now

Run an warranty job at least once a week.

1. In the OpenManage Integration for VMware vCenter, on the **Monitor** > **Job Queue** tab.
2. Click on **Warranty History** and **Hosts Warranty** to select the warranty job you want to run.
3. Click the **Run Now** button.
4. In the Success dialog box, click **Close**.

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

   A warranty job is now in queue.

Running a Chassis Warranty Job Now

Run an warranty job at least once a week.

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

Log

You can view user actions on the **Monitor** > **Log** tab of the OpenManage Integration for VMware vCenter.

You can sort the content on this page using the two drop-down lists. The first drop-down list lets you sort on file category, which includes:

- All Categories
- Info
- Warning
- Error

The second drop-down helps you sort on blocks of time, which include:

- Last Week
- Last Month
- Last Year
- Custom Range

  If you select custom range, you can pick the start and end date and click Apply.

You can also sort the datagrid columns in ascending or descending order by clicking the column header.

Use the Filter text box to search within your content.

At the bottom of the page grid, the following information is displayed:

Total items	Displays the total count of all log items.
Items per screen	Displays the number of log items on the displayed page. Use the drop-down box to set the number of items per page.
Page	Displays the page you are on. Type a page number in the text box or use the Previous and Next buttons to get you the page you want.
Previous or Next buttons	Buttons that guide you to the next or previous pages.
Export All icon	Use this to export log content to a CSV file.

Viewing the Logs

1. In OpenManage Integration for VMware vCenter, click the **Monitor** tab.
2. On the Log tab, view the user actions logs for the OpenManage Integration for VMware vCenter. The Log page shows:

All Categories	Enables you to filter and view the logs based on the following log types: • All Categories • Info • Warning • Error
Date Filter	Enable you to filter and view the logs by: • Last Week • Last Month • Last Year • Custom Range To filter the date based on the specific date, select **Custom Range** from the Date Filter drop-down list, enter **Start date** and **End date** based on the which you need to filter, and then click **Apply**.
Search	Enables you filter based on the log description or specific text in the log.

Table 2. Grid table details

Category	**Displays the category type.**
Date and Time	**Displays the date and time of the user action.**
Description	**Displays a description of the user action.**

3. To sort the data in the grid, click a column header.
4. To sort using categories or time blocks use the drop-down lists above the grid.
5. To Navigate page between pages of log items, use the Previous and Next buttons.

Exporting Log Files

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

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

6

Console Administration

Administration of the OpenManage Integration for VMware vCenter and its virtual environment is achieved by using two additional administration portals:

- Web-based Administration Console
- Console view for an individual server (the appliance virtual machine console).

Through the use of these two portals, global settings for vCenter management, OpenManage Integration for VMware vCenter database backup and restore, and reset/restart actions can be entered and used across all vCenter instances.

Topics:

Using the Administration Console

From the vCenter Registration window in the Administration Console, you can register a vCenter server, and upload or buy a license. If you are using a demo license, a Buy Software link displays from which you can purchase a full-version license for managing multiple hosts. In this section you can also modify, update, and unregister a server.

Related Tasks:

- Registering a vCenter server by a non-administrator user with necessary privileges on page 33
- Registering a vCenter Server
  - Modifying the vCenter Login
  - Updating the SSL Certificates for Registered vCenters
  - Uninstalling OpenManage Integration for VMware vCenter from vCenter
- Uploading a OpenManage Integration for VMware vCenter License

Registering a vCenter server by a non-administrator user with necessary privileges

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

Perform the following steps to enable a user with the required privileges to register a vCenter server:

1. Add a role and select the required privileges for the role or modify an existing role to change the privileges selected for that role. See VMware vSphere documentation for the steps required to create or modify a role and select privileges in the vSphere Web client. See Defining privileges on page 34 to select all the required privileges for the role.

   NOTE: The vCenter administrator should add or modify a role.
2. After you define a role and select privileges for the role, assign a user to the newly created role. See VMware vSphere documentation for more information on assigning permissions in the vSphere Web client. A vCenter server non-administrator user with the required privileges can now register and/or unregister vCenter, modify credentials, or update the certificate.

   NOTE: The vCenter administrator should assign permissions in the vSphere client.
3. Register a vCenter server by using a non-administrator user with the required privileges. See Registering a vCenter server by a non-administrator user with the required privileges on page 34.
4. Assign the Dell privileges to the role created or modified in step 1. See Assigning Dell privileges to the role in vSphere Web client on page 34.

Now, a non-administrator user with the required privileges can use the OMIVV features with Dell hosts.

Defining privileges

To enable a non-administrator user with the required privileges to register a vCenter server, select the following privileges:

- Alarms
  - Create alarm
  - Modify alarm
  - Remove alarm
- Extension
  - Register extension
  - Unregister extension
  - Update extension
- Global
  - Cancel task
  - Log event
  - Settings
- Host
  - CIM
    - CIM Interaction
  - Configuration
    - Advanced settings
    - Connection
    - Maintenance
    - Query patch
    - Security profile and firewall
  - Inventory
    - Add host to cluster
    - Add standalone host
- Host profile
  - Edit
  - View
- Permissions
  - Modify permission
  - Modify role
- Sessions
  - Validate session
- Task
  - Create task
  - Update task

NOTE: While registering a vCenter server by a non-administrator user with the necessary privileges, an error message is displayed if the mentioned privileges are not assigned.

Registering a vCenter server by a non-administrator user with the required privileges

You can register a vCenter server for the OMIVV appliance by using a non-administrator user with the required privileges. See Registering a vCenter Server on page 35 for more information on registering a vCenter server.

Assigning Dell privileges to the role in vSphere Web client

You can edit an existing role to assign Dell privileges.

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

To assign the Dell privileges to an existing role, perform the following:

1. Log in to the vSphere Web client with administrative rights.
2. Browse to **Administration → Role Manager** in vSphere Web client.
3. Select a vCenter server system from the drop-down menu.
4. Select a role and click **Edit role action**.
5. Select the following privileges and click **OK**.
   - Dell
     - Dell.Configuration
     - Dell.Deploy-Provisioning
     - Dell.Inventory
     - Dell.Monitoring
     - Dell.Reporting

   See Security Roles and Permissions on page 135 for more information on the available OMIVV roles within vCenter.

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

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

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

Registering a vCenter Server

You can register the OpenManage Integration for VMware vCenter after the OpenManage Integration for VMware vCenter is installed. OpenManage Integration for VMware vCenter uses the admin user account or a non-administrator user account with necessary privileges for vCenter operations. OpenManage Integration for VMware vCenter currently supports 10 vCenters per OMIVV appliance that can be changed later.

1. Open **Administration Console** from a supported browser.
2. To register a new vCenter server, in the left pane, click **VCENTER REGISTRATION**, and then click **Register New vCenter Server**.
3. In the **Register a New vCenter** dialog box, under **vCenter Name** do the following:
   a. In the **vCenter Server IP or Hostname** text box, enter the vCenter IP address or FQDN of the host.

      NOTE: Registering OMIVV with the VMware vCenter by using Fully Qualified Domain Name (FQDN) is highly recommended. For all registrations, the host name of vCenter should be properly resolvable by the DNS server. The following are the recommended practices for using the DNS server:
      - Assign a static IP address and host name when you deploy an OMIVV appliance with a valid DNS registration. A static IP address ensures that during the system restart, the IP address of the OMIVV appliance remains same.
      - Ensure that OMIVV host name entries are present in both forward and reverse lookups.

   b. In the **Description** text box, enter an optional description.
4. Under **vCenter User Account**, do the following:
   a. In the **vCenter User Name** text box, enter the administrator's user name or a non-administrator user name with the required privileges.
   b. In the **Password** text box, enter the password.
   c. In the **Verify Password** text box, enter the password again.
5. Click **Register**.

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

For example: Suppose, a user X with the necessary privileges registers OMIVV with vCenter and user Y has only Dell privileges. The 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.

OpenManage Integration for VMware vCenter Requirements

The OpenManage Integration for VMware vCenter (OMIVV) requires information from OpenManage on older generation servers, and more current platforms are restricted to start at the version of vSphere that understands the newer chipset. Due to this, there are limits on the version of vSphere that a given version of OMIVV works with.

Table 3. Supported ESXi versions on managed hosts

ESXi version support	Server generation		
	11G	12G	13G
v5.0	Y	Y	N
v5.0 U1	Y	Y	N
v5.0 U2	Y	Y	N
v5.0 U3	Y	Y	N
v5.1	Y	Y	N
v5.1 U1	Y	Y	N
v5.1 U2	Y	Y	Y
v5.1 U3	N	Y	Y (except M830, FC830, and FC430)
v5.5	Y	Y	N
v5.5 U1	Y	Y	N
v5.5 U2	Y	Y	Y
v5.5 U3	Y	Y	Y
v6.0	Y	Y	Y
v6.0 U1	Y	Y	Y
v6.0 U2	Y	Y	Y
v6.0 U3	Y	Y	Y

Table 4. Supported vCenter Server versions for release 3.2

vCenter version	Desktop client support	Web client support
v5.1 U2	Y	N
v5.1 U3	Y	N
v5.5 U1	Y	Y
v5.5 U2	Y	Y
v5.5 U3	Y	Y
v6.0	Y	Y

Table 4. Supported vCenter Server versions for release 3.2 (continued)

vCenter version	Desktop client support	Web client support
v6.0 U1	Y	Y
v6.0 U2	Y	Y
v6.0 U3	Y	Y

Modifying the vCenter Login

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

1. In OpenManage Integration for VMware vCenter, on the **Summary** tab, use the link to open the **Administration Console**.
2. In the Login dialog box, type your password.
3. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in the right pane. To open the **Modify vCenter Acct** window, under **Credentials**, click **Modify**.
4. Enter the vCenter **User Name**, **Password**, and **Verify Password**; the passwords must match.
5. To change the password, click **Apply**, or to cancel the change click **Cancel**.

NOTE: An error message is displayed if the necessary privileges are not assigned to a non-administrator user who is modifying the vCenter login credentials.

Updating The SSL Certificates For Registered vCenter Servers

If the SSL certificate is changed on a vCenter server, then use the following steps to import the new certificate for the OpenManage Integration for VMware vCenter. The OpenManage Integration for VMware vCenter uses this certificate to make sure the vCenter server it is talking to is the correct vCenter server and not an impersonator.

OpenManage Integration for VMware vCenter uses the openssl API to create the Certificate Signing Request (CSR) using the RSA encryption standard with a 2048 bit key length. The CSR generated by the OpenManage Integration for VMware vCenter is used to get a digitally signed certificate from a trusted Certification Authority. The OpenManage Integration for VMware vCenter uses the digital certificate to enable SSL on the Web server for secure communication.

1. Launch a web Browser then enter https://<ApplianceIPAdrdress>
2. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in the right pane. To update the certificates, click **Update**.

Uninstalling the OpenManage Integration for VMware vCenter

To remove the OpenManage Integration for VMware vCenter, it must be unregistered from the vCenter server using the Administration Console.

1. Launch a web browser then enter https://<ApplianceIPAdrdress>
2. In the **vCenter Registration** page, under the vCenter server table, unregister the OpenManage Integration for VMware vCenter by clicking **Unregister**.
   You may have more than one vCenter, so be sure select the right one.
3. In the **Unregister vCenter** dialog box that asks if you really want to unregister this server, click **Unregister**.

Uploading a OpenManage Integration for VMware vCenter License to the Administration Console

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console from **Help and Support** tab.
2. In the Login dialog box, type your password.
3. In the left pane, click **VCENTER REGISTRATION**. The registered vCenters are displayed in a table. To display the upload license dialog box, click **Upload License**.

4. To navigate to the license file, click the **Browse** button, to navigate to the license file, and then click **Upload**.

   NOTE: If the license file is modified or edited in any way, the appliance views it as corrupted and the file will not work.

   NOTE: You can add licenses if you need to add more hosts. Follow the process mentioned above to add more licenses.

   NOTE: If the number of successfully inventoried 11th, 12th, and 13th generation servers equals the number of purchased licenses. Edit existing connection profiles by removing few 11th, 12th, or 13th generation servers. Create a new connection profile for the removed 11th, 12th, or 13th generation servers.

Virtual Appliance Management

Virtual appliance management contains the OpenManage Integration for VMware vCenter network, version, NTP, and HTTPS information, and lets you:

- Restart the virtual appliance
- Update the virtual appliance and configure an update repository location
- Download a troubleshooting bundle
- Set up NTP servers
- Upload HTTPS certificates

Restarting the Virtual Appliance

Restarting the virtual appliance logs you out from the Administration Console, and the OpenManage Integration for VMware vCenter is unavailable until the virtual appliance and its services are active.

1. In OpenManage Integration for VMware vCenter, under Administrative Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. To restart the OpenManage Integration for VMware vCenter, click **Restart the Virtual Appliance**.
5. On the **Restart Virtual Appliance** dialog box, to restart the virtual appliance click **Apply** or click **Cancel** to cancel.

Updating a Repository Location and Virtual Appliance

Perform a backup prior to an update of the virtual appliance to make sure all data is protected. See, Managing Backup and Restore.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Next to Appliance Update, click **Edit**.
5. In the **Appliance Update** window, enter the **Repository Location URL**, and then click **Apply**.

   NOTE: If the update location is on an external network, such as the Dell FTP site, then a proxy must be entered in the HTTP Proxy area.

Updating the Virtual Appliance Software

To prevent data loss, perform an appliance backup prior to beginning the software update.

1. Launch a web Browser then enter https://<ApplianceIPAddress>.
2. In the left pane, click **APPLIANCE MANAGEMENT**.
3. To update the virtual appliance to the software version listed under **Appliance Update**, click **Update Virtual Appliance**.
4. In the **Update Appliance** dialog box, the current and available versions are listed. To begin the update, click **Update**.

5. The system is locked down and put into maintenance mode. When the update is complete, the Appliance page displays showing the newly installed version.

Downloading the Troubleshooting Bundle

Use this information to assist in troubleshooting issues, or send to Technical Support.

1. Launch a web Browser then enter https://<ApplianceIPAddress>.
2. In the left pane, click **APPLIANCE MANAGEMENT**.
3. To generate the troubleshooting bundle dialog box, click **Generate Troubleshooting Bundle**.
4. Click the **Download Troubleshooting Bundle** link.
5. To exit, click **Close**.

Setting Up The HTTP Proxy

You can set up the HTTP proxy settings using the Administration Console.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. In the **Appliance Management** page, scroll down to the **HTTP Proxy Settings**, and then click **Edit**.
5. In the **Edit** page, do the following:
   a. To enable the use of HTTP Proxy Settings, next to **Use HTTP Proxy Settings**, select **Enable**.
   b. In the **Proxy Server Address** text box, enter the proxy server address.
   c. In the **Proxy Server Port** text box, enter the proxy server port.
   d. To use proxy credentials, next to **Use Proxy Credentials**, select **Yes**.
   e. If you are using credentials, in the **User Name** text box, enter the user name.
   f. In the **Password** text box, type the password.
6. Click **Apply**.

Setting Up the NTP Servers

Use the Network Time Protocol (NTP) to synchronize the virtual appliance clocks to that of a NTP server.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Edit** under **NTP Settings**.
5. Select the **Enabled** check box. Enter the **host name** or **IP address** for a **Preferred** and **Secondary NTP Server** and click **Apply**.
6. To exit, click **Cancel**.

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

Generating a Certificate Signing Request

NOTE: You must upload the certificate before registering the OpenManage Integration for VMware vCenter with the vCenter.

Generating a new Certificate Signing Request prevents certificates that are created with the previously generated CSR from being uploaded to the appliance.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.

2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Generate Certificate Signing Request for HTTPS Certificates**. A message displays stating that if a new request is generated, then certificates created using the previous CSR can no longer be uploaded to the appliance. To continue with the request, click **Continue**, or **Cancel** to cancel.
5. Enter the **Common Name**, **Organizational Name**, **Organizational Unit**, **Locality**, **State Name**, **Country** and **Email** for the request. Click **Continue**.
6. Click **Download**, and then save the resulting certificate request to an accessible location.

Uploading an HTTPS Certificate

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

NOTE: You can use Microsoft Internet Explorer , Firefox, Chrome to upload certificates.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Upload Certificate for HTTPS Certificates**.
5. In the **Upload Certificates** dialog box, click **OK**.
6. To select the certificate to upload, click **Browse**, and then click **Upload**.
7. If you want to abort the upload, click **Cancel**.

   NOTE: The certificate must use PEM format.

Restoring the Default HTTPS Certificate

NOTE: If you want to upload a custom certificate for your appliance, you need to upload the new certificate prior to vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed in the Web client. To fix this issue, you need to unregister and reregister the appliance with the vCenter.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **APPLIANCE MANAGEMENT**.
4. Click **Restore Default Certificate** link under **HTTPS Certificates**.
5. In the restore default certificate dialog box, click **Apply**.

Setting up Global Alerts

Alert management lets you enter global settings for how alerts are stored for all vCenter instances.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **ALERT MANAGEMENT**. To enter new vCenter alert settings, click **Edit**.
4. Enter numeric values for the following items:
   - Maximum number of alerts
   - Number of days to retain alerts
   - Timeout for duplicate alerts (seconds)
5. To save your settings, click **Apply**, or click **Cancel** to cancel.

Managing Backup And Restore

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

- Configuring Backup And Restore
- Scheduling Automatic Backups
- Performing An Immediate Backup
- Restoring The Database From Backup

Configuring Backup And Restore

The backup and restore function backs up the OpenManage Integration for VMware vCenter database to a remote location from which it can be restored later. Profiles, templates, and host information are included in the backup. It is recommended that you schedule automatic backups to guard against data loss. After this procedure, you must configure a backup schedule.

NOTE: NTP Settings are not saved and restored.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE**.
4. To edit the current backup and restore settings, click **Edit**.
5. In the **Settings and Details** page, do the following:
   a. In the **Backup Location** text box, type the path to the backup files.
   b. In the **User Name** text box, type the user name.
   c. In the **Password** text box, type the password.
   d. Under **Enter the password used to encrypt backups**, type the encrypted password in the text box.

      The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.

   e. In the **Verify Password** text box, retype the encrypted password.
6. To save these settings, click **Apply**.
7. Configure the backup schedule. For more information, see Scheduling Automatic Backups.

Scheduling Automatic Backups

This is the second part of configuring backup and restore. For detailed information on configuring the backup location and credentials, see Configuring Backup And Restore.

To schedule an automatic backup:

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE**.
4. To edit the backup and restore settings, click **Edit Automatic Scheduled Backup** (this makes fields active).
5. To enable the backups, click **Enabled**.
6. Select the check boxes for the days of the week for which you want to run the backup.
7. In the **Time for Backup (24 Hour Time Format, HH:mm)** text box, enter the time in HH:mm format.
   The **Next Backup** populates with the date and time of the next scheduled backup.
8. Click **Apply**.

Performing An Immediate Backup

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.

3. In the left pane, click **BACKUP AND RESTORE**.
4. Click **Backup Now**.
5. To use location and encryption password from the Backup settings, in the **Backup Now** dialog box, select that check box.
6. Enter a **Backup Location**, **User Name**, **Password**, and **Encryption Password**.

   The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.

7. Click **Backup**.

Restoring the Database from a Backup

NOTE: The restore operation causes the virtual appliance to reboot after it has completed.

1. In OpenManage Integration for VMware vCenter, under Administration Console, use the link to open the Administration Console.
2. In the Login dialog box, type your password.
3. In the left pane, click **BACKUP AND RESTORE** and the current backup and restore settings are displayed.
4. Click **Restore Now**.
5. In the Restore Now dialog box, enter a File Location along with the **backup .gz** file (CIFS/NFS Format).
6. Enter the **User Name**, **Password**, and **Encryption Password** for the backup file.

   The encryption password can contain alpha numeric characters and the following special characters: !@#$%*. There is no length restriction.

7. To save your changes, click **Apply**.
   The appliance reboots or restarts once Apply is clicked.

Understanding the vSphere Client Console

The **vSphere Client Console** is found within the vSphere Client on a virtual machine. The **Console** works hand in hand with the Administration Console. The Console provides the ability to:

- Configure network settings
- Change the virtual appliance password
- Set the local timezone
- Reboot the virtual appliance
- Reset the virtual appliance to factory settings
- Refresh Console
- Log out from console
- Read-only user role
- Upgrading OpenManage Integration Plugin from 2.0 Version to the Current Version
- Migration Path to migrate from 2.x to the Current Version

Use the arrow keys to navigate up or down. Once you have selected the option you want, press **<ENTER>**. After you access the **Console** screen, VMware vSphere Client takes control of your cursor. To escape from that control, press **<CTRL> + <ALT>**.

Configuring Network Settings

Changes to the network settings are done in the vSphere Client Console.

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.

3. Do one of the following:
   - On the Object tab, select **Action** > **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. In the **Console** window, select **Configure Network**, then press **<ENTER>**.
5. Enter the desired network settings under **Edit Devices** or under **Edit DNS** configuration, then click **Save & Quit**. To abort any changes, click **Quit**.

Changing the Virtual Appliance Password

The virtual appliance password is changed in the vSphere Web Client using the Console.

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machines that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** > **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. On the Console, use the arrow keys to select **Change Admin Password** and press **<ENTER>**.
5. Enter the **Current Admin Password** and press **<ENTER>**.
   Admin passwords include one special character, one number, one uppercase, one lowercase, and at least 8 letters.
6. Enter a new password for **Enter new Admin Password** and press **<ENTER>**.
7. Type the new password again in **Please Confirm Admin Password** text box , and then press **<ENTER>**.

Setting The Local Time Zone

To set up the local time zone

1. Click the Console tab in the main VMware vCenter window to initiate the Administration Console.
2. Allow the OMIVV to finish booting up and then enter the user name as admin and press **Enter**.
3. Enter a new admin password. The password must be set as per the password complexity rules displayed. Press **Enter** **Password confirmation** dialog box is displayed.
4. Enter the password that was provided earlier and press **Enter**.
   Password Set confirmation message is displayed.
5. Press **Enter** to configure the network and time zone information in the OMIVV appliance.
6. To configure the OpenManage Integration for VMware vCenter time zone information, click on Date/Time Properties to set the time zone and date.
7. In the **Date and Time** tab, select the **Synchronize date and time over the network**.
   The **NTP Servers** window is displayed
8. Click on **Time Zone**, and select the applicable time zone and click **OK**.

Rebooting Virtual Appliance

To reboot the virtual appliance:

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** > **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. Use the arrow keys to select **Reboot this Virtual Appliance** and press **<ENTER>**.

5. The following message is displayed:

```
If there are any processes running on this appliance they will be terminated by this
action. Are you sure you wish to do this?
```

6. Enter **y** to reboot or **n** to cancel. The appliance is rebooted.

Resetting The Virtual Appliance To Factory Settings

To reset the virtual appliance to factory settings:

1. In vSphere Web Client, in the Navigator, select **vCenter**.
2. In the Navigator, select the Virtual Machine that you want to manage.
3. Do one of the following:
   - On the Object tab, select **Action** > **Open Console**.
   - Right-click the virtual machine that you selected and select **Open Console**.
4. Use the arrow keys to select **Reset this Virtual Appliance to Factory Settings** and press **<ENTER>**.
5. The following notice is displayed:

```
This operation is completely Irreversible if you continue you will completely reset
*this* appliance to its original settings. All changes you have made to this
appliance will be Lost. Are you sure you wish to Reset this Appliance to Factory
Settings?
```

6. Enter **y** to reset or **n** to cancel. The appliance is reset to the original factory settings and all the others settings and saved data will be lost.

   NOTE: When the virtual appliance is reset to factory settings, any updates made to the Network Configuration are preserved; these settings are not reset.

Refreshing the Console View

To refresh the Console view, select **Refresh** and press **<ENTER>**.

Logging out from the console

To log out from the console, click **Log out** in the top right corner against your logged-in account.

Read-only User Role

There is an unprivileged user role called readonly with shell access for diagnostic purposes. The read-only user has limited privileges to run the mount. The readonly user's password is set as **readonly**. The readonly user's password has changed from admin password (for OMIVV v1.0 to v3.2) for security purposes.

Upgrading OMIVV from existing version to current version

1. To open Administration Console, in the **Help and Support** tab of OpenManage Integration for VMware vCenter, click the link under **Administration Console** or start a web browser and provide the `https:\\<ApplianceIP|hostname>` url.
2. In the **Login** dialog box, type the password.
3. In Administration Console, in the left pane, click **APPLIANCE MANAGEMENT**.
4. In the **APPLIANCE MANAGEMENT** page, depending on your network settings, enable proxy and provide proxy settings if your network needs proxy.
5. To upgrade the OpenManage Integration plug in from an existing version to the current version, perform one of the following steps:

- Ensure that **Update Repository Path** is set to the path: http://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 `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest` in the **Update Repository Path** text box. To save, click **Apply**.
- If there is no internet connectivity, download all the files and folders from the `http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/` path and copy them to an HTTP share. In the **Appliance Management** window, in the **APPLIANCE UPDATE** section, click **Edit**, and then in the **Update Repository Path** text box, include the path to the offline HTTP share, and click **Apply**.

6. Compare the available virtual appliance version and current virtual appliance version and ensure that the available virtual appliance version is greater than the current virtual appliance version.
7. To apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
8. In the **UPDATE APPLIANCE** dialog box, click **Update**.
   After you click **Update**, you are logged off from the **ADMINISTRATION CONSOLE** window.
9. Close the web browser.

NOTE: Once the RPM upgrade is complete, you can view the login screen in the OMIVV console. Open a browser and provide the following link:`https:\\<ApplianceIP/hostname>\DellAdminPortal` and navigate to the **APPLIANCE UPDATE** area. You can verify that the available and current virtual appliance versions are same.

NOTE:

Migrating from 2.x to 3.2

You can start with a fresh deployment of the v3.2 OVF after uninstalling the old version and then migrate the data from older version (2.x) to 3.2 version by using backup and restore path.

To migrate from an older version to the OMIVV 3.2 version, perform the following steps:

1. Take a backup of the database for the older (v2.x) release.
   For more information, see *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals`.
2. Power off the older appliance from vCenter.
   NOTE: Do not unregister the OMIVV plug-in from vCenter. Unregistering the plug-in from vCenter removes all the alarms registered on vCenter by the OMIVV plug-in and all the customization that is performed on the alarms such as, actions and so on. For more information, see *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2* if you have unregistered the plug-in after the backup.
3. Deploy the new OpenManage Integration version 3.2 OVF.
   For more information on deploying the OVF, see *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2*.
4. Power on the OpenManage Integration version 3.2 appliance.
5. Set up the network and time zone on the appliance.
   Ensure that the new OpenManage Integration version 3.2 appliance has the same IP address as the old appliance. To set up the network details, see *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2*.
   NOTE: The OMIVV plug-in might not work properly if the IP address for the OMIVV 3.2 appliance is different from the IP address of the older appliance. In such a scenario, unregister and re-register all the vCenter instances.
6. Restore the database to the new OMIVV appliance.
   NOTE: If you have enabled Proactive HA on clusters, OMIVV unregisters the Dell Inc provider for those clusters and re-registers the Dell Inc provider after restore. Hence, health updates for the Dell hosts are not available until restore is complete.
   For more information, see **Restoring the OMIVV database from a backup** in the *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals`.
7. Upload the new license file.
   For more information, see *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2*.

8. Verify the appliance.

   For more information, see the *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2* to ensure that the database migration is successful.

9. Run the **Inventory** on all the hosts.

   NOTE:

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

   If the IP address of the new OMIVV version 3.2 appliance is changed from the old appliance, configure the trap destination for the SNMP traps to point to the new appliance. For 12th generation and higher generation servers, the IP change is fixed by running inventory on these hosts. For hosts earlier than 12th generation that were compliant with earlier versions, the IP change is displayed as noncompliant and requires you to configure Dell EMC OpenManage Server Administrator (OMSA). For more information on fixing the host compliance, see **Reporting and fixing compliance for vSphere hosts** in *OpenManage Integration for VMware vCenter User's Guide* available at `Dell.com/support/manuals`.

7

Settings

The Settings tab is used to do the following:

- Viewing Warranty Expiration Notification Settings
- Configuring Warranty Expiration Notification
- Setting Up The Firmware Update Repository
- Viewing the Alarm and Event Settings
- Configuring and Managing Events and Alarms
- Viewing and Configuring the Data Retrieval Schedules for Inventory and Warranty

Topics:

Editing the OMSA Link

This procedure assumes that you have already installed an OMSA Web Server and that you have previously configured this link using the Initial Configuration Wizard. See the *OpenManage Server Administrator Installation Guide* for the version of OMSA in use and for instructions on how to install and configure the Web Server.

If you have not provided a link while running the Configuration Wizard, you can edit this link in OpenManage Integration for VMware vCenter **Manage** > **Settings** tab. This is not applicable for Web Client.

NOTE: OMSA is only required on Dell PowerEdge 11th generation servers or earlier. Web Client Initial Configuration wizard does not have an option to provide the OMSA link. The OMSA link is applicable only for .net client.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under vCenter Settings and to the right side of the OMSA Web Server URL, click **Edit**.
2. In the OMSA Web Server URL dialog box, type the **URL**.
   You must include the full URL including the HTTPS.
3. Select **Apply these settings to all vCenters** check box to apply the OMSA URL to all vCenters. If you do not select this check box, the OMSA URL is applied only to only one vCenter.
4. Verify that the link works by navigating to the host Summary tab for this host. Verify that the OMSA Console link is live within the Dell Host Information.

Understanding Using OMSA with 11th Generation Servers

On servers earlier than Dell PowerEdge 12th generation servers, you must install OMSA to work with the OpenManage Integration for VMware vCenter. You can install OMSA automatically on Dell PowerEdge 11th generation hosts during deployment, or if you want to install it manually, you may still do so.

To configure OMSA on Dell PowerEdge 11th generation hosts, choose from the following:

- Deploying the OMSA Agent onto an ESXi System
- Setting up an OMSA Trap Destination

NOTE: Apart from the above options, you can use the .Net client and run Host Compliance, which can install and configure the OMSA Agent.

Deploying The OMSA Agent Onto An ESXi System

Install the OMSA VIB on an ESXi system to gather inventory and alert information from the systems.

NOTE: OpenManage agents are required on Dell hosts earlier than Dell PowerEdge 12th generation servers. Install OMSA using the OpenManage Integration for VMware vCenter or install manually to hosts prior to installing the OpenManage Integration for VMware vCenter. Details on manually installing the agents are at **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. If not already installed, install the vSphere command line tool (vSphere CLI) from **http://www.vmware.com**.
2. Enter the following command:

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

NOTE: It can take a few minutes for OMSA to install. This command requires a reboot of the host after it completes.

Setting Up An OMSA Trap Destination

This task is only for host systems using OMSA for event generation instead of iDRAC6. There is no additional configuration required for iDRAC6.

NOTE: OMSA is only required on Dell servers earlier than version Dell PowerEdge 12th generation servers.

1. Either use the link to the OMSA user interface found in the OpenManage Integration for VMware vCenter **Manage** > **Settings** tab, or navigate to the OMSA agent from a Web browser (**https://<HostIP>:1311/**).
2. Log in to the interface, and select the **Alert Management** tab.
3. Select **Alert Actions** and make sure that any events to be monitored have the **Broadcast Message** option set, so that the events are sent out.
4. At the top of the tab, select the **Platform Events** option.
5. Click the grey **Configure Destinations** button, and click the **Destination** link.
6. Select the **Enable Destination** check box.
7. Enter the OpenManage Integration for VMware vCenter appliance IP address in the **Destination IP Address** field.
8. Click **Apply Changes**.
9. Repeat step 1 to step 8 to configure additional events.

Viewing Warranty Expiration Notification Settings

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under Appliance Settings, click **Warranty Expiration Notification**.
2. Under Warranty Expiration Notification you can view the following:
   - Whether the setting is enabled or disabled
   - The number of days for the first Warning setting.
   - The number of days for the Critical warning setting.
3. To configure Warranty Expiration Notification, see Configuring Warranty Expiration Notifications.

Configuring Warranty Expiration Notification

You can configure warranty expiration thresholds to warn about warranty expiration.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under Appliance Settings, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.

2. In the Warranty Expiration Notification dialog box, do the following:
   a. If you want to enable this setting, select the **Enable warranty expiration notification for hosts** check box. Selecting the check box enables warranty expiration notification.
   b. Under Minimum Days Threshold Alert, do the following:
      i. In the Warning drop-down list, select the number of days before you want to be warned of the warranty expiration.
      ii. In the Critical drop-down list, select the number of days before you want to be warned of the warranty expiration.
3. Click **Apply**.

Configuring Events And Alarms

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

NOTE: OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later. For hosts prior to 12th generation, OMIVV supports SNMP v1 alerts in vCenter. For more information on setting trap destination, see Setting Up An OMSA Trap Destination.

NOTE: To receive Dell events, you must enable both alarms and events.

1. To the right side of Events and Alarms, click the **Edit** icon.
2. To enable all hardware alarms and events, select the **Enable Alarms for all Dell Hosts** check box.

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

3. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**. It may take up to a minute before the change takes effect.

   NOTE: This step is only seen if Enable Alarms For Dell Hosts is selected.

4. Under **Event Posting Level**, select one of the following:
   - Do not post any events

     This options blocks hardware events.
   - Post All Events

     This option posts all hardware events.
   - Post only Critical and Warning Events

     This option posts only critical or warning level hardware events.
   - Post only Virtualization-Related Critical and Warning Events

     This option posts only virtualization-related critical and warning events. This is the default event posting level.
5. If you want to apply these settings to all vCenters, select the **Apply these settings to all vCenters** check box.

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

   This option is grayed out if you already selected All Registered vCenters from the drop-down list on the Setting page.
6. To save, click **Apply**.

Viewing the Alarm and Event Settings

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

1. In the **OpenManage Integration for VMware vCenter** > **Manage** > **Settings** tab, under vCenter Settings, expand Events and Alarms.
2. Under Events and Alarms you can view the following:
   - vCenter Alarms for Dell Hosts: Displays either Enabled or Disabled.
   - Event Posting Level

     To see the event posting levels that can display, see Understanding Alarms and Events.
3. To configure alarms and events, see Configuring Events and Alarms

Viewing Events

Configure events before you can view them in the Events tab, see Configuring Events and Alarms.

View the events for a host, cluster or datacenter on the Events tab.

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

About Firmware Updates

The location where servers receive firmware updates is a global setting that is available in the OpenManage Integration for VMware vCenter on the Settings tab.

Firmware repository settings contain the firmware catalog location used to update deployed servers. There are two location types:

Dell (ftp.dell.com)	Uses the firmware update repository of Dell (**ftp.dell.com**). The OpenManage Integration for VMware vCenter downloads selected firmware updates from Dell repository.
Shared Network Folder	Created with Dell Repository Manager™. These local repositories are on CIFS or NFS file share.

NOTE: Once the repository is created, save it to a location that the registered hosts can access. Repository passwords cannot exceed 31 characters. Do not use any of the following characters in a password: @, &, %, ', ", ,(comma), <, >

The Firmware Update Wizard always checks for the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller, and attempts to update them to required minimum versions. Once iDRAC, Lifecycle Controller, and BIOS firmware versions meet minimum requirements, the Firmware Update wizard allows updates for all firmware including: iDRAC, Lifecycle Controller, RAID, NIC/LOM, Power Supply, BIOS, and so on.

Related Information:

- Setting Up the Firmware Update Repository on page 50

Setting Up the Firmware Update Repository

You can set up the firmware update repository on the OpenManage Integration for VMware vCenter Settings tab.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings** and to the right side of Firmware Update Repository, click the **Edit** icon.
2. In the Firmware Update Repository dialog box, select one of the following:
   - Dell Online

Default firmware repository (http://downloads.dell.com/published/Pages/index.html) with a staging folder. The OpenManage Integration for VMware vCenter downloads selected firmware updates and stores them in the staging folder, and then you need to run the firmware wizard to update the firmware.

- Shared Network Folder

  These are created with the Dell Repository Manager application. Locate these local repositories on Windows-based file shares. Use the live link to go to Dell Repository Manager.

3. If you selected **Shared Network Folder**, do the following:
   a. Enter the **Catalog File Location** using the following format:
      - NFS share for xml file: host:/share/filename.xml
      - NFS share for gz file: host:/share/filename.gz
      - CIFS share for xml file: \\host\share\filename.xml
      - CIFS share for gz file: \\host\share\filename.gz

   b. If the downloading of the files are in progress in the selected repository path which is displayed in the **Select Update Source** screen, an error message is displayed notifying that the download is in progress.
4. When the downloading of file is completed, click **Apply**.

Running The Firmware Update Wizard for a Single Host

This functionality is only available for 11th, 12th, and 13th generation Dell servers that have either an iDRAC Express or Enterprise card.

NOTE: To safeguard against browser timeout issues, change the default timeout to 30 seconds. For information on changing the default timeout setting, see How Come I see an Error Message Displayed After Clicking the Firmware Update Link in the Troubleshooting section of the *User's Guide*.

NOTE: To access the Firmware wizard, perform either of the following:

- Right-click **Host** > **All OpenManage Integration Actions** > **Firmware Update**.
- Click **Host** > **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
- Click **Host** > **Summary** > **Dell Host Information** > **Firmware Update**.

To run the Firmware Update Wizard:

1. In the **vSphere Web Client** click **Hosts**. A list of available hosts are displayed.
2. Select a host from the displayed list.
3. In the main menu, click **Monitor** and then select the **Dell Host Information** tab. The inventory information of the Dell Hosts is displayed.
4. Click **Firmware**, the available firmware with the details are displayed.
5. Click **Run Firmware Wizard**. The **Firmware Update** screen is displayed.
6. Click **Next**, the **Select Update Source** screen is displayed with the firmware update bundle for the given host is displayed. In the screen, select the firmware update bundle from the **Select an Update Bundle** drop-down list.

   NOTE:
   - 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.
   - 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.

7. Click **Next**. The **Select Components** screen is displayed which lists the firmware details for the components.
8. Select the desired firmware updates and click **Next**. The components that are either a downgrade or currently scheduled for update are not selectable. If you select the **Allow Firmware downgrade** check box, select the options that are listed as Downgrade. Selecting this option is only recommended to advanced users who understand the implications of downgrading firmware.
9. Click **Next.** The **Schedule Firmware Update** screen is displayed.
   - Enter the job name in the **Firmware Update Job Name** field and description in the **Firmware Update Description** field. This field entry is optional.
   - Select **Update Now** to start the firmware update job immediately.
   - **Schedule Update** button, select this radio button to run the firmware update job later and click **Next**. You can schedule the firmware update job after 30 minutes from the current time.

- In the Calendar box, select the month and day.
- In the Time text box, type the time in HH:MM, and then click Next. The time is the local time zone where your client is physically located. Invalid time values result in a blocked update.
- **Apply updates on next reboot.**

  To avoid a service interruption, it is recommended that the host enters maintenance mode before the reboot.
- **Apply updates and force reboot without entering maintenance mode.**

  The update is applied, and a reboot occurs even if the host is not in maintenance mode. This method is not recommended.

10. Click **Next**. The **Summary** page is displayed that provides details about all components after firmware update.
11. Click **Finish**.
12. To verify that the update was successful, in **Monitor** tab, select **Job Queue** > **Firmware Updates**, and review the **OpenManage Integration Overview** page to see the new versions.

Running the Update Firmware Wizard for a Cluster

This functionality is only available for 11th, 12th, and 13th generation Dell servers that have either an iDRAC Express or Enterprise card. If your firmware was installed on or after October 14th, 2010, you can automatically update your firmware versions using the Firmware Update Wizard. This wizard only updates hosts that are part of a connection profile and compliant in terms of firmware, CSIOR status, hypervisor, and OMSA status (11th generation servers only). Select a cluster that is listed in the Clusters view and use the Firmware Update Wizard. It typically takes from 30 to 60 minutes to update firmware components for each cluster. Enable DRS on a cluster so that virtual machines can be migrated when a host enters/exits maintenance mode during the firmware update process. You can only schedule or run one firmware update task at a time.

If you want to export from the wizard, use the **Export to CSV** button. Search is available for locating a specific cluster, datacenter, host, or any topic item from the datagrid except for Date Applied.

NOTE: VMware recommends clusters to be built with identical server hardware. For the firmware update at a cluster level with the number of hosts near the limits for a cluster (recommended by VMware) or composed of different models of Dell servers, usage of vSphere web client is recommended.

NOTE: For information on changing the default timeout setting, see the Troubleshooting section of the *User's Guide*.

You can view the status and manage Firmware update jobs from the **Job Queue** page. See, Viewing Firmware Details for Datacenters and Clusters.

1. Click **OpenManage Integration** icon, click **Clusters** that is displayed in the left pane. The list of clusters are displayed.
2. Click a cluster from the displayed list. The main menu is displayed with different options.
3. Click **Monitor** -->**Dell Cluster Information** -->**Firmware**. The **Run Firmware Wizard** screen is displayed.
4. Click **Run Firmware Wizard** link. The **Welcome** page is displayed.
5. Click **Next**. The **Select Update Source** screen is displayed where you can select the bundles. The Repository location is also displayed.
6. Select host from the displayed list in the **Select Bundles** area. You should select at least one bundle for firmware update. Each host has a drop-down list next to the host name from which you can select the required bundle.

   NOTE:
   - 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.
   - 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.
7. Click **Next**. The **Select Components** screen is displayed. This screen displays the details of components such as, model name, host name, service tag, component, and so on for the selected host.
8. Select at least one component from the list, and click **Next** to proceed. You can filter the content of the component data grid using the **Filter** field or, drag and drop columns within the component data grid. If you select the **Allow Firmware downgrade** check box, the existing firmware version rolls back to the previous available version.
9. Click **Next**, the **Schedule Firmware Update** screen is displayed.
   a. Enter the firmware update job name in the **Firmware Update Job Name** field. This value is mandatory.
   b. Enter the firmware update description in the **Firmware Update Description** field. This value is optional.
10. Select an option from the following.

a. **Update Now**, select this radio button to run the firmware update job now and click **Next**.
b. **Schedule Update** button, select this radio button to run the firmware update job later and click **Next**. You can schedule the firmware update job after 30 minutes from the current time.
c. In the **Calendar** box, select the month and day.
d. In the **Time** text box, type the time in HH:MM, and then click **Next**. The time is the local timezone where your client is physically located. Any invalid time values result in a blocked update.

11. The **Summary** screen is displayed with all the firmware update details.
12. Click **Finish** and the message, The **firmware update job has been created** for successful firmware update is displayed.

Viewing Firmware Update Status for Clusters and Datacenters

For information to display on this page, run or schedule a firmware update for a cluster or a host.

On this page you can refresh, purge, or abort your firmware update jobs.

1. From the OpenManage Integration, select **Monitor** > **Job Queue** > **Firmware Updates**.
2. To display the most recent information, click **Refresh**.
3. View the status in the datagrid. This grid offers the following information about firmware update jobs:
   - Status
   - Scheduled Time
   - Name
   - Description
   - vCenter
   - Collection Size

     The collection size is the number of servers on this firmware inventory job.
   - Progress Summary

     The progress summary lists the progress details of this firmware update.
4. To see more details about a particular job, in the datagrid for a particular job, click on a item of master datagrid. The details are displayed in the details datagrid.

   Here you can find the following details:
   - Host Name
   - Status
   - Start Time
   - End Time
5. If you want to abort a scheduled firmware update that is not running, click **Abort**.
6. If you want to modify a scheduled job click on **Modify**.
7. If you want to purge scheduled firmware updates, click **Purge Job Queue**.
   You can only purge jobs that are completed successfully or failed or else cancelled.
8. Select the **Older than date and job Status**, and click **Apply**. The selected jobs are then clear it from the queue.

Viewing the Data Retrieval Schedules for Inventory and Warranty

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **vCenter Settings**, click **Data Retrieval Schedule**.
   Clicking Data Retrieval Schedule expands to expose the schedules for inventory and warranty.
2. For either Inventory or Warranty Retrieval, view the settings:
   - Shows whether the option is enabled or disabled

- Displays the weekdays for which it is enabled.
- Displays the time of day it is enabled.

3. If you click **Data Retrieval Schedule** again, it rolls up the information into a single line and displays whether the option is enabled or disabled.
4. If you want to edit the Data Retrieval Schedule, see Modifying Inventory Job Schedules or Modifying a Warranty Job Schedule.

Understanding Using OMSA with 11th Generation Servers

On servers earlier than Dell PowerEdge 12th generation servers, you must install OMSA to work with the OpenManage Integration for VMware vCenter. You can install OMSA automatically on Dell PowerEdge 11th generation hosts during deployment, or if you want to install it manually, you may still do so.

To configure OMSA on Dell PowerEdge 11th generation hosts, choose from the following:

- Deploying the OMSA Agent onto an ESXi System
- Setting up an OMSA Trap Destination

NOTE: Apart from the above options, you can use the .Net client and run Host Compliance, which can install and configure the OMSA Agent.

Deploying The OMSA Agent Onto An ESXi System

Install the OMSA VIB on an ESXi system to gather inventory and alert information from the systems.

NOTE: OpenManage agents are required on Dell hosts earlier than Dell PowerEdge 12th generation servers. Install OMSA using the OpenManage Integration for VMware vCenter or install manually to hosts prior to installing the OpenManage Integration for VMware vCenter. Details on manually installing the agents are at **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. If not already installed, install the vSphere command line tool (vSphere CLI) from **http://www.vmware.com**.
2. Enter the following command:

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b <OMSA version X.X>
```

NOTE: It can take a few minutes for OMSA to install. This command requires a reboot of the host after it completes.

Setting Up An OMSA Trap Destination

This task is only for host systems using OMSA for event generation instead of iDRAC6. There is no additional configuration required for iDRAC6.

NOTE: OMSA is only required on Dell servers earlier than version Dell PowerEdge 12th generation servers.

1. Either use the link to the OMSA user interface found in the OpenManage Integration for VMware vCenter **Manage** > **Settings** tab, or navigate to the OMSA agent from a Web browser (**https://<HostIP>:1311/**).
2. Log in to the interface, and select the **Alert Management** tab.
3. Select **Alert Actions** and make sure that any events to be monitored have the **Broadcast Message** option set, so that the events are sent out.
4. At the top of the tab, select the **Platform Events** option.
5. Click the grey **Configure Destinations** button, and click the **Destination** link.
6. Select the **Enable Destination** check box.
7. Enter the OpenManage Integration for VMware vCenter appliance IP address in the **Destination IP Address** field.

8. Click **Apply Changes**.
9. Repeat step 1 to step 8 to configure additional events.

8

Viewing Warranty Expiration Notification Settings

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under Appliance Settings, click **Warranty Expiration Notification**.
2. Under Warranty Expiration Notification you can view the following:
   - Whether the setting is enabled or disabled
   - The number of days for the first Warning setting.
   - The number of days for the Critical warning setting.
3. To configure Warranty Expiration Notification, see Configuring Warranty Expiration Notifications.

Topics:

Configuring Warranty Expiration Notification

You can configure warranty expiration thresholds to warn about warranty expiration.

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under Appliance Settings, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.
2. In the Warranty Expiration Notification dialog box, do the following:
   a. If you want to enable this setting, select the **Enable warranty expiration notification for hosts** check box. Selecting the check box enables warranty expiration notification.
   b. Under Minimum Days Threshold Alert, do the following:
      i. In the Warning drop-down list, select the number of days before you want to be warned of the warranty expiration.
      ii. In the Critical drop-down list, select the number of days before you want to be warned of the warranty expiration.
3. Click **Apply**.

9

About Firmware Updates

The location where servers receive firmware updates is a global setting that is available in the OpenManage Integration for VMware vCenter on the Settings tab.

Firmware repository settings contain the firmware catalog location used to update deployed servers. There are two location types:

Dell (ftp.dell.com)	Uses the firmware update repository of Dell (**ftp.dell.com**). The OpenManage Integration for VMware vCenter downloads selected firmware updates from Dell repository.
Shared Network Folder	Created with Dell Repository Manager™. These local repositories are on CIFS or NFS file share.

NOTE: Once the repository is created, save it to a location that the registered hosts can access. Repository passwords cannot exceed 31 characters. Do not use any of the following characters in a password: @, &, %, ', ", ,(comma), <, >

The Firmware Update Wizard always checks for the minimum firmware levels for iDRAC, BIOS, and Lifecycle Controller, and attempts to update them to required minimum versions. Once iDRAC, Lifecycle Controller, and BIOS firmware versions meet minimum requirements, the Firmware Update wizard allows updates for all firmware including: iDRAC, Lifecycle Controller, RAID, NIC/LOM, Power Supply, BIOS, and so on.

Related Information:

- Setting Up the Firmware Update Repository on page 50

Topics:

Setting Up the Firmware Update Repository

You can set up the firmware update repository on the OpenManage Integration for VMware vCenter Settings tab.

1. In OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **Appliance Settings** and to the right side of Firmware Update Repository, click the **Edit** icon.
2. In the Firmware Update Repository dialog box, select one of the following:
   - Dell Online

     Default firmware repository (http://downloads.dell.com/published/Pages/index.html) with a staging folder. The OpenManage Integration for VMware vCenter downloads selected firmware updates and stores them in the staging folder, and then you need to run the firmware wizard to update the firmware.

   - Shared Network Folder

     These are created with the Dell Repository Manager application. Locate these local repositories on Windows-based file shares. Use the live link to go to Dell Repository Manager.

3. If you selected **Shared Network Folder**, do the following:
   a. Enter the **Catalog File Location** using the following format:
      - NFS share for xml file: host:/share/filename.xml
      - NFS share for gz file: host:/share/filename.gz
      - CIFS share for xml file: \\host\share\filename.xml
      - CIFS share for gz file: \\host\share\filename.gz

   b. If the downloading of the files are in progress in the selected repository path which is displayed in the **Select Update Source** screen, an error message is displayed notifying that the download is in progress.

4. When the downloading of file is completed, click **Apply**.

Running The Firmware Update Wizard for a Single Host

This functionality is only available for 11th, 12th, and 13th generation Dell servers that have either an iDRAC Express or Enterprise card.

NOTE: To safeguard against browser timeout issues, change the default timeout to 30 seconds. For information on changing the default timeout setting, see How Come I see an Error Message Displayed After Clicking the Firmware Update Link in the Troubleshooting section of the *User's Guide*.

NOTE: To access the Firmware wizard, perform either of the following:

- Right-click **Host** > **All OpenManage Integration Actions** > **Firmware Update**.
- Click **Host** > **Actions** > **All OpenManage Integration Actions** > **Firmware Update**.
- Click **Host** > **Summary** > **Dell Host Information** > **Firmware Update**.

To run the Firmware Update Wizard:

1. In the **vSphere Web Client** click **Hosts**. A list of available hosts are displayed.
2. Select a host from the displayed list.
3. In the main menu, click **Monitor** and then select the **Dell Host Information** tab. The inventory information of the Dell Hosts is displayed.
4. Click **Firmware**, the available firmware with the details are displayed.
5. Click **Run Firmware Wizard**. The **Firmware Update** screen is displayed.
6. Click **Next**, the **Select Update Source** screen is displayed with the firmware update bundle for the given host is displayed. In the screen, select the firmware update bundle from the **Select an Update Bundle** drop-down list.

   NOTE:
   - 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.
   - 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.

7. Click **Next**. The **Select Components** screen is displayed which lists the firmware details for the components.
8. Select the desired firmware updates and click **Next**. The components that are either a downgrade or currently scheduled for update are not selectable. If you select the **Allow Firmware downgrade** check box, select the options that are listed as Downgrade. Selecting this option is only recommended to advanced users who understand the implications of downgrading firmware.
9. Click **Next.** The **Schedule Firmware Update** screen is displayed.
   - Enter the job name in the **Firmware Update Job Name** field and description in the **Firmware Update Description** field. This field entry is optional.
   - Select **Update Now** to start the firmware update job immediately.
   - **Schedule Update** button, select this radio button to run the firmware update job later and click **Next**. You can schedule the firmware update job after 30 minutes from the current time.
   - In the Calendar box, select the month and day.
   - In the Time text box, type the time in HH:MM, and then click Next. The time is the local time zone where your client is physically located. Invalid time values result in a blocked update.
   - **Apply updates on next reboot.**

     To avoid a service interruption, it is recommended that the host enters maintenance mode before the reboot.
   - **Apply updates and force reboot without entering maintenance mode.**

     The update is applied, and a reboot occurs even if the host is not in maintenance mode. This method is not recommended.
10. Click **Next**. The **Summary** page is displayed that provides details about all components after firmware update.
11. Click **Finish**.
12. To verify that the update was successful, in **Monitor** tab, select **Job Queue** > **Firmware Updates**, and review the **OpenManage Integration Overview** page to see the new versions.

Running the Update Firmware Wizard for a Cluster

This functionality is only available for 11th, 12th, and 13th generation Dell servers that have either an iDRAC Express or Enterprise card. If your firmware was installed on or after October 14th, 2010, you can automatically update your firmware versions using the Firmware Update Wizard. This wizard only updates hosts that are part of a connection profile and compliant in terms of firmware, CSIOR status, hypervisor, and OMSA status (11th generation servers only). Select a cluster that is listed in the Clusters view and use the Firmware Update Wizard. It typically takes from 30 to 60 minutes to update firmware components for each cluster. Enable DRS on a cluster so that virtual machines can be migrated when a host enters/exits maintenance mode during the firmware update process. You can only schedule or run one firmware update task at a time.

If you want to export from the wizard, use the **Export to CSV** button. Search is available for locating a specific cluster, datacenter, host, or any topic item from the datagrid except for Date Applied.

NOTE: VMware recommends clusters to be built with identical server hardware. For the firmware update at a cluster level with the number of hosts near the limits for a cluster (recommended by VMware) or composed of different models of Dell servers, usage of vSphere web client is recommended.

NOTE: For information on changing the default timeout setting, see the Troubleshooting section of the *User's Guide*.

You can view the status and manage Firmware update jobs from the **Job Queue** page. See, Viewing Firmware Details for Datacenters and Clusters.

1. Click **OpenManage Integration** icon, click **Clusters** that is displayed in the left pane. The list of clusters are displayed.
2. Click a cluster from the displayed list. The main menu is displayed with different options.
3. Click **Monitor** -->**Dell Cluster Information** -->**Firmware**. The **Run Firmware Wizard** screen is displayed.
4. Click **Run Firmware Wizard** link. The **Welcome** page is displayed.
5. Click **Next**. The **Select Update Source** screen is displayed where you can select the bundles. The Repository location is also displayed.
6. Select host from the displayed list in the **Select Bundles** area. You should select at least one bundle for firmware update. Each host has a drop-down list next to the host name from which you can select the required bundle.

   NOTE:
   - 64-bit bundles are not supported for 12th generation hosts with iDRAC version 1.51 and earlier.
   - 64-bit bundles are not supported for 11th generation hosts on all iDRAC versions.

7. Click **Next**. The **Select Components** screen is displayed. This screen displays the details of components such as, model name, host name, service tag, component, and so on for the selected host.
8. Select at least one component from the list, and click **Next** to proceed. You can filter the content of the component data grid using the **Filter** field or, drag and drop columns within the component data grid. If you select the **Allow Firmware downgrade** check box, the existing firmware version rolls back to the previous available version.
9. Click **Next**, the **Schedule Firmware Update** screen is displayed.
   a. Enter the firmware update job name in the **Firmware Update Job Name** field. This value is mandatory.
   b. Enter the firmware update description in the **Firmware Update Description** field. This value is optional.
10. Select an option from the following.
    a. **Update Now**, select this radio button to run the firmware update job now and click **Next**.
    b. **Schedule Update** button, select this radio button to run the firmware update job later and click **Next**. You can schedule the firmware update job after 30 minutes from the current time.
    c. In the **Calendar** box, select the month and day.
    d. In the **Time** text box, type the time in HH:MM, and then click **Next**. The time is the local timezone where your client is physically located. Any invalid time values result in a blocked update.
11. The **Summary** screen is displayed with all the firmware update details.
12. Click **Finish** and the message, The **firmware update job has been created** for successful firmware update is displayed.

10

Understanding Events And Alarms for Hosts

You can edit events and alarms settings from the OpenManage Integration for VMware vCenter within **Manage** > **Settings** tab. From here you can select the Event Posting Level, enable Alarms for Dell Hosts, or Restore Default Alarms. You can configure events and alarms for each vCenter or all at once for all registered vCenters.

There are four event posting levels.

Table 5. Event Posting Level Descriptions

Event	Description
Do not post any Events	Do not have the OpenManage Integration for VMware vCenter forward any events or alerts into related vCenters.
Post all Events	Post all events, including informal events, that the OpenManage Integration for VMware vCenter receives from managed Dell hosts into related vCenters.
Post only Critical and Warning Events	Posts only events with either Critical or Warning criticality into related vCenters.
Post only Virtualization-Related Critical and Warning Events	Post Virtualization related events received from hosts into related vCenters. Virtualization related events are those that Dell has selected to be most critical to hosts running virtual machines.

When you configure your events and alarms, you can enable them. When enabled, critical hardware alarms can trigger the OpenManage Integration for VMware vCenter to put the host system into a maintenance mode, and in certain cases, migrate the virtual machines to another host system. The OpenManage Integration for VMware vCenter forwards events received from managed Dell hosts, and creates alarms for those events. Use these alarms to trigger actions from vCenter, like a reboot, maintenance mode, or migrate. For example, when a dual power supply fails and an alarm is created, the resulting action is to migrate the virtual machine on that machine to a new one.

A host enters or leaves maintenance mode only as when you request it. If the host is in a cluster when it enters maintenance mode, you are given the option to evacuate powered-off virtual machines. If this option is selected, each powered-off virtual machine is migrated to another host, unless there is no compatible host available for the virtual machine in the cluster. While in maintenance mode, the host does not allow deployment or *power-on* of a virtual machine. Virtual machines that are running on a host entering maintenance mode need to be either migrated to another host or shut down, either manually or automatically by VMware Distributed Resource Scheduling (DRS).

Any hosts outside of clusters, or in clusters without VMware Distributed Resource Scheduling (DRS) enabled, could see virtual machines being shut down due to a critical event. DRS continuously monitors usage across a resource pool and intelligently allocates available resources among virtual machines according to business needs. Use clusters with DRS configured in conjunction with Dell Alarms to make sure that virtual machines are automatically migrated on critical hardware events. Listed in the details of the on screen message are any clusters on this vCenter instance that may be impacted. Confirm that the clusters are impacted before enabling Events and Alarms.

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

NOTE: The OpenManage Integration for VMware vCenter pre-selects the virtualization-related events that are the essential to hosts successfully running virtual machines. Dell host alarms are disabled by default. If Dell alarms are enabled, the clusters should use the VMware Distributed Resource Scheduler to make sure that the virtual machines that send critical events are automatically migrated.

Topics:

Understanding Events And Alarms for Chassis

Events and alarms corresponding to a chassis are shown only at the vCenter level. Events and alarms settings that are done for hosts at every vCenter is also applicable at chassis level.. You can edit events and alarms settings from the OpenManage Integration for VMware vCenter within **Manage** > **Settings** tab. From here you can select the Event Posting Level, enable Alarms for Dell Hosts and Chassis, or Restore Default Alarms. You can configure events and alarms for each vCenter or all at once for all registered vCenters.

NOTE: To receive Dell events, you must enable both alarms and events.

Viewing Chassis Events

1. In the left pane select vCenter, click on vCenter Servers
2. Click on a specific vCenter.
3. On the Monitor tab, click Events.
4. To view more event details, select a specific event.

Viewing Chassis Alarms

1. In the left pane select vCenter, click on vCenter Servers
2. Click on a specific vCenter.
3. The alarms are displayed. Only the first 4 alarms are displayed. Click on Show All and the detailed list are displayed in the Monitor tab as All Issues.
4. Click on the Alarm in **Triggered Alarms** to view the Alarm Definition.

Configuring Events And Alarms

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

NOTE: OMIVV supports SNMP v1 and v2 alerts for 12th generation hosts and later. For hosts prior to 12th generation, OMIVV supports SNMP v1 alerts in vCenter. For more information on setting trap destination, see Setting Up An OMSA Trap Destination.

NOTE: To receive Dell events, you must enable both alarms and events.

1. To the right side of Events and Alarms, click the **Edit** icon.
2. To enable all hardware alarms and events, select the **Enable Alarms for all Dell Hosts** check box.

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

3. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**.
   It may take up to a minute before the change takes effect.

   NOTE: This step is only seen if Enable Alarms For Dell Hosts is selected.

4. Under **Event Posting Level**, select one of the following:
   - Do not post any events

     This options blocks hardware events.
   - Post All Events

     This option posts all hardware events.

- Post only Critical and Warning Events

  This option posts only critical or warning level hardware events.

- Post only Virtualization-Related Critical and Warning Events

  This option posts only virtualization-related critical and warning events. This is the default event posting level.

5. If you want to apply these settings to all vCenters, select the **Apply these settings to all vCenters** check box.

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

   This option is grayed out if you already selected All Registered vCenters from the drop-down list on the Setting page.
6. To save, click **Apply**.

Viewing Events

Configure events before you can view them in the Events tab, see Configuring Events and Alarms.

View the events for a host, cluster or datacenter on the Events tab.

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

Viewing the Alarm and Event Settings

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

1. In the **OpenManage Integration for VMware vCenter** > **Manage** > **Settings** tab, under vCenter Settings, expand Events and Alarms.
2. Under Events and Alarms you can view the following:
   - vCenter Alarms for Dell Hosts: Displays either Enabled or Disabled.
   - Event Posting Level

     To see the event posting levels that can display, see Understanding Alarms and Events.
3. To configure alarms and events, see Configuring Events and Alarms

Viewing the Data Retrieval Schedules for Inventory and Warranty

1. In the OpenManage Integration for VMware vCenter, on the **Manage** > **Settings** tab, under **vCenter Settings**, click **Data Retrieval Schedule**.
   Clicking Data Retrieval Schedule expands to expose the schedules for inventory and warranty.
2. For either Inventory or Warranty Retrieval, view the settings:
   - Shows whether the option is enabled or disabled
   - Displays the weekdays for which it is enabled.
   - Displays the time of day it is enabled.
3. If you click **Data Retrieval Schedule** again, it rolls up the information into a single line and displays whether the option is enabled or disabled.
4. If you want to edit the Data Retrieval Schedule, see Modifying Inventory Job Schedules or Modifying a Warranty Job Schedule.

11

Viewing Associated Host for a Chassis

You can view information about the associated host for the selected chassis on the **Manage** page.

To view information about the associated host:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Manage** tab.
   The following information about the associated host is displayed:
   - Host Name (If you click the selected host IP, the details about the host is displayed.)
   - Service Tag
   - Model
   - iDRAC IP
   - Slot Location
   - Last Inventory

12

Chassis Management

The OpenManage Integration for VMware vCenter allows you to view additional information for a selected Chassis. In the Chassis Information tab, you can view the chassis overview details for an individual chassis, information about hardware inventory, firmware and management controller. The following three tabs are displayed for each chassis and varies for some chassis based on the models.

Summary tab

Monitor tab

Manage tab

Topics:

Viewing Chassis Summary Details

You can view the Chassis summary details for an individual chassis on the Chassis **Summary** page.

To view the Chassis summary details:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Summary** tab.

   The following information about the selected Chassis is displayed:

   - Name
   - Model
   - Firmware Version
   - Service Tag
   - CMC (If you click the **CMC** link, the Chassis Management Controller page is displayed.)

     NOTE: If you do not inventory chassis, you can see only Service Tag and CMC IP address.

5. You can view the health status of the devices associated with the selected chassis. The main pane displays the overall health of a chassis. The valid health indicators are **Healthy**, **Warning**, **Critical**, **Not Present**. In the **Chassis Health** grid view, the health of each component is displayed. The chassis health parameters are applicable for models **VRTX version 1.0 and later**, **M1000e version 4.4 and later**. For 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).

NOTE: The overall health indicates the health based on the chassis with the least health parameter. For example, if there are 5 healthy signs and 1 warning sign, the overall health is shown as warning.

6. You can view the CMC **Enterprise** or **Express** with the license type and expiry date for a chassis. This is not applicable for M1000e chassis.
7. In the **Warranty** Icon the number of remaining days and the days used for a server. If you have more than one warranty, then the last day of the last warranty is considered to calculate the number of days left for warranty.
8. The **Active Errors** table lists and displays the errors for a chassis which are displayed in the **Chassis Health** page. For M1000e version 4.3 and below, the active errors are not displayed.

Viewing Hardware Inventory: Fans

You can view information about the fans within the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of Fans information.

To view information about fans:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration**, click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the fans, perform one of the following:
   a. In the **Overview** tab, click **Fans**.
   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory,** and then click **Fans**.

   The following information is displayed:
   - Name
   - Present
   - Power State
   - Reading
   - Warning Threshold
   - Critical Threshold
     - Minimum
     - Maximum

Viewing Hardware Inventory: I/O Modules

You can view information about the I/O Modules for the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of I/O Modules information.

To view information about I/O Modules:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the **I/O Modules**, perform one of the following:
   a. In the **Overview** tab, click **I/O Modules**.
   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory,** and then click **I/O Modules**.

   The following information is displayed:

- Slot/Location
- Present
- Name
- Fabric
- Service Tag
- Power Status

To view additional information, select the corresponding I/O module and following information is displayed:

- Role
- Firmware Version
- Hardware Version
- IP Address
- Subnet Mask
- Gateway
- Mac Address
- DHCP Enabled

Viewing Hardware Inventory: iKVM

You can view information about the iKVM for the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of iKVM information.

NOTE: You can view information about the iKVM only for PowerEdge M1000e Chassis.

To view information about iKVM:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the **iKVM**, perform one of the following:
   a. In the **Overview** tab, click **iKVM**.
   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory,** and then click **iKVM**.

   The following information is displayed:
   - iKVM Name
   - Present
   - Firmware Version
   - Front Panel USB/Video Enabled
   - Allow access to CMC CLI

   NOTE: The iKVM tab will be displayed only if the chassis contains iKVM module.

Viewing Hardware Inventory: PCIe

You can view information about the PCIe for the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of PCIe information.

To view information about PCIe:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the PCIe, perform one of the following:

   NOTE: PCIe information is not applicable for M1000e chassis.

   a. In the **Overview** tab, click **PCIe**.

   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **PCIe**.

   The following information is displayed:
   - PCIe Slot
     - Slot
     - Name
     - Power Status
     - Fabric
   - Server Slot
     - Name
     - Number

   To view additional information, select the corresponding PCIe and following information is displayed:
   - Slot Type
   - Server Mapping
   - Assignment Status
   - Allocated Slot Power
   - PCI ID
   - Vendor ID

Viewing Hardware Inventory: Power Supplies

You can view information about the Power Supply Units for the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of Power Supply Unit information.

To view information about the Power Supply Unit:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the Power Supply Units, perform one of the following:

   a. In the **Overview** tab, click **Power Supplies**.

   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **Power Supplies**.

   The following information is displayed:
   - Name
   - Capacity
   - Present

- Power State

Viewing Hardware Inventory: Temperature Sensors

You can view information about temperature sensors for the selected chassis. To view the information on this page, you must run an inventory job. You can export a CSV file of temperature sensors information.

To view information about the temperature sensors:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. To view information about the temperature sensors, perform one of the following:
   a. In the **Overview** tab, click **Temperature Sensors**.
   b. In the **Monitor** tab, expand the left pane, click **Hardware Inventory**, and then click **Temperature Sensors**.

   The following information is displayed:
   - Location
   - Reading
   - Warning Threshold
     - Minimum
     - Maximum
   - Critical Threshold
     - Minimum
     - Maximum

   NOTE: For PowerEdge M1000e chassis, information about temperature sensors is displayed only for chassis. For other chassis, information about temperature sensors is displayed for chassis and associated modular servers.

Viewing Warranty Details

Warranty window stores the warranty details.

To view information about warranty:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. The **Warranty** tab contains the following:
   a. **Provider**
   b. **Description**
   c. **Status**
   d. **Start Date**
   e. **End Date**
   f. **Days Left**
   g. **Last Updated**

Viewing Storage

Storage window stores the information for the chassis.

To view information about storage:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. The **Storage** tab contains the following:
   a. **Virtual Disks**
   b. **Controllers**
   c. **Enclosures**
   d. **Physical Disks**
   e. **Hot Spares**

   When you click each 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.
6. For M1000e chassis, if you have a storage module, the following storage details are displayed in a grid view without any additional information.
   a. Name
   b. Model
   c. Service Tag
   d. IP Address (Link to storage)
   e. Fabric
   f. Group Name
   g. Group IP Address (link to storage group)

Viewing Firmware Details for a Chassis

You can view information about the firmware details for the selected chassis. You can export a CSV file of firmware information.

To view information about firmware:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.
3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. Click the double arrow mark and expand the left pane, and then click **Firmware**.
   The following information is displayed:
   - Component
   - Current Version
6. If you click **Launch CMC**, the **Chassis Management Controller** page is displayed.

Viewing Management Controller Details for a Chassis

You can view information about the management controller details for the selected chassis.

To view information about the management controller:

1. On the **Home** page, click **vCenter**.
2. In the left pane, under **OpenManage Integration,** click **Dell Chassis**.

3. In the left pane, select the corresponding chassis IP.
4. Click the **Monitor** tab.
5. Click the double arrow mark and expand the left pane, and then click **Management Controller**.
6. On the **Management Controller** page, to view additional information, click the arrow mark and expand the left column. The following information is displayed:
   - General
     - Name
     - Firmware Version
     - Last Update Time
     - CMC Location
     - Hardware Version
   - Common Network
     - DNS Domain Name
     - Use DHCP for DNS
     - MAC Address
     - Redundancy Mode
   - CMC IPv4 Information
     - IPv4 Enabled
     - DHCP Enabled
     - IP Address
     - Subnet Mask
     - Gateway
     - Preferred DNS Server
     - Alternate DNS Server

13

Monitoring a Single Host

The OpenManage Integration for VMware vCenter lets you view detailed information for a single host. You can access hosts in VMware vCenter from the left side Navigator. This displays all hosts for all vendors. Click on a specific Dell host to find more detailed information. To quickly view a list of Dell Hosts, from within OpenManage Integration for VMware vCenter, in the left Side Navigator, click Dell Hosts.

- Viewing Host Summary Details
- Viewing Hardware: FRU Details for a Single Host
- Viewing Hardware: Processor Details for a Single Host
- Viewing Hardware: Power Supply Details for a Single Host
- Viewing Hardware: Memory Details for a Single Host
- Viewing Hardware: NICs Details for a Single Host
- Viewing Hardware: PCI Slot Details for a Single Host
- Viewing Hardware: Remote Access Card Details for a Single Host
- Viewing Storage Details for a Single Host
  - Viewing Storage: Virtual Disk Details for a Single Host
  - Viewing Storage: Physical Disk Details for a Single Host
  - Viewing Storage: Controller Details for a Single Host
  - Viewing Storage: Enclosure Details for a Single Host
- Viewing Firmware Details for a Single Host
- Viewing Power Monitoring for a Single Host
- Viewing Warranty Status for a Single Host
- Quickly Viewing Only Dell Hosts

Topics:

- Viewing Host Summary Details
- Launching Management Consoles
- Launching the Remote Access Console (iDRAC)
- Setting Up Physical Server Blink Indicator Light
- Setting Up Physical Server Blink Indicator Light

Viewing Host Summary Details

View the host summary details for an individual host on the Host Summary page. This page displays various portlets. Two among of those portlets are applicable to the OpenManage Integration for VMware vCenter.

The portlets are:

- Dell Host Health
- Dell Host information

You can drag and drop the two portlets to the position you want and you can format and customize the two portlets like other portlets as per your requirement.

1. In the OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. In the Objects tab, select the specific host you want to review.

3. Click the **Summary** tab.
4. View the host summary details:

Alerting system	If there are alerts for the OpenManage Integration for VMware vCenter, they display in a yellow box below the status area and above the portlets.
Notification area	Dell products integrate information in this right side-panel area. You can find information about: ● Recent Tasks ● Work In Progress ● Alarms Dell alarm information displays in this notification area portlet.

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

Service Tag	The Service Tag for your Dell PowerEdge server. Use this ID when you call for support.
Model Name	Displays the servers model name.
Fault Resilient Memory	This is a BIOS attribute and is enabled in the BIOS during initial setup of the server and displays the memory operational mode of the server. You need to restart your system when you change memory operational mode value. This is applicable for R620, R720, T620, M620 servers with ESXi 5.5 or later version. This is applicable for 12th generation of PowerEdge servers and above that support Fault Resilient Memory option, running ESXi 5.5 or later version. The four different values are: ● Enabled and Protected: This value indicates that the system is supported and operating system version is ESXi 5.5 or later and the memory operational mode in BIOS is set to FRM. ● 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 here 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.
Non-Uniform Memory Access (NUMA) Fault Resilient Memory (FRM)	NUMA FRM is a new memory operating mode available on the BIOS settings of high-end Dell's 13th generation of PowerEdge systems with at least two or four processors. This mode establishes an area of memory that is fault-resilient on all CPUs, providing the same protection to the hypervisor against uncorrectable memory errors that would affect it, as well as maintaining NUMA memory functionality and performance. The four different values are: ● NUMA Enabled and Protected: This value indicates that the system is supported and operating system version is ESXi 5.5 or later and the memory operational mode in BIOS is set to NUMA FRM. ● 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 here memory operational mode in BIOS is not set to NUMA FRM. ● Blank: If memory operational mode in BIOS is not supported the NUMA FRM attribute is not displayed.
Identification	● Host name The name of your Dell host. ● Power State Displays if your power is ON or OFF. ● iDRAC IP Displays the iDRAC IP address. ● Management IP Displays the management IP address. ● Connection Profile Displays the connection profile name for this host.

	• Model Displays the Dell 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	• Hypervisor Displays the Hypervisor version. • BIOS Version Displays the BIOS version. • Remote Access Card Version Displays the remote access card version.
Management Consoles	The management consoles are used to launch external system management consoles, such as: • Remote Access Console (iDRAC) Launches the Integrated Dell Remote Access Controller (iDRAC) web user interface.
Host Actions	Blink Indicator Light lets you set up your physical server to blink at various time intervals.

6. View the Dell Host Health portlet:

Dell Host Health	Component health is a graphical representation of the status of all major host server components: Server Global status, Server, Power supply, Temperature, Voltages, Processors, Batteries, Intrusion, Hardware log, Power management, Power and Memory. The chassis health parameters are applicable for models **VRTX version 1.0 and later**, **M1000e version 4.4 and later**. For versions less than 4.3 only two health indicators are displayed, namely **Healthy** and **Warning or Critical** (Inverted triangle with an exclamatory mark in orange color). The overall health indicates the health based on the chassis with the least health parameter. For example, if there are 5 healthy signs and 1 warning sign, the overall health is shown as warning. Options include: • Healthy (green check mark) - component operating normally • Warning (yellow triangle with exclamation point) - component has a non-critical error • Critical (red X) - component has a critical failure • Unknown (question mark) - status is unknown for the component

Launching Management Consoles

There are two management consoles you can launch from the Dell Server Management Portlet. These include:

- Remote Access Console (iDRAC Console)

  Launch the Remote Access Console to access the iDRAC user interface.

- OMSA Console

Launch the OMSA Console to access the OpenManage Server Administrator user interface. Before launching OMSA console, OMSA URL has to be configured in the Open Management Integration for VMware vCenter.

Launching the OMSA Console

Before you can launch the OMSA Console, you must set up the OMSA URL and install and configure the OMSA Web Server. Set up the OMSA URL from the Settings Tab.

NOTE: You must install OMSA to monitor and manage Dell PowerEdge 11th generation servers using OpenManage Integration for VMware vCenter.

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

Launching the Remote Access Console (iDRAC)

You can launch the iDRAC user interface from the Dell Server Management Portlet.

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

Setting Up Physical Server Blink Indicator Light

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

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

Setting Up Physical Server Blink Indicator Light

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

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

14

OpenManage Integration for VMware vCenter licensing

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

- Evaluation license—when the OMIVV version 3.2 appliance is powered on for the first time, an evaluation license is automatically installed. The trial version contains an evaluation license for five hosts (servers) managed by the OpenManage Integration for VMware vCenter. This is applicable only for 11th and later generations of the Dell servers and is a default license, which is for a 90 days trial period.
- Standard license—the full product version contains a standard license for up to 10 vCenter servers and you can purchase any number of host connections managed by OMIVV.

When you upgrade from an evaluation license to a full standard license, you will receive an email about the order confirmation, and you can download the license file from the Dell Digital store that is available at http://www.dell.com/support/licensing. Save the license .XML file to your local system, and upload the new license file by using the **Administration Console**.

Licensing presents the following information:

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

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

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital store that is available at http://www.dell.com/support/licensing . If you are unable to download your license key(s), contact Dell Support by going to www.dell.com/support/softwarecontacts to locate the regional Dell Support phone number for your product.

Topics:

Buying and uploading software license

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

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

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

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

15

Viewing Hardware: FRU Details for a Single Host

View the Field Replaceable Unit (FRU) details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Host tab, select the specific host for which you want to view Hardware: FRU details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Hardware: FRU sub-tab, view the following:

Part Name	Displays the FRU part name.
Part Number	Displays the FRU part number.
Manufacturer	Displays the manufacturer's name.
Serial Number	Displays the Manufacturer's serial number.
Manufacture Date	Displays the manufacture date.

16

Viewing Hardware: Processor Details for a Single Host

View the processor details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Object tab, select the specific host for which you want to view processor details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Hardware: Processor sub-tab, view the following:

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.

17

Viewing Hardware: Power Supply Details for a Single Host

View the virtual power supply details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Power Supply details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Power Supply** sub-tab, view the following:

Type	Displays the type of power supply. Power supply types include: • UNKNOWN • LINEAR • SWITCHING • BATTERY • 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.

18

Viewing Hardware: Memory Details for a Single Host

View the memory details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Memory details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Memory** sub-tab, view the following:

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.

19

View Hardware: NICs Details for a Single Host

View the Network Interface Card (NIC) details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: NICs details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: NICs** sub-tab, view the following:

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.

20

Viewing Hardware: PCI Slots for a Single Host

View the PCI slot details for a single host on the Dell Host Information tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: PCI Slot details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: PCI Slots** sub-tab, view the following:

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.

21

Viewing Hardware: Remote Access Card Details for a Single Host

View the Remote Access Card details for a single host on the Dell Host nformation tab. For information to appear on this page, you must run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view Hardware: Remote Access Card details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Hardware: Remote Access Card** sub-tab, view the following:

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.

22

Viewing Storage Details for a Single Host

View the storage details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. See Running an Inventory Job Now. This page displays different options depending on what is selected from the View drop-down list. If you select Physical Disks, another drop-down list appears. This new drop-down list called Filter lets you filter your physical disk options.

NOTE: Hardware views are directly reporting the data from OMSA and iDRAC.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific Host for which you want to view Storage: Physical Disk details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the **Storage** sub-tab, view the following:

Storage	Displays the counts of Virtual Disks, Controllers, Enclosures, and associated Physical Disks with its Global Hot Spare and Dedicated Hot Spare counts. When you selected from the View drop-down list, the option is highlighted here.
View	Displays the page options you want to view for this host: • Virtual Disks • Physical Disks • Controllers • Enclosures

Topics:

Viewing Storage: Virtual Disk Details for a Single Host

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

If you selected Virtual Disks from the View drop-down list, view these options:

Name	Displays the name of the virtual disk.
Device FQDD	Displays the FQDD.
Physical Disk	Displays on which physical disk the virtual disk is located.
Capacity	Displays the capacity of the virtual disk.
Layout	Displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual disk.
Media Type	Displays either SSD or HDD.
Controller ID	Displays the controller ID.
Device ID	Displays the device ID.
Stripe Size	The stripe size refers to the amount of space that each stripe consumes on a single disk.

Bus Protocol	This displays the technology that the physical disks included in the virtual disk are using. Possible values are: • SCSI • SAS • SATA
Default Read Policy	The default read policy supported by the controller. Options include: • Read-Ahead • No-Read-Ahead • Adaptive Read-Ahead • Read Cache Enabled • Read Cache Disabled
Default Write Policy	The default write policy supported by the controller. 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.

Viewing Storage: Physical Disk Details for a Single Host

The storage options on the Host Storage page depend on what you select from the View drop-down list. When you select this option the Filter drop-down list displays. You can filter your physical disks on the following options:

- All Physical Disks
- Global Hot Spares
- Dedicated Hot Spares
- The last option displays custom named virtual disks.

If you selected Physical Disks from the View drop-down list, view these options:

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. Options include: • ONLINE • READY • DEGRADED • FAILED • OFFLINE

	• REBUILDING • INCOMPATIBLE • REMOVED • CLEARED • SMART ALERT DETECTED • UNKNOWN • FOREIGN • UNSUPPORTED
Configured	Displays whether the disk is configured.
Hot Spare Type	Shows the hot spare type. Options include: • No No means there is no hot spare. • Global A global hot spare is an unused backup disk that is part of the disk group. • Dedicated A dedicated hot spare is an unused backup disk that is assigned to a single virtual disk. When a physical disk in the virtual disk fails, the hot spare is activated to replace the failed physical disk without interrupting the system or requiring your intervention.
Virtual Disk	Displays the name of the virtual disk.
Bus Protocol	Displays the bus protocol.
Controller ID	Displays the controller ID.
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.

Viewing Storage: Controller Details for a Single Host

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

If you selected Controllers from the View drop-down list, view these options:

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 newer version is available.
Driver Version	Displays the driver version.

Patrol Read State	Displays the Patrol Read State.
Cache Size	Displays the cache size.

Viewing Storage: Enclosure Details for a Single Host

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

If you selected Enclosures from the View drop-down list, view these options:

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.

23

Viewing Firmware Details for a Single Host

View the firmware details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now. This host page lets you use the search filter and export a CSV file of firmware information.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view firmware details.
3. On the Monitor tab, select the **Dell Host Information** tab, and on the Firmware sub-tab, view the following:

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.

24

Viewing Power Monitoring for a Single Host

View the power monitoring details for a single host on the Dell Host Information tab. For information to appear on this page, run an inventory job. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

NOTE: Host time, as used here, means the local time where the host is located.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific Host for which you want to view power monitoring details.
3. On the Monitor tab, select the **Dell Host Information Host** tab, and on the Power Monitoring sub-tab, view the following:

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.
Reading	This instantaneous value is the average value of readings over a one-minute time period.
Type:	Displays the energy statistics type.
Measurement Start Time (Host Time)	Displays the date and time when the host peak power began.
Peak Time (Host Time)	Displays the date and time of the host peak amps.
Peak Reading	The System Peak Power statistic is the peak power consumed by the system (in Watts).

25

Viewing Warranty Status for a Single Host

You must have run a warranty job to view a warranty status. See Running a Warranty Job Now.

View the warranty status details for a single host on the Dell Host Information tab. The Warranty Status page lets you monitor the warranty expiration date. 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. See Warranty History.

1. In OpenManage Integration for VMware vCenter, in the Navigator, click **Hosts**.
2. On the Objects tab, select the specific host for which you want to view warranty summary details.
3. On the Monitor tab, click **Dell Host Information** , click **Warranty** sub-tab, it displays information about:

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.

26

Quickly Viewing Only Dell Hosts

When you want to quickly view only Dell hosts, you can do this from within OpenManage Integration for VMware vCenter, and in the Navigator you can select Dell Hosts.

1. In VMware vCenter home page, click the **OpenManage Integration** icon.
2. In the Navigator, under OpenManage Integration for VMware vCenter, click Dell Hosts.
3. On the Dell Host tab, view the following information:

Host Name	Displays a link using the IP address for each Dell host. Click a specific host link to view the Dell host information.
vCenter	Displays the vCenter IP address for this Dell host.
Cluster	If this Dell host is in a cluster, the cluster name displays here.
Connection Profile	Displays the name of the connection profile.

27

Monitoring Hosts on Clusters and Datacenters

The OpenManage Integration for VMware vCenter lets you view detailed information for all hosts included in a datacenter or cluster. These pages let you sort data by clicking the data grid row header. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Details include:

- Viewing Host Overview Details
- Viewing Hardware: FRUs
- Viewing Hardware: Processor Details
- Viewing Hardware: Power Supply Details
- Viewing Hardware: Memory Details
- Viewing Hardware: NICs
- Viewing Hardware: PCI Slot Details
- Viewing Hardware: Remote Access Card Details
- Viewing Storage: Physical Disk Details
- Viewing Storage: Virtual Disk Details
- Viewing Firmware Details
- Viewing Power Monitoring
- Viewing Warranty Summary Details

28

Viewing Overview Details for Datacenters and Clusters

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

NOTE: Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid

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

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

Datacenter/ Cluster Information	Displays the following: • Datacenter/cluster name • The number of Dell managed hosts • Total Energy Consumption. This link takes you to the Power Monitoring page for this datacenter or cluster.
Hardware Resources	Displays the following: • Total Processors This link takes you to the Processor Details page. • Total Memory This link takes you to the Memory Details page for this datacenter or cluster. • Virtual Disk Capacity This link takes you to the Virtual Disk page for this datacenter or cluster.
Warranty Summary	Displays the warranty status for the selected host. Status options include: • Expired warranty • Active warranty • Unknown warranty The link takes you to the Warranty Summary page.
Host	Displays the host name.
Service Tag	Displays the host Service Tag.
Model	Displays the Dell 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: Location displays the slot location. Otherwise Location displays, “Not Applicable.”

iDRAC IP	Displays the iDRAC IP address.
Service Console IP	Displays the Service Console IP.
CMC URL	Blades only: The CMC URL is the Chassis URL. Otherwise 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 last inventory job.
Connection Profile	Displays the name of the connection profile.
Remote Access Card Version	Displays the remote access card version.
BIOS Firmware Version	Displays the BIOS firmware version.

29

Viewing Hardware: FRUs for Datacenters or Clusters

View the Field Replaceable Unit (FRU) details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offer filter/search functionality on the data grid. The data you view may vary depending on which view you are accessing the data. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Object tab, select the specific datacenter or cluster for which you want to view Hardware: FRU details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: FRU** sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Part Name	Displays the FRU part name.
Part Number	Displays the FRU part number.
Manufacturer	Displays the manufacturer's name.
Serial Number	Displays the Manufacturer's serial number.
Manufacture Date	Displays the manufacture date.

30

Viewing Hardware: Processor Details for Datacenters or Clusters

View the processor details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Datacenter or Cluster tab, select the specific datacenter or cluster for which you want to view Processor details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the Hardware: Processor sub-tab, view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
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.

31

Viewing Hardware: Power Supply Details for Datacenters and Clusters

View the virtual power supply details for a datacenter or cluster on the Dell Datacenter or Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vCenter, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view Hardware: Power Supply details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the **Hardware: Power Supply** sub-tab, view the following:

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Type	Displays the type of power supply. Power supply types include: • UNKNOWN • LINEAR • SWITCHING • BATTERY • 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

32

Viewing Hardware: Memory Details for Datacenters and Clusters

View the memory details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator area, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab, select the specific datacenter or cluster for which you want to view the Hardware: Memory details.
4. On the **Monitor** tab, select the **Dell Datacenter/Cluster Information** tab, and navigate to **Hardware** > **Memory** sub-tab, to view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Slot	Displays the DIMM slot.
Size	Displays the memory size.
Type	Displays the memory type.

33

Viewing Hardware: NICs Details for Datacenters and Clusters

View the Network Interface Card (NIC) details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator area, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab click on a specific datacenter or cluster for which you want to view Hardware related NICs details.
4. On the **Monitor** tab, click **Dell Datacenter/Clusters Information**, and click on **Hardware** > **NICs**, to view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
Name	Displays the product name.
Manufacturer	Displays only the manufacturer name.
MAC Address	Displays the NIC mac address.

34

Viewing Hardware: PCI Slot Details for Datacenters and Clusters

View the PCI slot details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator area, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab click on a specific Datacenter or Cluster.
4. On the **Monitor** tab, select the **Dell Datacenter/Cluster Information** tab, and click **Hardware** > **PCI Slots:** , to view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
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.

35

Viewing Hardware: Remote Access Card Details

View the Remote Access Card details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator area, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab, click on a specific datacenter or cluster.
4. On the **Monitor** tab, click **Dell Datacenter/Cluster Information** tab, and navigate to **Hardware** > **Remote Access Card** to view the following:

Host	Displays the host name.
Service Tag	Displays the Service Tag.
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.

36

Viewing Storage: Physical Disks for Datacenters and Clusters

View the physical storage details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. See Running an Inventory Job Now.

NOTE: Hardware views are directly reporting the data from OMSA and iDRAC.

1. In VMware vSphere Web Client, in the Navigator, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab, select the specific datacenter or cluster.
4. On the **Monitor** tab, click **Dell Datacenter/Cluster Information** tab, and navigate to **Storage** > **Physical Disk**, to view the following:

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

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Capacity	Displays the physical disk capacity.
Disk Status	Displays physical disk status. Options include: • ONLINE • READY • DEGRADED • FAILED • OFFLINE • REBUILDING • INCOMPATIBLE • REMOVED • CLEARED • SMART ALERT DETECTED • UNKNOWN • FOREIGN • UNSUPPORTED **NOTE:** For more information about the meaning of these alerts, see the *OpenManage™ Server Administrator Storage Management User's Guide*, located at: http://support.dell.com/support/edocs/software/svradmin/5.1/en/omss_ug/html/adprin.html.
Model Number	Displays the model number of the physical storage disk.
Host	Displays the host name.
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.
Hot Spare Type	Shows the hot spare type. Options include: ● No No means there is no hot spare. ● Global A global hot spare is an unused backup disk that is part of the disk group. ● Dedicated A dedicated hot spare is an unused backup disk that is assigned to a single virtual disk. When a physical disk in the virtual disk fails, the hot spare is activated 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.

37

Viewing Storage: Virtual Disk Details for Datacenters and Clusters

View the virtual storage details for a datacenter or cluster on the Dell Datacenter/Cluster tab. For information to appear on this page, you must run an inventory job. The data you view may vary depending on which view you are accessing the data. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid.

1. In VMware vSphere Web client, in the Navigator area, click **vCenter Inventory Lists**.
2. Click **Datacenters** or **Clusters**.
3. On the **Objects** tab, select the specific datacenter or cluster.
4. On the **Monitor** tab, click **Dell Datacenter/Cluster Information** tab, and navigate to **Storage** > **Virtual Disk** to view the following:

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

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Name	Displays the name of the virtual disk.
Physical Disk	Displays on which physical disk the virtual disk is located.
Capacity	Displays the capacity of the virtual disk.
Layout	Displays the layout type of the virtual storage. This means the type of RAID that was configured for this virtual disk.
Host	Displays the host name.
Name	Displays the virtual disk name.
Last Inventory	Displays the day, date and time the inventory was last run.
Controller ID	Displays the controller ID.
Device ID	Displays the device ID.
Media Type	Displays either SSD or HDD.
Bus Protocol	This displays the technology that the physical disks included in the virtual disk are using. Possible values are: • SCSI • SAS • SATA
Stripe Size	The stripe size refers to the amount of space that each stripe consumes on a single disk.
Default Read Policy	The default read policy supported by the controller. Options include: • Read-Ahead • No-Read-Ahead • Adaptive Read-Ahead • Read Cache Enabled • Read Cache Disabled

Default Write Policy	The default write policy supported by the controller. Options include: ● Write-Back ● Force Write Back ● Write Back Enabled ● Write-Through ● Write Cache Enabled Protected ● Write Cache Disabled
Disk Cache Policy	The default cache policy supported by the controller. Options include: ● Enabled This means cache I/O. ● Disabled This means direct I/O.

38

Viewing Firmware Details for Datacenters and Clusters

View the firmware details for datacenters or clusters on the Dell Host tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view firmware details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on the Firmware sub-tab, view the following:

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Name	Displays the name of all the firmware on this host.
Version	Displays the version of all the firmware on this host.

39

Viewing Warranty Summary Details for Datacenters and Clusters

You must have run a warranty job to view a warranty summary. See Running a Warranty Job Now.

View the warranty summary details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. The Warranty Summary page lets you monitor the warranty expiration date. 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. See Warranty History.

1. In VMware vSphere Web Client, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view warranty summary details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information** tab, and on Warranty Summary sub-tab, view the following:

Warranty Summary	The host warranty summary is displayed using icons to visually show the number of hosts in each status category.
Host	Displays the name of the host.
Service Tag	Displays the Service Tag for 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 vCentercannot get warranty status because the warranty job has not run, an error has occurred getting the data, or the system does not have a warranty.
Days Left	Displays the number of days left for the warranty.

40

Viewing Power Monitoring for Datacenters and Clusters

View the power monitoring details for a datacenter or cluster on the Dell Datacenter/Cluster Information tab. For information to appear on this page, you must run an inventory job. Datacenter and cluster pages let you export information to a CSV file and offers filter/search functionality on the data grid. Hardware views are directly reporting the data from OMSA and iDRAC. See Running an Inventory Job Now.

1. In VMware vSphere Web Client, in the Navigator, click **vCenter**.
2. Click **Datacenters** or **Clusters**.
3. On the Objects tab, select the specific datacenter or cluster for which you want to view power monitoring details.
4. On the Monitor tab, select the **Dell Datacenter/Cluster Information Host** tab, and on the Power Monitoring sub-tab, view the following:

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

Host	Displays the name of the host.
Service Tag	Displays the Service Tag.
Current Profile	Displays power profile to maximize your system's performance 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 began.
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 beginning date and time of the host peak amps.
System Peak Amps End Date	Displays the end date and time of the host peak amps.

41

Troubleshooting

Use this section to find answers to troubleshooting questions. This section includes:

- Frequently asked questions (FAQ)
- Contacting Dell on page 125
- Related product information

Topics:

Frequently Asked Questions (FAQ)

This section contains some common questions and solutions.

OMIVV cannot act as a provisioning server during the auto discovery process

If OMIVV IP address is used as a provisioning server in the iDRAC settings for the newly added Dell servers, these Dell servers will not be auto discovered. The auto discovery process fails as OMIVV 3.2 does not support MD5 encrypted SSL certificate signatures to enhance more secure encryption.

Resolution: None.

Intermittent Inventory failure for 1st time after OSD

In case of intermittent inventory failure post first time deployment, user might observe the error "No inventory record found for the host <IP / Host name>"

Resolution: Intermittent inventory failure post first time OSD can be resolved by running the inventory manually.

Test connection for iDRAC in the connection profile page fails in DNC once OSD is successful

After OS deployment, immediate test connection to iDRAC fails and shows an error, "Fail - Unable to connect to iDRAC" in the connection profile page.

Resolution: This issue occurs since BMC is unable to obtain an IP address. To resolve this issue, you must restart the management network. If the issue still persist, user will have to restart the ESXi host.

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

Dell Management Center does not display all the relevant logs when trying to filter a severity category. How can I view all the logs?

When you select a severity category to filter the log data by choosing **All Categories** from the drop-down, all the logs belonging to specific category are displayed accurately. However, if you filter by choosing **Info** from the drop-down, the Firmware update logs are not displayed and only the task initiation logs are displayed.

Resolution: To view all the logs in Dell Management Center, select **All Categories** from the Filter drop-down.

Version Affected: 3.1

How do I resolve error code 2000000 caused by VMware Certificate Authority (VMCA)?

When you run the vSphere certificate manager and replace the vCenter server or Platform Controller Service (PSC) certificate with a new CA certificate and key for vCenter 6.0, OMIVV displays error code 2000000 and throws an exception.

Resolution: To resolve the exception, you should update the ssl Anchors for the services. The ssl Anchors can be updated by running the `ls_update_certs.py` scripts on PSC. The script takes the old certificate thumbprint as the input argument and the new certificate is installed. The old certificate is the certificate before the replacement and the new certificate is the certificate after the replacement. Visit http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701 and http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121689 for more information.

Updating the ssl Anchors in Windows vSphere 6.0

1. Download the lstoolutil.py.zip file from http://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2121701.
2. Copy the lstoolutil.py file to the `%VMWARE_CIS_HOME%"\VMware Identity Services\lstool\scripts\` folder.

   NOTE: Do not replace the lstoolutil.py file if you are using vSphere 6.0 Update 1.

You can use the following relevant procedures to update the ssl Anchors:

- Updating the ssl Anchors for vCenter installed on Windows operation system: Replace the certificates on vCenter Windows installation by using vSphere Certificate Manager utility. See Replacing the certificates on vCenter Windows installation on page 111.
- Updating the ssl Anchors for the vCenter server appliance: Replace the certificates on vCenter server appliance by using vSphere Certificate Manager utility. See Replacing the certificates on the vCenter server appliance on page 111.

The output obtained from the mentioned procedures should display `Updated 24 service (s)` and `Updated 26 service (s)` respectively. If the output displayed is `Updated 0 service (s)`, the old certificate thumbprint is incorrect. You can perform the following steps to retrieve the old certificate thumbprint. Also, use the following procedure to retrieve the old certificate thumbprint, if **vCenter Certificate Manager** is not used to replace the certificates:

NOTE: Run the `ls_update_certs.py` with the old thumbprint obtained.

1. Retrieve the old certificate from the Managed Object Browser (MOB). See Retrieving the old certificate from Managed Object Browser (MOB) on page 112.
2. Extract the thumbprint from the old certificate. See Extracting thumbprint from the old certificate on page 113.

Version Affected: 3.0 and later, vCenter 6.0 and later

Replacing the certificates on vCenter Windows installation

Perform the following steps if vSphere Certificate Manager utility is used to replace the certificates on vCenter Windows installation:

1. Connect to External Platform Services Controller through remote desktop connection.
2. Open command prompt in administrative mode.
3. Create the `c:\certificates` folder by using the following command: `mkdir c:\certificates`
4. Retrieve the old certificate by using the following command: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output c:\certificates\old_machine.crt`
5. Retrieve the old certificate thumbprint by using the following command: `"%VMWARE_OPENSSL_BIN%" x509 -in C:\certificates\old_machine.crt -noout -sha1 -fingerprint`

   NOTE: The retrieved certificate thumbprint is in the following format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   The thumbprint is a sequence of numbers and alphabets which appears as follows:`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

6. Retrieve the new certificate by using the following command: `"%VMWARE_CIS_HOME%"\vmafdd\vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output c:\certificates\new_machine.crt`
7. Perform the following steps:
   a. Run `ls_update_certs.py` by using the following command. `"%VMWARE _PYTHON_BIN%" ls_update_certs.py --url`
   b. Replace psc.vmware.com by Lookup_Service_FQDN_of_Platform_Services_Controller and the 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 thumbprint with the thumbprint obtained in step 5 by using the following command: `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile c:\certificates\new_machine.crt --user Administrator@vsphere.local --password Password`

      NOTE: Ensure to provide valid credentials.

8. Log out and log in to the vCenter Web client after all the services are updated successfully.

OMIVV now launches successfully.

Replacing the certificates on the vCenter server appliance

Perform the following steps if vSphere Certificate Manager utility is used to replace the certificates on the vCenter server appliance:

1. Log in to the External Platform Services Controller appliance through console or a secure shell (SSH) session.
2. Run the following command to enable accessing the Bash shell: `shell.set --enabled true`
3. Type **`shell`** and press **Enter**.
4. Create folders or certificates by using the following command: `mkdir /certificates`
5. Retrieve the old certificate by using the following command: `/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store BACKUP_STORE --alias bkp___MACHINE_CERT --output /certificates/old_machine.crt`
6. Retrieve the old certificate thumbprint by using the following command: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

   NOTE: The retrieved certificate thumbprint is in the following format: `SHA1 Fingerprint=13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

   The thumbprint is a sequence of numbers and alphabets which appears as follows:`13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88`

7. Retrieve the new certificate by using the following command:`/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT --output /certificates/new_machine.crt`
8. Run the following command to change the directory: `cd /usr/lib/vmidentity/tools/scripts/`
9. Perform the following steps:
   a. Run `ls_update_certs.py` by using the following command. `python ls_update_certs.py --url`
   b. Replace psc.vmware.com by Lookup_Service_FQDN_of_Platform_Services_Controller and the 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 thumbprint with the thumbprint obtained in step 6 by using the following command: `https://psc.vmware.com/lookupservice/sdk --fingerprint 13:1E:60:93:E4:E6:59:31:55:EB:74:51:67:2A:99:F8:3F:04:83:88 --certfile /certificates/new_machine.crt --user Administrator@vsphere.local --password "Password"`

   NOTE: Ensure to provide valid credentials.

10. Log out and log in to the vCenter Web client after all the services are updated successfully.

OMIVV now launches successfully.

Retrieving the old certificate from Managed Object Browser (MOB)

You can retrieve the old certificate for the vCenter server system by connecting to Platform Service Controller (PSC) by using the Managed Object Browser (MOB).

To retrieve the old certificate, you should find the sslTrust field of the ArrayOfLookupServiceRegistrationInfo managed object by performing the following steps:

NOTE: In this guide, the `C:\certificates\` folder location is used to store all certificates.

1. Create the `C:\certificates\` folder on PSC by using the following command: `mkdir C:\certificates\`.
2. Open the following link in a browser: `https://<vCenter FQDN/IP address>/lookupservice/mob?moid=ServiceRegistration&method=List`
3. Log in with the `administrator@vsphere.local` user name and provide the password when prompted.

   NOTE: If you are using a custom name for vCenter Single Sign-On (SSO) domain, use that user name and password.

4. In **filterCriteria**, modify the value field to show only the tags **<filtercriteria></filtercriteria>** and click **Invoke Method**.
5. Search for the following hostnames depending on the certificates that you are replacing:

Table 6. Search criteria information

Trust anchors	Search criteria
vCenter server	Use Ctrl+F to search, vc_hostname_or_IP.example.com on the page
Platform Services Controller	Use Ctrl+F to search, psc_hostname_or_IP.example.com on the page

6. Locate the value of the corresponding sslTrust field. The value of the sslTrust field is Base64 encoded string of the old certificate.
7. Use the following examples when updating the Platform Services Controller or vCenter Server trust anchors.

   NOTE: The actual string is shortened significantly to improve legibility.

   - For vCenter server

Table 7. vCenter server example

Name	Type	Value
url	anyURI	https://vcenter.vmware.local:443/sdk

   - For Platform Services Controller

Table 8. Platform Services Controller example

Name	Type	Value
url	anyURI	https://psc.vmware.local/sts/STSService/vsphere.local

8. Copy the content of the sslTrust field into a text document and save the document as `old_machine.txt`.
9. Open the `old_machine.txt` in a text editor.
10. Append the following at the starting and end of the `old_machine.txt` file respectively:

    `-----BEGIN CERTIFICATE-----`

    `-----END CERTIFICATE-----`
11. Save `old_machine.txt` now as `old_machine.crt`.

You can now extract the thumbprint from this certificate.

Extracting thumbprint from the old certificate

You can extract the thumbprint from the old certificate and upload it to the Platform Services by using the following options:

- Extract the thumbprint by using a Certificate Viewer Tool. See Extracting the certificate thumbprint by using a Certificate Viewer tool on page 113.
- Extract the thumbprint by using a command line on the appliance. See Extracting Thumbprint by using the command line on page 113.

Extracting the certificate thumbprint by using a Certificate Viewer tool

Perform the following steps to extract the certificate thumbprint:

1. In Windows, double-click the `old_machine.txt` file to open it in Windows Certificate Viewer.
2. In Windows Certificate Viewer, select the **SHA1 Thumbprint** field.
3. Copy the thumbprint string into a plain text editor and replace the spaces with colons or remove the spaces from the string. For example, the thumbprint string can appear as either of the following:
   - ea87e150bb96fbbe1fa95a3c1d75b48c30db7971
   - ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71

Extracting Thumbprint by using the command line

You can see the following sections for extracting thumbprint by using the command line on the appliance and Windows installation.

Extracting thumbprint by using the Command Line on the vCenter server appliance

Perform the following steps:

1. Move or upload the old_machine.crt certificate to PSC in the `C:\certificates\old_machine.crt` location that is created in step 1 of retrieving the old certificate procedure. You can use Windows Secure Copy (WinSCP) or another SCP client to move or upload the certificate.
2. Log in to the External Platform Services Controller appliance through Secure Shell (SSH).
3. Run the following command to enable accessing the Bash shell: `shell.set --enabled true`.
4. Type `shell` and press **Enter**.
5. Run the following command to extract the thumbprint: `openssl x509 -in /certificates/old_machine.crt -noout -sha1 -fingerprint`

NOTE: The thumbprint appears as a sequence of numbers and letters after the equal sign, which is as follows: `SHA1 Fingerprint= ea:87:e1:50:bb:96:fb:be:1f:a9:5a:3c:1d:75:b4:8c:30:db:79:71`

Extracting thumbprint by using the Command Line on Windows installation

Perform the following steps:

1. Move or upload the old_machine.crt certificate to PSC in the `C:\certificates\old_machine.crt` location that is created in step 1 of retrieving the old certificate procedure. You can use Windows Secure Copy (WinSCP) or another SCP client to move or upload the certificate.
2. Connect to External Platform Services Controller through remote desktop connection.
3. Open command prompt in administrative mode.
4. Run the following command to extract the thumbprint: `"%VMWARE_OPENSSL_BIN%" x509 -in c:\certificates\old_machine.crt -noout -sha1 -fingerprint`

NOTE: The thumbprint appears as a sequence of numbers and letters after the equal sign, which is as follows: `SHA1 Fingerprint=09:0A:B7:53:7C:D9:D2:35:1B:4D:6D:B8:37:77:E8:2E:48:CD:12:1B`

Run the ls_update_certs.py with the old thumbprint. Log out and log in to the vCenter Web client after the services are updated successfully. The Dell plug-in launches successfully.

Firmware Update Wizard shows a message mentioning that the bundles are not retrieved from firmware repository. How can I continue with the firmware update?

In Web client, when you are running the Firmware Update wizard for a single host, the **Select Components** screen displays the firmware details for the components. If you select the desired firmware updates and click **Back** twice to arrive at the **Welcome** page and then click **Next**, a message is displayed mentioning that the bundles are not retrieved from firmware repository in the **Select Update Source** screen.

Resolution: You can select the desired firmware updates and click **Next** to continue with the firmware update.

Version Affected: 3.0 and later

Firmware Update for 30 Hosts through Cluster level Fails

VMware recommends clusters to be built with identical server hardware. For the firmware update at a cluster level with the number of hosts near the limits for a cluster (recommended by VMWare) or composed of different models of Dell servers, usage of vSphere web client is recommended.

Warranty and Inventory schedule for all vCenters is not applying when selected under "Dell Home > Monitor > Job Queue > Warranty/Inventory History >Schedule"

A customer navigates to the job queue page, selects a vCenter and selects the modify schedule button. When the dialog comes up, they see a checkbox that says apply this new setting to all registered vCenters. When they select this and press Apply, it only applies the setting to the particular vCenter they initially selected and not all vCenters. The 'Apply to All Registered vCenters' is not applicable when Warranty or Inventory schedule is modified from the Job Queue page.

Resolution: Use the modify Warranty or Inventory schedule from the Job Queue only to modify the selected vCenter.

Versions Affected: 2.2 and later

I see a web communication error in the vCenter web client after changing the DNS settings in OpenManage Integration for VMware vCenter?

If you see any kind of web communication error in the vCenter web client while doing any OMIVV related tasks after changing the DNS settings , clear the browser cache or logout and login from the web client.

'Settings' page fails to load, if we navigate away and go back to ‘Settings’ page

For vSphere v5.5, in the Web Client, if you navigate away and go back to the ‘Settings’ page, sometimes the page fails to load and the spinner continues to show. This is a refresh issue and the page is not getting refreshed correctly.

Resolution: Click the global refresh and the screen will refresh correctly.

Versions Affected: 2.2 and 3.0

Why do I see “Task cannot be scheduled for the time in the past” error in inventory schedule/Warranty schedule page of Initial Configuration Wizard?

In the Web Client, if the user picks ‘All registered vCenters’ in the Initial Configuration wizard, and if there are some vCenters with no hosts or vCenters where some have Inventory or Warranty task already scheduled and some with no Inventory or Warranty schedule set yet, then the user will sometimes see an error “Task cannot be scheduled for the time in the past”.

Resolution: If you have situations where there are some vCenters with no hosts or vCenters where some have Inventory or Warranty task already scheduled and some with no Inventory or Warranty schedule set yet, run the setting of Inventory and Warranty schedule separately again from the Settings page for those vCenters.

Versions Affected: 2.2 and later

Why is the Installation date showing up as 12/31/1969 for some of the firmware on the firmware page?

In the Web Client, the installation date is showing up as 12/31/1969 for some firmware items on the firmware page for a host. If the firmware installation date is not available, then this very old date is shown.

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

Why is successive Global refresh cause exception to be thrown in Recent Task window?

If a customer tries to press the refresh button repeatedly, the VMware UI may throw an exception.

Resolution: User should dismiss this error and can continue on.

Version Affected: 2.2 and later

Why is the Web client UI distorted for few of the Dell screens in IE 10?

In some cases, when a popup dialog is presented, the data in the background may turn completely white and be distorted.

Resolution: Close the dialog, the screen will return back to normal.

Version Affected: 2.2 and later

Why am I not seeing the OpenManage Integration Icon on the Web Client even if the registration of the plug-in to the vCenter was successful?

OpenManage Integration icon is not displayed on the Web client unless the vCenter Web Client services are restarted or the Box is rebooted. When a user registers the OpenManage Integration for VMware vCenter appliance, it registers with both the Desktop client and the Web client. If a user unregisters the appliance and then either reregisters the same version or registers a new version of the appliance, it will successfully register with both clients, but the Dell icon may not appear in the Web Client. This is due to a caching issue from VMware. To clear the issue, a user needs to restart the Web Client Service on the vCenter Server. Only then will the plug-in appear in the UI.

Resolution: Restart the Web Client Service on the vCenter Server.

Version Affected: 2.2 and later

Even if my repository has bundles for selected 11G system, why is firmware update showing that I have no bundles for Firmware Update?

When I added a host to the connection profile in lockdown mode, the inventory kicked off but failed stating that “No Remote Access Controller was found or Inventory is not supported on this host.” Inventory is supposed to work for a host in lockdown mode, right?

If you put the host in lockdown mode or remove a host from lockdown mode, you must wait 30–minutes before performing the next operation. If you use a 11G host for firmware update, the firmware update wizard will not show any bundles even if the repository provided has bundles for that system. This occurs because the 11G host might have not been configured for OMSA to send traps to OpenManage Integration.

Resolution: Ensure that the host is compliant using the host Compliance screen of OpenManage Integration desktop client. If it is not compliant, use the fix Host Compliance to get it compliant.

Version Affected: 2.2 and later

On running a warranty retrieval job, the warranty job status is not listed in the Warranty Job Queue page

If your network needs proxy details to connect to the internet and the proxy is not set on the OMIVV appliance, the warranty retrieval job fails and the job is not listed under warranty job queue.

Resolution: Set the proxy details and trigger the warranty job again.

Version Affected: All

Why is the DNS configuration settings restored to original settings after appliance reboot if using DHCP for appliance IP and DNS settings overwritten

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 will be different from DHCP.

Version Affected: All

Using OpenManage Integration for VMware vCenter to update an Intel Network card with the firmware version of 13.5.2 is not supported.

There is a known issue with Dell PowerEdge 12th generation servers and some Intel Network cards with the firmware version of 13.5.2. Updating some models of Intel network cards at this version of firmware fails when the firmware update is applied using the Lifecycle Controller. Customers with this version of firmware must update the network driver software using an operating system. If the Intel Network card has a version of firmware other than 13.5.2, you can update using OpenManage Integration for VMware vCenter. For more information, see http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx

NOTE: Note: When using the one-to-many firmware update, avoid selecting Intel network adapters that are at version 13.5.2, as the update will fail and stop the update task from updating remaining servers.

Using OpenManage Integration for VMware vCenter to update an 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. You must use the custom catalog to update the firmware to 15.5.0 first before updating the firmware to 16.x.

Version Affected: All

On trying a firmware update with an invalid DUP, the hardware update job status on the vCenter console neither fails nor times-out for hours, though the job status in LC says 'FAILED'. Why is this happening?

When the invalid DUP is picked for firmware update, the status of the task in the vCenter console window remains 'In Progress' but the message is changed to the reason of failure. This is a known VMware defect and will be fixed in the future releases of VMware vCenter.

Resolution: The task has to be cancelled manually.

Version Affected: All

Administration Portal is still showing the unreachable Update Repository location.

If the user provided a unreachable Update Repository path, the error message "Failed: Error while connecting to the URL …. " is displayed on the top of the Appliance Update view, however the Update Repository Path is not cleared out to the value before update.

Resolution: Move out of this page to another page and make sure the page is refreshed.

Version Affected: All

Why did my system not enter maintenance mode when I performed a 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.

Why is the chassis global health still healthy when some of the power supply status has changed to critical?

The global health of the chassis with respect to the power supply is based on the redundancy policies and the whether the chassis power needs are satisfied by the PSU that are still online and functional. So even if some of the PSU are out of power the overall power requirement of the chassis are met. So the global health of the chassis is Healthy. For more details on the Power Supply and Power Management look in the user's guide for Dell PowerEdge M1000e Chassis Management Controller Firmware document.

Why is the processor version "Not Applicable" in Processor view in the System overview page?

In case of PowerEdge 12th Generation Dell Servers and higher generations, the processor version is in the Brand column. In case of lower generation servers processor version is shown in the Version column.

I get an exception whenever I click finish after editing a connection profile through Web Client. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. The connection profile can be edited through the Desktop client. Re-registering the vCenter server to the same appliance will not solve this. A new setup registered with FQDN is required.

I am unable to see the connection profiles to which a host belongs to when I create or edit a connection profile in web GUI. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. Re-registering the vCenter server to the same appliance will not solve this. A new setup registered with FQDN is required.

On editing a Connection profile the select host window in the Web UI is blank. Why?

This happens when the vCenter server is registered to the appliance through IP instead of FQDN. Re-registering the vCenter server to the same appliance will not solve this . A new setup registered with FQDN is required.

How Come I See An Error Message Displayed After Clicking The Firmware Link?

If you have a slow network speed (9600BPS), you may get a Communication Error Message. This error message may display when you click the Firmware link in the vSphere Client for the OpenManage Integration for VMware vCenter. It happens when the connection times out while trying to obtain the Software Inventory list. Microsoft Internet Explorer initiates this timeout. For Microsoft Internet Explorer versions 9/10, the default "Receive Time out" value is set to 10 seconds. Fix this issue by using the following steps.

Figure 1. Firmware link communication error

1. Open Microsoft Registry Editor (Regedit).
2. Navigate to the following location:
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Add a DWORD value for ReceiveTimeout.
4. Set the value to 30 seconds (30000) [This value may need to be a higher value in your environment].
5. Exit Regedit.
6. Restart Internet Explorer.

NOTE: Just opening a new Internet Explorer window is not enough. Restart the Internet Explorer browser.

What generation of Dell servers does the OpenManage Integration for VMware vCenter configure and support for SNMP traps?

OpenManage Integration for VMware vCenter supports OMSA SNMP traps on pre-12th generation servers and iDRAC traps on 12th generation servers.

What vCenters are managed by OpenManage Integration for VMware vCenter?

OpenManage Integration for VMware vCenter manages only registered vCenters in either linked mode or not in a linked mode also.

Does OpenManage Integration for VMware vCenter support vCenter in linked mode?

Yes , OpenManage Integration for VMware vCenter supports up to 10 vCenters either in a linked mode or not in a linked mode also. For more information on how OpenManage Integration for VMware vCenter works in linked mode, see the white paper, *OpenManage Integration for VMware vCenter: Working in Linked Mode* on www.Dell.com.

What are the Required Port Settings for the OpenManage Integration for VMware vCenter?

NOTE: When deploying the OMSA agent using the *Fix non-compliant vSphere hosts* link available from the Compliance window in the OpenManage Integration for VMware vCenter, the OpenManage Integration for VMware vCenter starts the http Client service and enables port 8080 on releases after ESXI 5.0 to download OMSA VIB and install it. Once the OMSA installation is completed the service automatically stops and the port is closed.

Use these port settings for the OpenManage Integration for VMware vCenter.

Table 9. Virtual Appliance Ports

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
53	DNS	TCP	None	Out	DNS client	No
80	HTTP	TCP	None	Out	Dell Online Data Access	No
80	HTTP	TCP	None	In	Administration Console	No
162	SNMP Agent	UDP	None	In	SNMP Agent (server)	No
11620	SNMP Agent	UDP	None	In	SNMP Agent (server)	No
443	HTTPS	TCP	128–bit	In	HTTPS server	No
443	WSMAN	TCP	128–bit	In/Out	iDRAC/OMSA communication	No
4433	HTTPS	TCP	128–bit	In	Auto Discovery	No
2049	NFS	UDP	None	In/Out	Public Share	No
4001–4004	NFS	UDP	None	In/Out	Public Share	No
11620	SNMP Agent	UDP	None	In	SNMP Agent (server)	No

Table 10. Managed Nodes

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
162, 11620	SNMP	UDP	None	Out	Hardware events	No
443	WSMAN	TCP	128–bit	In	iDRAC/OMSA communication	No
4433	HTTPS	TCP	128–bit	Out	Auto Discovery	No
2049	NFS	UDP	None	In/Out	Public Share	No
4001–4004	NFS	UDP	None	In/Out	Public Share	No
443	HTTPS	TCP	128–bit	In	HTTPS server	No
8080	HTTP	TCP		In	HTTP server; downloads the OMSA VIB and	No

Table 10. Managed Nodes (continued)

Port Number	Protocols	Port Type	Max. Encryption Level	Direction	Usage	Configurable
					fixes non-compliant vSphere hosts	
50	RMCP	UDP/TCP	128–bit	Out	Remote Mail Check Protocol	No
51	IMP	UDP/TCP	N/A	N/A	IMP Logical Address Maintenance	No
5353	mDNS	UDP/TCP		In/Out	Multicast DNS	No
631	IPP	UDP/TCP	None	Out	Internet Printing Protocol (IPP)	No
69	TFTP	UDP	128–bit	In/Out	Trivial File Transfer	No
111	NFS	UDP/TCP	128–bit	In	SUN Remote Procedure Call (Portmap)	No
68	BOOTP	UDP	None	Out	Bootstrap Protocol Client	No

What are the Minimum requirements for successful installation and operation of the virtual appliance?

The following settings outline the minimum appliance requirements:

- Google Chrome, version 28 and later

  .
- Microsoft Internet Explorer, version 9 and 10
- Mozilla Firefox, version 22 and later
- Reserved Memory: 2 GB

  NOTE: For optimal performance Dell recommends 3 GB.
- Disk: 43.5 GB.
- CPU: 2 virtual CPUs.

How come I do not see my new iDRAC version details listed on the vCenter Hosts & Clusters page?

After the successful completion of a firmware update task in the vSphere Desktop client's recent tasks pane, refresh the Firmware Update page and verify the firmware versions. If the page shows the old versions, then go to Host Compliance page in OpenManage Integration for VMware vCenter and check the CSIOR status of that host. If CSIOR is not enabled, then enable CSIOR and reboot host. If the CSIOR was already enabled, then login to the iDRAC console, reset iDRAC, wait for few minutes, and then refresh the Firmware Update page in vSphere Desktop client.

How Do I Test Event Settings by Using OMSA to Simulate a Temperature Hardware Fault?

To make sure that events are functioning correctly:

1. In the OMSA user interface, navigate to **Alert Management** > **Platform Events**.
2. Select the **Enable Platform Event Filter Alerts** check box.
3. Scroll down to the bottom, and click **Apply Changes**.
4. To make sure that a specific event is enabled, such as temperature warning, from the tree on the left, select **Main System Chassis**.
5. Under **Main System Chassis**, select **Temperatures**.
6. Select the **Alert Management** tab, and select **Temperature Probe Warning**.
7. Select the **Broadcast a Message** check box, and select **Apply Changes**.
8. To cause the temperature warning event, from the tree view on the left, select **Main System Chassis**.
9. Select **Temperatures** under **Main System Chassis**.
10. Select the **System Board Ambient Temp** link, and select the **Set to Values** option button.
11. Set the **Maximum Warning Threshold** to below the current listed reading; for example if the current reading is 27, set the threshold to **25**.
12. Select **Apply Changes**, and the temperature warning event is generated. To cause another event, restore the original settings using the same **Set to Values** option. Events are generated as warnings, and then to a normal state. If everything is working properly, navigate to the **vCenter Tasks & Events** view; a temperature probe warning event should be displayed.

    NOTE: There is a filter for duplicate events; if you try to trigger the same event too many times in a row, you will only receive one event. Allow at least 30 seconds between events to see all events.

I Have the OMSA Agent Installed on a Dell Host System, But I Still Get an Error Message That OMSA is Not Installed. What Should I Do?

To resolve this issue on an 11th generation server:

1. Install **OMSA** with the **Remote Enablement** component on the host system.
2. If you are using the command line to install OMSA, make sure to specify the **-c option**. If OMSA is already installed, reinstall it with the -c option and restart the service:

```
srvadmin-install.sh -c
srvadmin-services.sh restart
```

For an ESXi host, you must install **OMSA VIB** using the **VMware Remote CLI tool**, and reboot the system.

Can the OpenManage Integration for VMware vCenter Support ESXi with Lockdown Mode Enabled?

Yes. Lockdown Mode is supported in this release on hosts ESXi 5.0 and above.

When I tried to use lockdown mode, it failed.

When I added a host to the connection profile in lockdown mode, the inventory kicked off but failed stating that “No Remote Access Controller was found or Inventory is not supported on this host.” Inventory is supposed to work for a host in lockdown mode, right?

If you put the host in lockdown mode or remove a host from lockdown mode, you must wait 30–minutes before performing the next operation on the OpenManage Integration for VMware vCenter.

What Setting Should I Use For UserVars.CIMoeMProviderEnable With ESXi 4.1 U1?

Set **UserVars.CIMoemProviderEnabled** to 1.

I Am Using A Reference Server to Create a Hardware Profile But it Failed. What Should I Do?

Check to make sure that minimum recommended versions of iDRAC firmware, Lifecycle Controller firmware, and BIOS are installed.

To make sure that the data retrieved from the reference server is current, enable **Collect System Inventory On Restart (CSIOR)**, and restart the reference server prior to extraction of data.

I Am Attempting to Deploy ESXi on a Blade Server and it Failed. What Should I Do?

1. Make sure the **ISO location (NFS path)** and staging **folder paths** are accurate.
2. Make sure the **NIC** selected during assignment of server identity is on the same network as the virtual appliance.
3. If using **static IP address**, make sure the network information provided (including subnet mask and default gateway) is accurate. In addition, , make sure the IPaddress is not already assigned on the network.
4. Make sure at least one **Virtual Disk** is seen by the system. ESXi also installs to an internal RIPS SD card.

Why are My Hypervisor Deployments Failing on my Dell PowerEdge R210 II Machines?

A timeout issue on Dell PowerEdge R210 II systems produces a hypervisor deployment failure error due to the failure of the BIOS to boot from the attached ISO. To resolve this issue, manually install hypervisor on the machine.

The NFS Share is Set Up With the ESXi ISO, but Deployment Fails with Errors Mounting the Share Location.

To find the solution:

1. Make sure the iDRAC is able to ping the appliance.
2. Make sure your network is not running too slow.
3. Make sure the ports: 2049, 4001 - 4004 are open and the firewall is set accordingly.

How Do I Force Removal of the Virtual Appliance?

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, and then click **Invoke method**.
7. Enter the extension key to unregister com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient, and then click **Invoke method**.
8. In the vSphere Web client, power off the OpenManage Integration for VMware vCenter and delete it. The key to unregsiter must be for the Web Client.

Entering a Password in the Backup Now Screen Receives an Error Message

If you are using a low resolution monitor, the Encryption Password field is not visible from the BACKUP NOW window. You must scroll down the page to enter the encryption password.

In the vSphere Web Client, Clicking the Dell Server Management Portlet Or the Dell Icon Returns A 404 Error.

Check if the appliance is running; if not, then restart it from the vSphere Web client. Wait for a few minutes for the virtual appliance Web service to start, and refresh the page. If the error continues, try and ping the appliance using the IP address or fully-qualified domain name from a command line. If the ping does not resolve, review your network settings to make sure they are correct.

My Firmware Update Failed. What Do I Do?

Check the virtual appliance logs to see if the tasks timed out. If so, iDRAC needs to be reset by performing a cold reboot. Once the system is up and running, check to see if the update was successful by either running an inventory or using the Firmware tab.

My vCenter Registration Failed. What Can I Do?

vCenter registration can fail due to communication issues, therefore if you are experiencing these issues, one 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: Make sure that the virtual appliance can resolve the DNS server you entered.

Performance during Connection Profile Test Credentials is extremely 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 iDRAC console, and choose one of the following:
   - iDRAC 6 : Select **iDRAC settings** > **Network/Security tab** > **Users tab**.
   - iDRAC 7 : Select **iDRAC settings** > **Users tab**.
   - iDRAC 8 : Select **iDRAC settings** > **Users tab**.
4. To edit the settings, in the User ID column, click the link for the admin (root) user.
5. Click **Configure User**, and then click **Next**.
6. In the User Configuration page for the selected user, select the check box next to Enable user, and then and click **Apply**.

Does the OpenManage Integration for VMware vCenter support the VMware vCenter Server appliance?

Yes, the OpenManage Integration for VMware vCenter supports the VMware vCenter Server appliance since v2.1.

Does the OpenManage Integration for VMware vCenter support the vSphere Web Client?

Yes, the OpenManage Integration for VMware vCenter supports the VMware vSphere Web client.

Why is my firmware level still not updated when I have performed firmware update with Apply on Next reboot option and the system was rebooted?

To update firmware, run the inventory on the host after the reboot is completed. In some cases, 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.

Why is the host still shown under the chassis even after removing the host from the vCenter tree?

The hosts under the chassis are identified as part of the chassis inventory. After a successful chassis inventory, the host list under the chassis is updated. Therefore, even if the host is removed from the vCenter tree, the host still shows under the chassis till the next chassis inventory is run.

In the Administration Console, why the Update Repository Path is not set to default path after I reset the 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 default path.

Resolution: In the Administration Console, manually copy the path in the **Default Update Repository** field to **Update Repository Path** field.

After backup and restore of OpenManage Integration for VMware vCenter, why alarm settings are not restored?

Restoring the OpenManage Integration for VMware vCenter appliance backup does not restore all the Alarm settings. However, in the OpenManage Integration for VMware GUI, the **Alarms and Events** field displays the restored settings.

Resolution: In the OpenManage Integration for VMware GUI, in the **Manage** > **Settings** tab, manually change the **Events and Alarms** settings.

Contacting Dell

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Go to dell.com/support
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

OpenManage Integration for VMware vCenter Related Information

- View or download Dell server documentation for PowerEdge™ Servers: Dell PoweEdge manuals
- Dell OpenManage System Administrator documents: Dell OMSA documents
- Dell Lifecycle Controller documentation: DLCI documentation

42

Virtualization-related Events For Dell PowerEdge Servers

The following table contains virtualization-related critical and warning events, including event name, description and severity level for 11th, 12th, and 13th generation of PowerEdge servers.

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers

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

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

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

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended 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 exceeded its warning threshold.	Warning	No action
Dell - Temperature sensor detected a failure value	A temperature sensor on the backplane board, system board, or drive carrier in the specified system exceeded its failure threshold value.	Error	Put the system into maintenance mode
Dell - Temperature sensor detected a non-recoverable value	A temperature sensor on the backplane board, system board, or drive carrier in the specified system detected an error from which it cannot recover.	Error	No action
Dell - Fan sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action
Dell - Fan sensor detected a warning value	Fan Sensor reading in the host <x> exceeded a warning threshold value.	Warning	No Action
Dell - Fan sensor detected a failure value	A fan sensor in the specified system detected the failure of one or more fans.	Error	Put the system into maintenance mode
Dell - Fan sensor detected a nonrecoverable value	A fan sensor detected an error from which it cannot recover.	Error	No action
Dell - Voltage sensor returned to a normal value	Sensor Returned to Normal Value	Info	No action

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended 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	Controller warning. Refer to the Tasks & Events tab on the vSphere client for details.	Warning	No action
Dell - Storage: Controller failure	Controller failure. Refer to the Tasks & Events tab on the vSphere client for details.	Error	Put the system into maintenance mode
Dell - Storage: Channel Failure	Channel failure.	Error	Put the system into maintenance mode
Dell - Storage: Enclosure hardware information	Enclosure hardware information.	Info	No action
Dell - Storage: Enclosure hardware warning	Enclosure hardware warning.	Warning	No action
Dell - Storage: Enclosure hardware failure	Enclosure hardware error.	Error	Put the system into maintenance mode
Dell - Storage: Array disk failure	Array disk failure.	Error	Put the system into maintenance mode
Dell - Storage: EMM failure	EMM failure.	Error	Put the system into maintenance mode
Dell - Storage: power supply failure	Power supply failure.	Error	Put the system into maintenance mode
Dell - Storage: temperature probe warning	Physical disk temperature probe warning, too cold or too hot	Warning	No action
Dell - Storage: temperature probe failure	Physical disk temperature probe error, too cold or too hot.	Error	Put the system into maintenance mode
Dell - Storage: Fan failure	Fan failure.	Error	Put the system into maintenance mode
Dell - Storage: Battery warning	Battery warning.	Warning	No action
Dell - Storage: Virtual disk degraded warning	Virtual disk degraded warning.	Warning	No action
Dell - Storage: Virtual disk degraded failure	Virtual disk degraded failure	Error	Put the system into maintenance mode

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended action
Dell - Storage: Temperature probe information	Temperature probe information	Info	No action
Dell - Storage: Array disk warning	Array disk warning.	Warning	No action
Dell - Storage: Array disk information	Array disk information.	Info	No action
Dell - Storage: Power supply warning	Power supply warning.	Warning	No action
Dell - Chassis Intrusion - Physical Security Violation	Chassis Intrusion - Physical Security Violation	Error	No Action
Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	Chassis Intrusion (Physical Security Violation) Event Cleared	Info	No Action
Dell - CPU Presence (Processor Presence detected)	CPU Presence (Processor Presence detected)	Info	No Action
Dell - System Event Log (SEL) Full (Logging Disabled)	System Event Log (SEL) Full (Logging Disabled)	Error	No Action
Dell - System Event Log (SEL) Cleared	System Event Log (SEL) Cleared	Info	No Action
Dell - SD Card redundancy Has Returned to Normal	SD Card redundancy Has Returned to Normal	Info	No Action
Dell - SD Card Redundancy has been Lost	SD Card Redundancy has been Lost	Error	No Action
Dell - SD Card Redundancy Degraded	SD Card Redundancy Degraded	Warning	No Action
Dell - Module SD Card Present (SD Card Presence Detected)	Module SD Card Present (SD Card Presence Detected)	Info	No Action
Dell - Module SD Card Failed (Error)	Module SD Card Failed (Error)	Error	No Action
Dell - Module SD Card Write Protect(Warning)	Module SD Card Write Protect (Warning)	Warning	No Action
Dell - Module SD Card not Present	Module SD Card not Present	Info	No Action
Dell - Watchdog Timer Expired	Watchdog Timer Expired	Error	No Action
Dell - Watchdog Reset	Watchdog Reset	Error	No Action
Dell - Watchdog Power Down	Watchdog Power Down	Error	No Action
Dell - Watchdog Power cycle	Watchdog Power cycle	Error	No Action
Dell - System Power Exceeds PSU Wattage	System Power Exceeds PSU Wattage	Error	No Action
Dell - System Power Exceeds Error Cleared	System Power Exceeds Error Cleared	Info	No Action
Dell - Power Supply Inserted	Power Supply Inserted	Info	No Action

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended action
Dell - Internal Dual SD Module is present	Internal Dual SD Module is present	Info	No Action
Dell - Internal Dual SD Module is online	Internal Dual SD Module is online	Info	No Action
Dell - Internal Dual SD Module is operating normally	Internal Dual SD Module is operating normally	Info	No Action
Dell - Internal Dual SD Module is write protected	Internal Dual SD Module is write protected	Warning	No Action
Dell - Internal Dual SD Module is writable	Internal Dual SD Module is writable	Info	No Action
Dell - Integrated Dual SD Module is absent	Integrated Dual SD Module is absent	Error	No Action
Dell - Integrated Dual SD Module redundancy is lost	Integrated Dual SD Module redundancy is lost	Error	No Action
Dell - Internal Dual SD Module is redundant	Internal Dual SD Module is redundant	Info	No Action
Dell - Internal Dual SD Module is not redundant	Internal Dual SD Module is not redundant	Info	No Action
Dell - Integrated Dual SD Module failure	Integrated Dual SD Module failure	Error	No Action
Dell - Internal Dual SD Module is offline	Internal Dual SD Module is offline	Warning	No Action
Dell - Integrated Dual SD Module redundancy is degraded	Integrated Dual SD Module redundancy is degraded	Warning	No Action
Dell - SD card device has detected a warning	SD card device has detected a warning	Warning	No Action
Dell - SD card device has detected a failure	SD card device has detected a failure	Error	No Action
Dell - Integrated Dual SD Module warning	Integrated Dual SD Module warning	Warning	No Action
Dell - Integrated Dual SD Module information	Integrated Dual SD Module information	Info	No Action
Dell - Integrated Dual SD Module redundancy information	Integrated Dual SD Module redundancy information	Info	No Action
Dell - Network failure or critical event	Network failure or critical event	Error	No Action
Dell - Network warning	Network warning	Warning	No Action
Dell - Network information	Network information	Info	No Action
Dell - Physical disk failure	Physical disk failure	Error	No Action
Dell - Physical disk warning	Physical disk warning	Warning	No Action
Dell - Physical disk information	Physical disk information	Info	No Action
Dell - An error was detected for a PCI device	An error was detected for a PCI device	Error	No Action

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended action
Dell - A warning event was detected for a PCI device	A warning event was detected for a PCI device	Warning	No Action
Dell - An informational event was detected for a PCI device	An informational event was detected for a PCI device	Info	No Action
Dell - Virtual Disk Partition failure.	Virtual Disk Partition failure.	Error	No Action
Dell - Virtual Disk Partition warning.	Virtual Disk Partition warning.	Warning	No Action
Dell - Cable failure or critical event	Cable failure or critical event	Error	No Action
Dell - Chassis Management Controller detected an error.	Chassis Management Controller detected an error.	Error	No Action
Dell - IO Virtualization failure or critical event.	IO Virtualization failure or critical event.	Error	No Action
Dell - Link status failure or critical event.	Link status failure or critical event.	Error	No Action
Dell - System: Software configuration failure.	System: Software configuration failure.	Error	No Action
Dell - Storage Security failure or critical event.	Storage Security failure or critical event.	Error	No Action
Dell - Chassis Management Controller audit failure or critical event.	Chassis Management Controller audit failure or critical event.	Error	No Action
Dell - Power Supply audit failure or critical event.	Power Supply audit failure or critical event.	Error	No Action
Dell - Power usage audit failure or critical event.	Power usage audit failure or critical event.	Error	No Action
Dell - Configuration: Software configuration failure.	Configuration: Software configuration failure.	Error	No Action
Dell - Chassis Management Controller detected a warning.	Chassis Management Controller detected a warning.	Warning	No Action
Dell - Link status warning.	Link status warning.	Warning	No Action
Dell - Security warning.	Security warning.	Warning	No Action
Dell - System: Software configuration warning.	System: Software configuration warning.	Warning	No Action
Dell - Storage Security warning.	Storage Security warning.	Warning	No Action
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 - PCI device audit warning.	PCI device audit warning.	Warning	Put the system into maintenance mode
Dell - Power Supply audit warning.	Power Supply audit warning.	Warning	No Action

Table 11. Virtualization-related Events of 11th, 12th, and 13th Generation PowerEdge Servers (continued)

Event Name	Description	Severity	Recommended action
Dell - Power usage audit warning.	Power usage audit warning.	Warning	No Action
Dell - Security configuration warning.	Security configuration warning.	Warning	No Action
Dell - Configuration: Software configuration warning.	Configuration: Software configuration warning.	Warning	No Action

A

Topics:

- Security Roles and Permissions

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 that could lead to issues. The Backup Database are fully encrypted using custom security phrases, and therefore the data cannot be misused.

By default, users in the Administrators group have all the privileges. Administrators can use all the functions of the OpenManage Integration for VMware vCenter within VMware vSphere Client or Web Client. If you want a user with necessary privileges to manage the product, then create a role with necessary privileges, assign the role to a user, register a vCenter server using the user, and include both the Dell roles.

Data Integrity

Communication between the OpenManage Integration for VMware vCenter , Administration Console, and vCenter is accomplished using SSL/HTTPS. The OpenManage Integration for VMware vCenter generates an SSL certificate used for trusted communication between vCenter and the appliance. It also verifies and trusts the vCenter server's certificate before communication and the OpenManage Integration for VMware vCenter registration. OpenManage Integration for VMware vCenter Console tab (in 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-site request forgeries to fail.

A secure Administration Console session has a five minutes idle timeout, and the session is only valid in the current browser window and/or tab. If the user tries to open the session in a new window or tab, a security error is created that asks for a valid session. This action also prevents the user from clicking any malicious URL that could try to attack the Administration Console session.

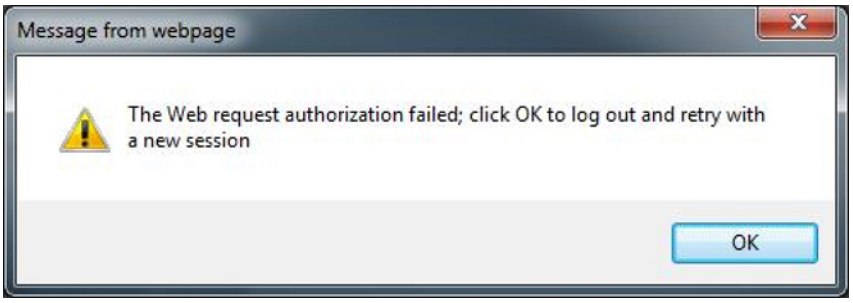

Figure 2. Error Message

Access Control Authentication, Authorization, and Roles

The OpenManage Integration for VMware vCenter uses the web Client's current user session and the stored administration credentials for the OpenManage Integration to perform vCenter operations. 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). Access Roles on the VMware vCenter Home page.

Dell Operational 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 12. 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

This role contains the privileges specifically 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

Understanding Privileges

Every action performed by the OpenManage Integration for VMware vCenter is associated with a privilege. The following sections list the available actions and the associated privileges:

- Dell.Configuration.Perform vCenter-Related Tasks
  - Exit and enter maintenance mode
  - Get the vCenter user group to query the permissions
  - Register and configure alerts, for example enable/disable alerts on the event settings page
  - Post events/alerts to vCenter
  - Configure event settings on the event settings page
  - Restore default alerts on the event settings page
  - Check DRS status on clusters while configuring alerts/events settings
  - Reboot host after performing update or any other configuration action
  - Monitor vCenter tasks status/progress
  - Create vCenter tasks, for example firmware update task, host configuration task, and inventory task
  - Update vCenter task status/progress
  - Get host profiles
  - Add host to data center
  - Add host to cluster
  - Apply profile to host
  - Get CIM credentials
  - Configure hosts for compliance
  - Get the compliance tasks status
- Dell.Inventory.Configure ReadOnly
  - Get all vCenter hosts to construct the vCenter tree while configuring connection profiles
  - Check if the host is a Dell server when the tab is selected
  - Get the vCenter's Address/IP

- Get host IP/Address
- Get the current vCenter session user based on the vSphere client session ID
- Get the vCenter inventory tree to display the vCenter inventory in a tree structure.

- Dell.Monitoring.Monitor
  - Get host name for posting the event
  - Perform the event log operations, for example get the event count, or change the event log settings
  - Register, unregister, and configure events/alerts – Receive SNMP traps and post events
- Dell.Configuration.Firmware Update
  - Perform firmware update
  - Load firmware repository and DUP file information on the firmware update wizard page
  - Query firmware inventory
  - Configure firmware repository settings
  - Configure staging folder and perform update 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

B