OpenManage Integration for VMware vCenter Quick Install Guide for vSphere Desktop Client Version 3.2

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.

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

Contents

Installing OpenManage Integration for VMware vCenter

Installation introduction

This guide provides step-by-step instructions for installing and configuring the OpenManage Integration for VMware vCenter (OMIVV). Once the installation is complete, see *OpenManage Integration for VMware vCenter User's Guide* available at **dell.com/support/manuals** for information about all aspects of administration including inventory management, monitoring and alerting, updating firmware, deployments and provisioning, and warranty management.

Prerequisites

The following information is needed before you start installing OMIVV:

- TCP/IP address information to be assigned to the OMIVV virtual appliance.
- A user name and password for the OMIVV to access the vCenter server. This user should be an administrator role that has all needed permissions. For information on the available OMIVV roles within vCenter, see *OpenManage Integration for VMware vCenter User's Guide* available at **dell.com/support/manuals**.
- Root password for ESXi host systems or the active directory credentials, which has admin rights on the host.
- User name and password associated with iDRAC Express or Enterprise.
- Make sure that vCenter server and vSphere client are available.
- Location of the OMIVV OVF file.
- Your VMware vSphere environment must meet the virtual appliance, port access, and listening port requirements. In addition, OMIVV URL must be in the trusted sites of Internet Explorer browser.

> **NOTE:**
> Install Adobe Flash Player on the vSphere client system. For accessing from Windows Server 2012 and later, you must enable the **Desktop Experience Feature** to enable the flash player for Internet Explorer browser. Install the OMIVV (virtual appliance) on any ESXi host. For more information on the supported Flash Player version, see the *OpenManage Integration for VMware vCenter Compatibility Matrix.*

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

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 **NOTE: The OMIVV shows the VMware Tools as Running (Out-of-date) when deployed on ESXi 5.5 and later.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

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

Hardware Requirements

Following are the hardware requirements for OMIVV:

- Supported servers and minimum BIOS requirements
- Supported iDRAC versions (both deployment and management)

- OMSA support for older servers and ESXi version support (both deployment and management). For more information, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at **dell.com/support/manuals**.

Software Requirements

The vSphere environment must meet virtual appliance, port access, and listening port requirements.

VMware vSphere has both a desktop client and Web client.

For specific software requirements, see *OpenManage Integration for VMware vCenter Compatibility Matrix* available at **dell.com/support/manuals**.

OpenManage Integration for VMware vCenter Port Requirements

Port	Console
443 (https) and 80 (http)	Administration console
4433 (https)	Auto discovery and handshake
162 and 11620	SNMP trap listener
2049, 4001, 4002, 4003, 4004	NFS Share

Installation and Configuration Overview

The following information is an outline of the OMIVV installation process. To begin the actual installation, see Deploying the OMIVV OVF Using the vSphere Client.

Installation Overview

1. Install OMIVV.

    a. Make sure vCenter server is up and running.

    b. Deploy an Open Virtualization Format (OVF) file that contains the OMIVV using the vSphere client.

    c. Upload the license file.

    d. Register the OMIVV with vCenter server using the Administration Console.

2. Complete the steps in the Configuration Wizard.
3. Enable Dell events to set up event filter options on the Settings page.
4. Enable firmware updates to download firmware updates and make them available to applicable systems.
5. Configure the Dell iDRAC user name and password.

Deploying the OMIVV OVF Using the vSphere Client

This procedure assumes that you have downloaded the zip file from the Dell Web site.

To deploy the OMIVV OVF using the vSphere Client:

1. Unzip the file containing the OMIVV virtual disk, and run **setup.exe**.
2. Double-click the Setup.exe file to agree to the EULA, extract and obtain the OVF file.
3. Copy/move the OVF file to a location accessible to the VMware vSphere host to which you will upload the appliance.
4. Start the VMware vSphere client.
5. From the VMware vSphere client, select **File → Deploy OVF Template**.
6. In the **Source** window, use the **Browse** button to locate the OVF package. The location can be a local drive, network drive, CD/DVD, or from the Internet. The OMIVV file size is approximately 1.5 GB.

    > **NOTE: The install can take 10-30 minutes if the OVF package resides on a network share. For the quickest installation, it is recommended that you host the OVF on a local drive.**

7. Click **Next.**
8. In the **OVF Template Details** window, review the information presented.
9. Click **Next**.
10. In the **Name and Location** window, do the following:

    a. In the **Name** text box, enter the name of the template. This name can contain up to 80 characters.
    b. In the **Inventory Location** list, select a location to store the template.
11. Click **Next.**
12. Depending on the vCenter configuration, one of the following options displays:
    - If resource pools are configured — On the Resource Pool page, select the pool of virtual servers to which the OMIVV is deployed.
    - If resource pools are *not* configured — On the Hosts/Clusters page, select the host or cluster to which the OMIVV is deployed.
13. If there is more than one datastore available on the host, the Datastore page is displayed. Select the location to store OMIVV files, and click **Next**.
14. In the **Disk Format** window, select the format in which you want to store the virtual disks:

    a. **Thick Provision Lazy Zeroed**
        A lazy-zeroed thick disk has all the disk space allocated at the time of creation, but each block is zeroed only on first write. This results in a shorter creation time, but reduces the performance the first time a block is written to. Subsequent writes have the same performance as eager-zeroed thick disks.

    b. **Thick Provision Eager Zeroed [Recommended]**
        An eager-zeroed thick disk has all the space allocated and zeroed out at the time of creation. This increases the time it takes to create the disk, but results in the best performance, even on the first write to each block.

    c. **Thin Provision [Not Recommended]**
        Space required for a thin-provisioned virtual disk is allocated and zeroed upon first write, as opposed to upon creation. There is a higher I/O cost (similar to that of lazy-zeroed thick disks) during the first write to an unwritten file block, but on subsequent writes thin-provisioned disks have the same performance as eager-zeroed thick disks.
15. Click **Next**.
16. Select the appropriate network for the appliance under **Destination Networks** and click **Next**.

    ✎ NOTE: It is recommended that OMIVV and vCenter Server are on the same network.
17. In the **Ready to Complete** window, review the selected options for the OVF deployment task and select **Power on after deployment** and click **Finish**. The deployment job runs and provides a completion status window where you can track the job progress.

Registering a vCenter server by using a user with necessary privileges

You can register vCenter servers for the OMIVV appliance with vCenter administrator credentials of the vCenter server or a user with 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 relevant 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 vSphere client. See Defining privileges to select all the relevant 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 and their role to the relevant inventory object. See VMware vSphere documentation for more information on assigning permissions in the vSphere client. A vCenter server user with the required privileges can now register and/or unregister vCenter.

    ✎ NOTE: The vCenter administrator should assign permissions in the vSphere client.
3. Register a vCenter server in the administration console by using a user with necessary privileges. See Registering a vCenter server by using a user with necessary privileges.
4. Associate the Dell privileges to the role created or modified in step 1 for performing the OMIVV operations. See Assigning Dell privileges to the role.

Now, a user with the required privileges can experience the OMIVV features with Dell hosts.

Defining privileges

To enable a 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: If the mentioned privileges are not assigned, an error message is displayed while registering a vCenter server by using a user with the available privileges.

Registering a vCenter server by using a user with necessary privileges

You can register a vCenter server for the OMIVV appliance by using a user with the required privileges. See step 21 of Registering OMIVV within vCenter And Importing The License File for more information on registering a vCenter server.

Assigning Dell privileges to the role

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

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

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

1. Log in to the vSphere client with administrative rights.
2. On the vSphere client **Home** page, click **Roles**.
3. Right-click the role to edit and select **Edit Role**.
4. Select the following privileges for Dell Infrastructure Deployment Role, Dell Operational Role, and click **OK**.
   - Dell

     – Dell.Configuration
     – Dell.Deploy-Provisioning
     – Dell.Inventory
     – Dell.Monitoring
     – Dell.Reporting

   See the Security Roles and Permissions section in *OpenManage Integration for VMware vCenter User's Guide* 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.

Registering OMIVV within vCenter And Importing The License File

Perform the following steps to register a vCenter server:

1. From vSphere client, select **Home → Hosts and Clusters**, then in the left panel, locate the deployed OMIVV, and then click **Power on the virtual machine** if not powered on already.
2. Click the **Console** tab in the main VMware vCenter window to initiate the Administration Console.
3. Allow the OMIVV to finish booting up and then enter the user name as **admin** and press **Enter**.
4. Enter a new admin password. The password must be set as per the password complexity rules displayed. Press **Enter**.
5. Re-enter the password that was provided earlier and press **Enter**.

   Press **Enter** to configure the network and time zone information in the OMIVV appliance.
6. To configure the OMIVV time zone information, click **Date/Time Properties** to set the time zone and date.
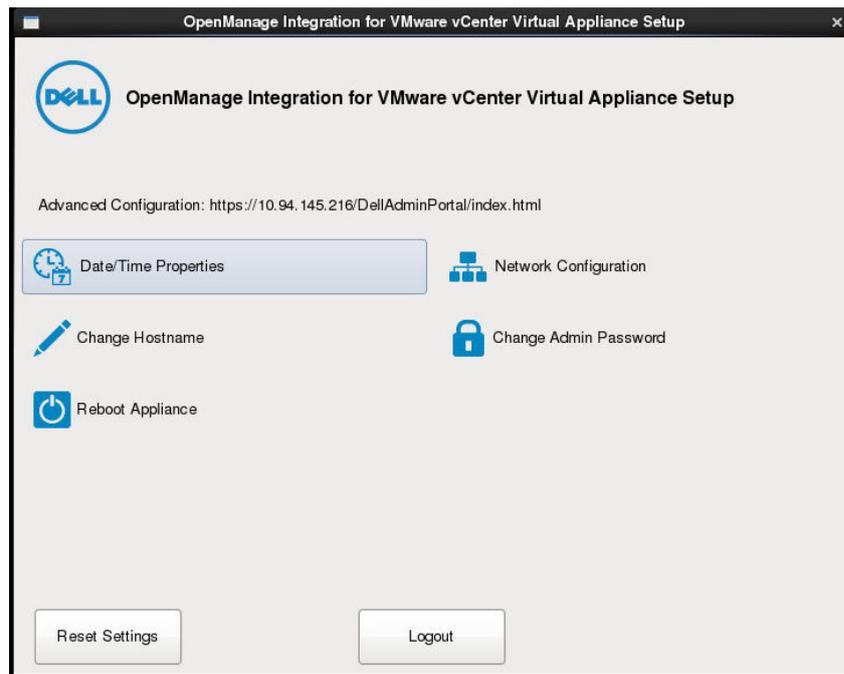
Figure 1. Console tab

7. In the **Date and Time** tab, select **Synchronize date and time over the network**.
    The NTP Servers box is displayed.
8. Add valid NTP server details to which your vCenter is synchronized with.
9. Click **Time Zone**, and select the applicable time zone and click **OK**.
10. To configure static IP to the OMIVV appliance, click **Network Configuration** or, skip to step 17.
11. Select **Auto eth0**, and then click **Edit**.
12. Select the **IPV4 Settings** tab and select **Manual** in the **Method** drop-down.
13. Click **Add** and add a valid IP Address Netmask and Gateway information.
14. Add the DNS Server detail in the **DNS Servers** field.
15. Click **Apply**.
16. To change the hostname of OMIVV appliance, click **Change Hostname**.
17. Enter a valid hostname and click **Update hostname**.
18. Open a Web browser and type the IP address or hostname of the appliance.
    For example: **https://10.210.126.120** or **https://myesxihost**. The URL is not case-sensitive.
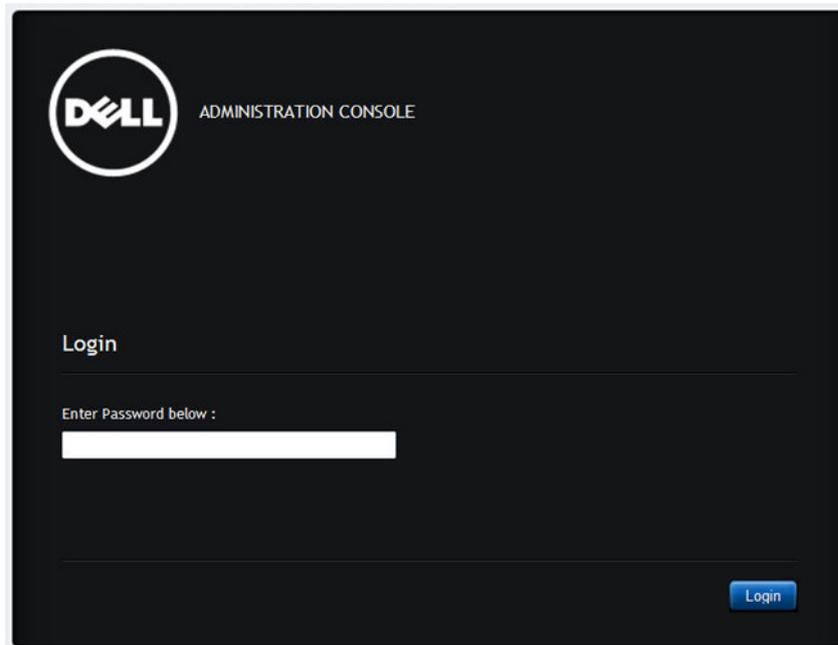
Figure 2. Administration Console

19. In the **Administration Console** login window, enter the password, and then click **Login**.
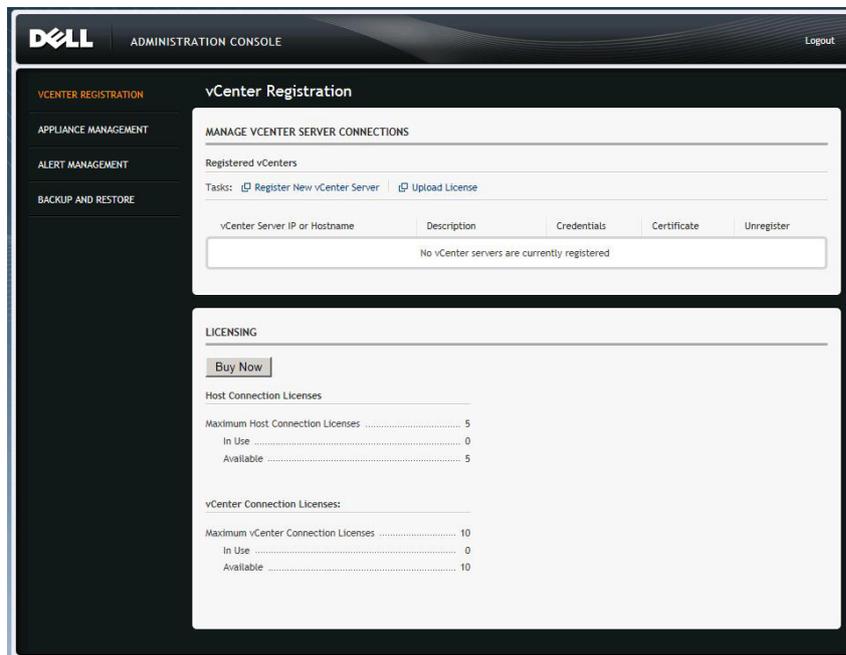
Figure 3. vCenter Registration Window from within the Administration Console

20. In the **vCenter Registration** window, click **Register a new vCenter Server**.
21. In the **Register a New vCenter** window, do the following:
    a. Under **vCenter Name**, in the **vCenter Server IP or Hostname** text box, enter the server IP or hostname and then in the **Description** text box, enter the description, which is optional.
    b. Under **vCenter User Account**, in the **vCenter User Name** text box, enter the Admin user name or the user name with the necessary privileges. Enter the username as domain\user or domain/user or user@domain. The Admin user account or the user name with the necessary privileges is used by the OMIVV for vCenter administration.

> ✐ NOTE: One instance of OMIVV can support up to 10 vCenters which are part of the same vCenter SSO. Multiple independent instances of vCenters are not currently supported.

> ✐ NOTE: Registering OMIVV using Fully Qualified Domain Name (FQDN) is highly recommended. For FQDN based registrations, the host name of the vCenter should be properly resolvable by the DNS server.

    c. In the **Password** text box, enter the password.

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

22. Click **Register**.

23. Do one of the following:

   - If you are using the OMIVV trial version, go to step 25.

   - If you are using the full product version, there is a **license.xml** file that is sent as an attachment to the registered e-mail. This file contains your product license, and you must import this license to your virtual appliance. To import the license file, click **Upload License.**

24. In the **Upload License** window, click the **Browse** button to navigate to the license file. Click **Upload** to import the license file.

> ✐ NOTE: If the license file is modified or edited, the license file does not work.

25. Once the OMIVV is registered, the OMIVV icon is displayed under the **Management** category of the vCenter home page.
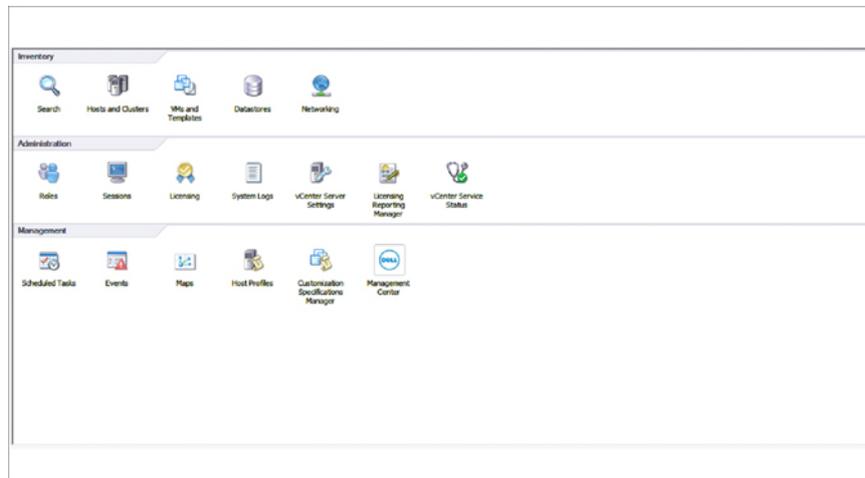

Figure 4. The OMIVV Successfully Added to vCenter

> ✐ 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 machine into maintenance mode or reboot the host.

Installation Verification

The following steps verify that the OMIVV installation is successful:

1. Log on to vSphere client and confirm that the OMIVV icon appears inside the vSphere Client. If it does not, restart the vSphere Client and check again.

2. Check that vCenter can communicate with the OMIVV by attempting a ping command from the vCenter server to the virtual appliance IP address or hostname.

3. In **vSphere Client**, click **Plug-in → Managed Plug-in.** In the **Plug-in Manager** window verify that the OMIVV is installed and enabled.

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 proxySee Setting Up a Proxy Server.

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 Recovering OMIVV after unregistering the earlier plug-in version 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 Deploy Plug-In OVF Using the vSphere Client.

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 Registering OMIVV within vCenter And Importing The License File.

    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 Registering OMIVV and Importing The License File.

8. Verify the appliance.

   For more information, see the Installation Verification 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**.

Recovering OMIVV after unregistering earlier version of OMIVV

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

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

1. Perform step 3 through step 5 in Migrating from 2.x to 3.2.
2. Register the plug-in to the same vCenter that you had registered in the earlier plug-in.
3. To complete the migration, perform step 6 through step 8 in Migrating from 2.x to 3.2.

Configuring OpenManage Integration for VMware vCenter

After you do the basic installation of the OMIVV, it should be configured. This is typically done using the Configuration Wizard, but you can also do it using the Settings page options in the Dell Management Center.

The user interface in both the pane is similar except in the wizard, you **Save and Continue**, whereas in the **Settings** options you click **Apply**.

This section tells you how to configure using the wizard. For information about using the Dell Management Center's **Settings** options for configuring the OMIVV, see *OpenManage Integration for VMware vCenter User's Guide* available at **dell.com/support/manuals**.

Configuration Wizard welcome page

After you install the OMVV, it must be configured.

1. In **vSphere Client**, from the **Home** page, under the **Management** tab, click the **Dell Management Center** icon.
   The first time you click the **Dell Management Center** icon, it opens the **Configuration Wizard**. You can also access this wizard on the **Dell Management Center → Settings** page.
2. In the **Welcome** tab, review the steps, and then click **Next**.

Creating a new Connection Profile [Wizard]

A connection profile stores the 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 might assign multiple servers to a single connection profile. Creating the Connection Profile is similar between the Configuration Wizard and the Dell Management Center, under **Settings** option. You can configure OMIVV to connect to iDRAC and Host using Active directory credential. Prior to 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. The active directory credential can be same for both iDRAC and host or it can be set as separate active directory credential. The user credential must have administrative privilege.

> **NOTE: With installations on hosts that are using 12th or later generation of the Dell PowerEdge servers, the OMSA agent installation is not required. For installations on 11th generation servers, OMSA agent is automatically installed during the deployment process.**

> **NOTE: You are not allowed to 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 wizard, perform the following steps:

1. From the **Connection Profiles** tab, click **Create New**.
2. In the **Profile Name and Description** panel, enter the profile name, and a description that is optional that are used to help manage custom connection profiles, and then click **Next**.
3. In the **Associated Hosts** section, select the hosts to be associated with the Connection Profile, and then click **Next**.
4. View the information about credentials and connection protocols and click **Next**.
5. In the iDRAC panel, type the iDRAC credential information.

a. For iDRACs already configured and enabled for Active Directory on which you want to use Active Directory, select the **Use Active Directory** check box; otherwise configure the iDRAC local credentials. Enter **User Name**, **Password**, and **Verify Password**. The user name can contain up to 16 characters including white space. The passwords must match and use ASCII-printable characters only.

b. For **Certificate Check**, select **Enable** to download and store the iDRAC certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.

6. Click **Next**.

7. In the **Host Root Credentials** panel, do the following:

a. You must select the **Use Active Directory** check box to enable active directory credentials. Enter the User Name, Password, and Verify Password.

b. If you do not select **Use Active Directory**, enter the **Password**, for the **root** user and **verify password**. The passwords must match.

c. For **Certificate Check**, select **Enable** to download and store the OMSA/ESXi certificate and validate it during all future connections, or select **Disable** to perform no check and not store the certificate.

8. Click **Next**.

9. The **Test Connection** window tests the entered iDRAC and Host root Credentials on the selected servers. Test connection is optional but is recommended.

   - To begin the test, select the hosts, and click **Test Selected**. The other options are disabled.
   - To abort all the tests before completion, click **Abort All Tests**.

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

11. To continue on to configure Events and Alarms, click **Save and Continue**.

Configuring Events And Alarms [Wizard]

Configure events and alarms using the Configuration Wizard or from the Dell Management Center, Settings option for Events and Alarms. In order to receive the events from the servers, OMIVV is configured as the trap destination. For 12th generation hosts and later, the SNMP trap destination is set in iDRAC. For hosts prior to 12th generation, trap generation is set in OMSA.

> 📝 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.

To configure events and alarms, perform the following steps:

1. In the **Configuration Wizard**, under **Event Posting Levels**, select one of the following:
   - Do not post any events — Blocks hardware events.
   - Post All Events — Posts all hardware events.
   - Post only Critical and Warning Events — Posts only critical or warning level hardware events.
   - Post only Virtualization-Related Critical and Warning Events — Posts only virtualization-related critical and warning events; this is the default event posting level.

2. To enable all hardware alarms, select the **Enable Alarms for Dell Hosts** check box.

   > 📝 NOTE: Dell hosts that have alarms enabled respond to critical events by entering maintenance mode.

3. In the dialog box that is displayed, click **Continue** to accept this change, or click **Cancel**.

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

4. To restore the default vCenter alarm settings for all managed Dell servers, click **Restore Default Alarms**.

   It might take up to a minute before the change takes effect.

5. To continue the wizard, click **Save and Continue**.

> 📝 NOTE: Restoring the OMIVV appliance backup does not restore all the Alarm settings. However, in the OMIVV GUI, the Alarms and Events field displays the restored settings. To resolve this issue, in the OMIVV GUI, in the Manage → Settings tab, manually change the Events and Alarms settings.

Setting Up A Proxy Server [Wizard]

Set the proxy server in the Configuration Wizard or later using the Dell Management Center, **Settings → Proxy** page.

To set up a proxy server:

1. In the **Configure HTTP Proxy window**, do one of the following:
   - To not use a proxy server, click **Save and Continue**.
   - To use a proxy server, under **Settings** enter a **Proxy Server Address**.
2. Enter the **Proxy Port number**.
3. Select the **Credentials Required** check box, if needed.
4. If you selected **Credentials Required**, do the following:
   a. In the **Proxy User Name** text box, type the proxy user name.
   b. In the **Proxy Password** text box, type the proxy password.
   c. In the **Verify Password** text box, re-type the proxy password.
5. Under **Proxy**, select the **Use Proxy** check box.
6. To save these options and continue, click **Save and Continue**.

Scheduling Inventory Jobs [Wizard]

The inventory schedule configuration is similar from the Configuration Wizard or from the **Dell Management Center → Settings** option. The only difference is that the wizard provides an option to select if you want to run the inventory immediately.

> **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.**

To schedule an inventory job:

1. In the **Configuration Wizard**, in the **Inventory Schedule** window, do one of the following:
   - To run inventory schedules, click **On Selected Days**.
   - To not run inventory schedules, select **Do not run inventory on Dell hosts**.
2. If you select **On Selected Days**, then do the following:
   a. Select the check box next to each day of the week that you want to run the inventory.
   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 **Save and Continue**.

Running A Warranty Retrieval Job [Wizard]

The warranty retrieval job configuration is similar between the wizard and from the **Dell Management Center → Settings** option. In addition, you can run the Warranty Retrieval Job now, from Job Queue.

To run a warranty retrieval job:

1. In the **Configuration Wizard**, on the **Warranty Schedule** window, do one of the following:
   - To run warranty schedules, click **On Selected Days**.
   - To not run warranty schedules, select **Do not retrieve Warranty Data**.
2. If you selected **On Selected Days**, then do the following:
   a. Select the text box next to each day of the week that you want to run the warranty jobs.
   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 **Save and Continue**.

    ![NOTE icon] **NOTE: OMIVV connects to internet to fetch the warranty information of your hosts. Depending on your network settings, you might have to configure proxy for the warranty job to run successfully.**

Configuring the Deployment Credentials [Wizard]

Deployment credentials are used to communicate securely with a bare-metal system that is discovered. For secure communication with iDRAC, OMIVV uses deployment credentials from initial discovery until the end of the deployment process.

![WARNING icon] **WARNING: This feature is not functional in this release for security reasons.**

Setting The Default Firmware Update Repository [Wizard]

Firmware repository settings contain the firmware catalog location used to update deployed servers. You can set up firmware repository initially here in the wizard or later from the Dell Management Center Settings option. In addition, you can run the firmware update later from the OpenManage Integration tab.

To set the default firmware update repository:

1. In the **Configuration Wizard**, on the **Firmware Repository** page, to choose the default repository for firmware updates, select one of the following:
    *   Dell Online

        Default firmware repository (ftp.dell.com) with a staging folder. The OMIVV downloads selected firmware updates and stores them in the staging folder, and then they are applied as necessary.

        ![NOTE icon] **NOTE: OMIVV connects to internet to get the catalog and firmware packages applicable to your hosts. Depending on your network settings, you might have to configure proxy for the firmware update task to run successfully from Dell online.**
    *   Local/shared repository

        These are created with the Dell Repository Manager application. This local repository should be a network share. OMIVV supports both NFS and CIFS shares.
2. If you selected **Local/shared repository**, 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 using a CIFS share, enter the **User Name**, **Password**, and **Verify Password**; the passwords must match. These fields are only active when entering a CIFS share.

        ![NOTE icon] **NOTE: The @ character is not supported for use in shared network folder user names/passwords.**
    c. To validate your entries click **Begin Test**.
3. To save this selection and continue the **Configuration Wizard**, click **Save and Continue**.

Enabling The OMSA Link [Wizard]

To launch OMSA within the OMIVV virtual appliance, the OMSA Web Server must be installed and configured. See *Dell OpenManage Server Administrator Installation Guide* for instructions on how to install and configure the Web Server.

![NOTE icon] **NOTE: OMSA is only required on Dell servers prior to 12th Generation.**

You can use OMSA to:

- Manage vCenter elements (detailed sensor/component-level health information).
- Clear command logs and system event logs (SELs).
- Obtain NIC statistics.
- Make sure that the OMIVV captures events from a selected host.

1. In the **Configuration Wizard**, on the **OpenManage Server Admin** page, use the **OMSA Web Server URL** text box to enter the OMSA URL. You must include the full URL including the HTTPS.
2. To save this URL and finish the Configuration Wizard, click **Finish**.

Configuring NFS Shares

To use NFS shares with the OMIVV for backup and restore operations, firmware updates, and as a staging folder, there are certain configuration items that you must complete. CIFS shares do not require additional configuration.

To configure NFS shares:

1. On the Linux or Unix OS machine hosting the NFS shares, edit **/etc/exports** to add: **/share/path <appliance IP> (rw) *(ro)**.

   This allows the virtual appliance full read and write access to the share, but limits all other users to read only.
2. Start nfs services:

```
service portmap start
service nfs start
service nfslock status
```

   📝 **NOTE: The steps above may vary depending on the Linux distribution in use.**

3. If any of the services were already running:

```
exportfs -ra
```

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.

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.**

Options after uploading Licenses

License file for new purchases

When you place an order for purchasing a new license, an email is sent from Dell about the order confirmation, and you can download the new license file from the Dell Digital store that is available at http://www.dell.com/support/licensing. The license is in an .xml format. If the license is in a .zip format, extract the license .xml file from the .zip file before uploading.

Stacking licenses

Starting from the OMIVV version 2.1, OMIVV can stack multiple standard licenses to increase the number of supported hosts to the sum of the hosts in the uploaded licenses. An evaluation license cannot be stacked. The number of supported vCenter servers cannot be increased by stacking, and requires the use of multiple appliances.

There are some restrictions around the functionality of stacking licenses. If a new standard license is uploaded before the existing standard license expires, the licenses stack. Otherwise, if the license expires and a new license is uploaded, only the number of hosts from the new license is supported. If there are already multiple licenses uploaded, the number of supported hosts are the sum of the hosts in the non-expired licenses at the time the last license was uploaded.

Expired licenses

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

Replacement of licenses

If there is a problem with your order and you receive a replacement license from Dell, the replacement license contains the same entitlement ID of the previous license. When you upload a replacement license, the license is replaced if a license was already uploaded with the same entitlement ID.

Enforcement

Appliance updates

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

Evaluation License

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

Adding hosts to connection profiles

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

4

More Configuration Information

For a complete guide on OMIVV configuration, management, and deployment options, see *OpenManage Integration for VMware vCenter User's Guide* available at **Dell.com/support/manuals**.

5

Related documentation and resources

In addition to this guide, you can access the other guides available at **dell.com/support/manuals**. On the Manuals page, click **View products** under the **Choose from all products** category. In the **All products** section, click **Software & Security** → **Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 3.2** to access the following documents:

- *OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.2*
- *OpenManage Integration for VMware vCenter for Desktop Client User's Guide Version 3.2*
- *OpenManage Integration for VMware vCenter for Web Client User's Guide Version 3.2*
- *OpenManage Integration for VMware vCenter Release Notes Version 3.2*
- *OpenManage Integration for VMware vCenter Compatibility Matrix Version 3.2*

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

Accessing documents from Dell support site

You can access the required documents in one of the following ways:

- Using the following links:

    – For all Enterprise Systems Management documents — **Dell.com/SoftwareSecurityManuals**
    – For OpenManage documents — **Dell.com/OpenManageManuals**
    – For Remote Enterprise Systems Management documents — **Dell.com/esmmanuals**
    – For OpenManage Connections Enterprise Systems Management documents — **Dell.com/ OMConnectionsEnterpriseSystemsManagement**
    – For Serviceability Tools documents — **Dell.com/ServiceabilityTools**
    – For OpenManage Connections Client Systems Management documents — **Dell.com/DellClientCommandSuiteManuals**
    – For OpenManage Virtualization Solution documents — **Dell.com/VirtualizationSolutions**
- From the Dell Support site:

    a. Go to **Dell.com/Support/Home**.

    b. Under **Select a product** section, click **Software & Security**.

    c. In the **Software & Security** group box, click the required link from the following:
        – **Enterprise Systems Management**
        – **Remote Enterprise Systems Management**
        – **Serviceability Tools**
        – **Dell Client Command Suite**
        – **Connections Client Systems Management**
        – **Virtualization Solutions**

    d. To view a document, click the required product version.
- Using search engines:

    – Type the name and version of the document in the search box.