OpenManage Integration for VMware vCenter Quick Installation Guide for vSphere Web Client Version 3.1

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.

January 2016

Rev. A00

Contents

1

Quick Start Installation

Installation Introduction

This guide provides step-by-step instructions for the installation and configuration of OpenManage Integration for VMware vCenter (OMIVV) on Dell servers. After the installation is complete, for information about all aspects of administration including: inventory management, monitoring and alerting, firmware updates, and warranty management, see the *OpenManage Integration for VMware vCenter User's Guide* available at **dell.com/support/manuals**.

Prerequisites

The following prerequisites must be fulfilled before you start the product installation:

- TCP/IP address information to be assigned to the OMIVV virtual appliance.
- A user name and password for OMIVV to access the vCenter server. This should be an administrator role that has all necessary permissions. For more information about 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 that has administrative rights on the host.
- User name and password associated with iDRAC Express or Enterprise.
- Make sure the vCenter server is currently running.
- Know the location of the OMIVV OVF file.
- Install the OMIVV (virtual appliance) on any ESXi host.
- Your VMware vSphere environment must meet virtual appliance, port access, and listening port requirements. In addition, install Adobe Flash Player on the client system. 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 impact overall functionality of the virtual appliance.

NOTE: The OMIVV shows the VMware Tools as Running (Out-of-date) when deployed on ESXi 5.5 and later.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

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

Hardware Requirements

OMIVV provides full support for several generation of Dell servers, with full feature support for servers with iDRAC Express or Enterprise. Extensive information on the platform requirements can be found in the *OpenManage Integration for VMware vCenter Release Notes* available at **Dell.com/support/manuals**. To verify that your host servers are eligible, refer to the tables in the *OpenManage Integration for VMware vCenter Compatibility Matrix* available at **Dell.com/support/manuals**.

- Supported server and minimum BIOS
- iDRAC supported versions (both deployment and management)
- OMSA support for older servers and ESXi version support (both deployment and management)

Software Requirements

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

NOTE: VMware vSphere has both a desktop client and Web client.

Requirements for Web Client

Supported for vCenter 5.5 or later.

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 number	Description
443 (https) and 80 (http)	For Administration Console
4433 (https)	For auto discovery and handshake
162 and 11620	For SNMP trap listener
2049, 4001, 4002, 4003, 4004	For NFS share

Installation and Configuration Overview

The following high-level steps outline the overall installation procedure for OMIVV. These procedures assume that the required hardware is in place and running the required VMware vCenter software.

The following information is an outline of the installation process. To begin the actual installation, see the Deploy OVF Using Web Client section.

Installation Overview

1. Install OMIVV.
    a. Be sure that systems are connected and the vCenter server is up and running.

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

c. Upload the license file.

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

2. Complete the **Initial Configuration Wizard**.

Deploying the OMIVV OVF Using the vSphere Web Client

This procedure assumes that you have downloaded and extracted the product zip file (Dell_OpenManage_Integration_<version number>.<build number>.zip) from the Dell website.

To deploy the OMIVV OVF using the vSphere Web Client:

1. Locate the OMIVV virtual disk that you downloaded and extracted and run **Dell_OpenManage_Integration.exe**.
2. Accept the **EULA** and save the OVF file.
3. Copy or move the OVF file to a location accessible to the VMware vSphere host to which you will upload the appliance.
4. Start the **VMware vSphere Web Client**.
5. From the **VMware vSphere Web Client**, select a host and in the main menu click **Actions** → **Deploy OVF Template**.

   You can also right-click **Host** and select **Deploy OVF Template.**

   The **Deploy OVF Template** wizard is displayed.
6. In the **Select Source** window, do the following:
   a. **URL**: If you want to download the OVF package from internet, select **URL**.
   b. **Local file**: If you want to select the OVF package from your local system, select the **Local file** and click **Browse**.

   NOTE: The installation can take between 10 to 30 minutes, if the OVF package resides on a network share. For a quick installation, it is recommended that you host the OVF on a local drive.
7. Click **Next.** The **Review Details** window is displayed.
8. The following information is displayed in the **Review Details** window:
   a. **Product**: The OVF template name is displayed.
   b. **Version**: The version of the OVF template is displayed.
   c. **Vendor**: The vendor name is displayed.
   d. **Publisher**: The publisher details are displayed.
   e. **Download Size**: The actual size of the OVF template in Gigabytes.
   f. **Size on Disk**: Details of thick and thin provisioned details are displayed.
   g. **Description**: You can view the comments.
9. Click **Next**. The **Select Name and Folder** window is displayed.
10. In the **Select Name and Folder** window, do the following:

    a. In **Name**, enter the name of the template. This name can contain up to 80 characters.
    b. In the **Select a folder or datacenter** list, select a location to deploy the template.
11. Click **Next.**

    The **Select Storage** window is displayed.
12. In the **Select Storage** window, do the following:

a. From the **Select Virtual Disk Format** drop-down list, select either Thick Provision (lazy Zeroed), Thick Provision (Eager zeroed), or Thin Provision to store the virtual disk. It is recommended that you select Thick Provision (Eager Zeroed).
b. From the **VM Storage Policy** drop-down list, select one of the policies.

13. Click **Next**. The **Setup Networks** window is displayed.
14. The **Setup Networks** window is displayed which contains details about the source and destination networks. Click **Next**.

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

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

    The deployment job runs and provides a completion status window where you can track 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 Web 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 Web 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 Web 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 in vSphere Web client.

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 8 of Registering OpenManage Integration for VMware vCenter and Importing The License File 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. When completed, these privileges are applied to the user or group that is assigned the edited role.

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 for Dell Infrastructure Deployment Role, Dell Operational Role, and click **OK**.
   - Dell
     - Dell.Configuration
     - Dell.Deploy-Provisioning
     - Dell.Inventory
     - Dell.Monitoring
     - Dell.Reporting

   See *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 OpenManage Integration for VMware vCenter and Importing The License File

This procedure assumes that you have received the licenses in the form of an e-mail attachment from **download_software@dell.com**. If you have more than one license, you can add the licenses one after another. The license file is available as an XML format file.

NOTE: If you want to upload a custom certificate for your appliance, you must 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 must unregister and re-register the appliance with vCenter.

1. From the vSphere Web Client, click **Home → Hosts and Clusters**, then in the left panel, locate the OMIVV that you just deployed, and click **Power on the virtual machine**.

   During deployment, if you select **Power on after Deployment**, the VM is powered on automatically after deployment is complete.
2. Click the **Console** tab in the main **VMware vCenter** window to run the **Administration Console**.
3. Allow the OMIVV to finish booting up, and then enter the user name for the administrator (the default is Admin), and then set a password.
4. Configure the OMIVV network and time zone information.

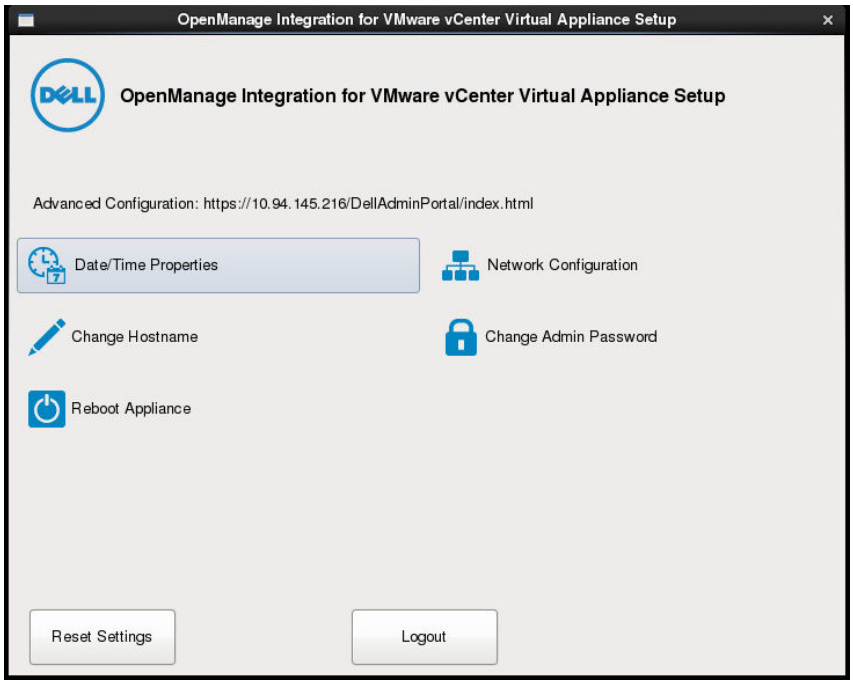

Figure 1. Console tab

5. To open the **Administration Console** for the product, open a Web browser and type the IP address or hostname of the appliance.

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

   For example: **https://10.210.126.120** or **https://myesxihost**

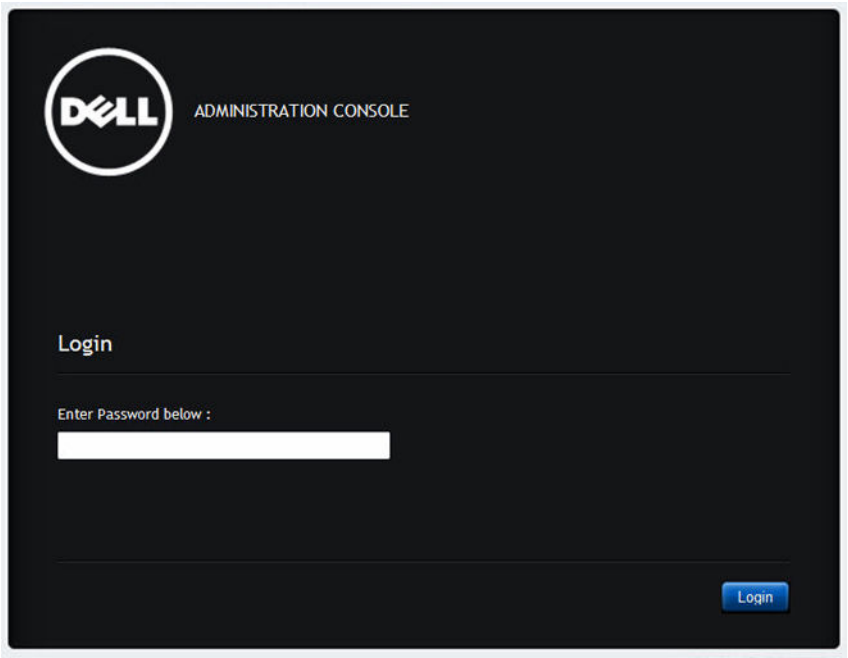

Figure 2. Administration Console

6. In the **Administration Console** login window, enter the password, and then click **Login**.

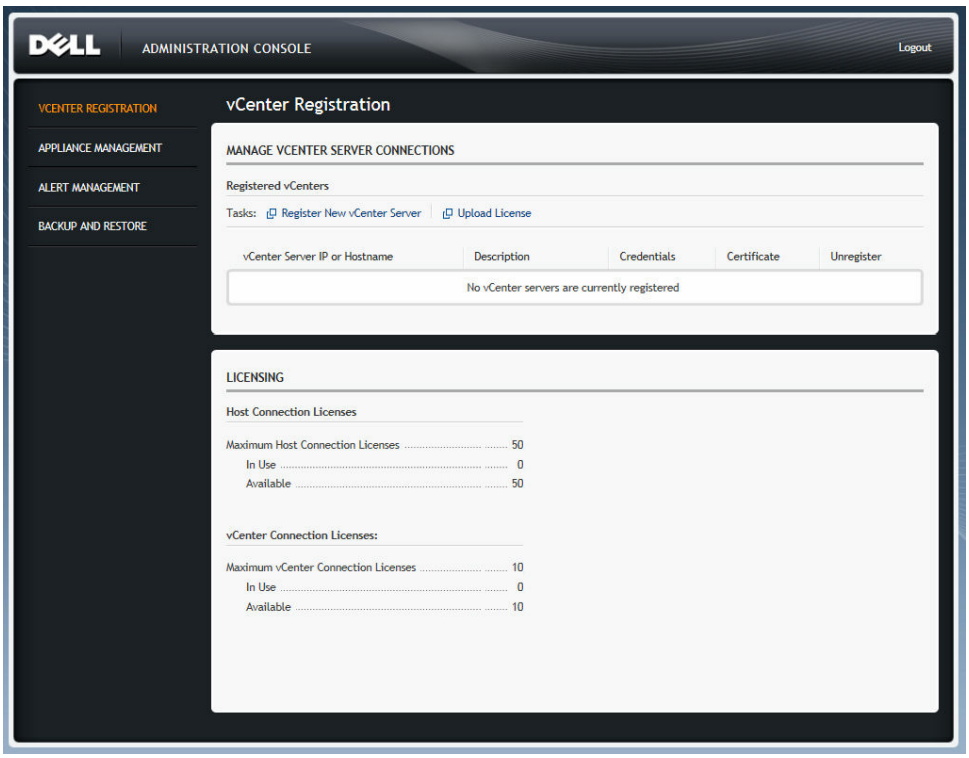

Figure 3. vCenter Registration Window from within the Administration Console

7. In the **vCenter Registration** window, click **Register New vCenter Server**.

8. In the **Register New vCenter Server** 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 that is optional.

      NOTE: Registering OpenManage Integration for VMware vCenter with the VMware vCenter using Fully Qualified Domain Name (FQDN) is highly recommended. For FQDN based registrations, the hostname of the vCenter should be properly resolvable by the DNS server.

   b. Under **vCenter User Account**, in **vCenter User Name**, enter the Admin user name or the user name with necessary privileges.

      Enter the **username** as **domain\user** or **domain/user** or **user@domain**. The Admin user account or the user with necessary privileges is used by the OMIVV administration.

   c. In **Password**, enter the password.
   d. In **Verify Password**, enter the password again.
9. Click **Register**.

   NOTE: One instance of OMIVV can support upto 10 vCenters which are a part of the same vCenter SSO. Multiple independent instances of vCenters are currently not supported.
10. Do one of the following:
    - If you are using the OMIVV trial version, go to step 12.
    - If you are using the full product version, the license file will be e-mailed to you, and you must import this license to your virtual appliance. To import the license file, click **Upload License.**
11. In the **Upload License** window, click **Browse** to navigate to the license file and then click **Upload** to import the license file.

    NOTE:
    - If the license file is modified or edited in any way, the license file will not work and you must send an e-mail with the original order number to **download_software@dell.com**. The license XML file is used in this procedure and it does not come with a hard coded file name.
    - You cannot use an individual license XML file to upload, instead use the license XML file included in a compressed file.
12. After OMIVV is registered, OMIVV is shown under the Administration category of the Web Client home page.

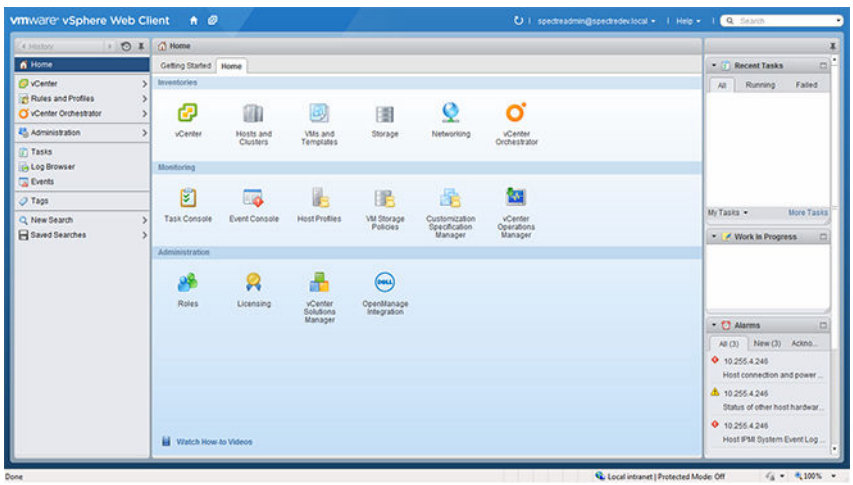

Figure 4. The OpenManage Integration for VMware vCenter Successfully Added to vCenter

NOTE: For all vCenter operations, OMIVV uses the privileges of a registered user and not the privileges of a 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 was successful:

1. Close any vSphere Client windows and start a new vSphere Web Client.
2. Confirm that the OMIVV icon appears inside vSphere Web Client.
3. Make sure that vCenter can communicate with the OMIVV by attempting a PING command from the vCenter server to the virtual appliance IP address or hostname.
4. In **vSphere Web Client**, click **Plug-ins** → **Managed Plug-ins**.
5. In the **Plug-in Manager** window verify the OMIVV is installed and enabled.

Upgrading OpenManage Integration Plugin from 3.0 version to the current version

To upgrade OpenManage Integration plug-in from version 3.0 to the current version, perform the following steps:

1. Open a web browser and enter the Administration Console URL displayed in the vSphere vCenter **Console** tab for the virtual machine you want to configure. You can also use the link displayed on the **Help and Support** page in the Dell Management Console. The URL is represented in the following format and is case-insensitive: https://<ApplianceIPAddress>
2. In the left pane of the **ADMINISTRATION CONSOLE** window, click **APPLIANCE MANAGEMENT**.
3. Depending on your network settings, enable proxy and provide proxy settings if your network needs proxy.
4. To upgrade OpenManage Integration plug-in from version 3.0 to the current version, do one of the following:
   - Ensure that **Update Repository Path** is set to http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ path. If the path is different, in the **Appliance Management** window, in the **APPLIANCE UPDATE** section, click **Edit** to update the path to **http://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/** in the **Update Repository Path** text box. Click **Apply** to save the updates.
   - 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, update the path to the offline HTTP share, and click **Apply**.
5. 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.
6. To apply the update to the virtual appliance, under **Appliance Settings**, click **Update Virtual Appliance**.
7. In the **UPDATE APPLIANCE** dialog box, click **Update**. After you click **Update**, you are logged off the **ADMINISTRATION CONSOLE** window.

NOTE: While upgrading OMIVV from 3.0 to the current version, the custom certificate is not migrated and you must reapply the settings that you had applied for the certificate.

Migration Path to migrate from 2.x to 3.1

You can migrate from older version (2.x) to the version 3.1 release using the Backup and Restore path or start with a fresh deployment of the v3.1 OVF after uninstalling the old version.

Do the following to migrate from older version to the OMIVV 3.1 version:

1. Take a backup of the database for the older (v2.x) release.

   For more information, see *OpenManage Integration for VMware vCenter version 3.1 User's Guide* available at **dell.com/support/manuals**.
2. Power off the older appliance from vCenter.

   NOTE: Do not unregister the plug-in from vCenter. Unregistering the plug-in from vCenter removes all the Alarms registered on vCenter by the plug-in and removes all the customization performed on the alarms like actions and so on. For more information, see Recover OpenManage Integration for VMware vCenter if the older plug-in is unregistered if you have already unregistered the plug-in after the backup.
3. Deploy the new OpenManage Integration version 3.1 OVF.

   For more information on deploying the OVF, see Deploying the OMIVV OVF Using the vSphere Web Client.
4. Power on the OpenManage Integration version 3.1 appliance.
5. Set up the network and time zone on the appliance.

   It is mandatory that the new OpenManage Integration version 3.1 appliance has the same IP address as the old appliance. To set up the network details, see Registering OpenManage Integration for VMware vCenter and Importing The License File.

   NOTE: The plug-in might not work properly if the IP address for the OMIVV 3.1 appliance is different from the IP address of the older appliance. In such a scenario, you need to un-register and re-register all the vCenter instances.
6. Restore the database to the new appliance.

   For more information, see **Restoring The Database From A Backup** in the *OpenManage Integration for VMware vCenter Version 3.1 User Guide* available at **dell.com/support/manuals**.
7. Upload the new license file.

   For more information, see Registering OpenManage Integration for VMware vCenter and Importing The License File.
8. Verify the appliance.

   For more information, see the **Installation Verification** section in this guide to ensure that the database migration is successful.
9. Run the **Inventory** on all the hosts.

NOTE:

It is recommended that you run the inventory on all the hosts managed by the plug-in again after the upgrade. For more information, see the section **Running Inventory Jobs** for steps to run the inventory on demand.

If the IP address of the new OMIVV version 3.1 appliance has changed from that of the old appliance, the trap destination for the SNMP traps must be configured to point to the new appliance. For 12G and 13G servers, this is fixed by running the Inventory on these hosts. For all 11G or earlier generation hosts that were complaint with earlier versions, this IP change shows up as non-complaint and requires you to configure OMSA. For more information on fixing the host compliance, see **Running the Fix Non-Compliant VSphere hosts Wizard** in the *OpenManage Integration for VMware vCenter Version 3.1 User Guide* available at **dell.com/support/manuals**.

Recover OpenManage Integration for VMware vCenter if the older plug-in is unregistered

If you have unregistered the plug-in after taking backup of the database of the older 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 Migration Path to migrate from 2.x to 3.1.
2. Register the plug-in to the same vCenter that you had registered in the older plug-in.
3. Complete step 6 through step 8 in Migration Path to migrate from 2.x to 3.1 to complete the migration.

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.

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**.

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

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, 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 the **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 the Plus Icon displayed on the top left corner of the **Associated Chassis** page.

3

Additional Configuration Settings

The following configuration settings are optional. However, it can be used for monitoring the hosts in your VMware vCenter using the plug-in.

- Warranty Expiration Notification
- Firmware Update Repository
- OMSA Web Server URL

Warranty Expiration Notification

Viewing Warranty Expiration Notification Settings

1. In the OMIVV, click **Manage** → **Settings** tab.
2. Under **Appliance Settings**, click **Warranty Expiration Notification**.
   The **Warranty Expiration Notification** page displays the following:
   - Indicates whether the setting is enabled or disabled
   - The number of days set for the first warning setting.
   - The number of days set for the critical warning setting
3. To configure the Warranty Expiration Notification, see Configuring Warranty Expiration Notifications.

Configuring Warranty Expiration Notification

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

1. In the OMIVV, click **Manage** → **Settings**.
2. Under **Appliance Settings**, to the right side of **Warranty Expiration Notification**, click the **Edit** icon.
3. In the **Warranty Expiration Notification** dialog box, to enable warranty expiration notification, select **Enable warranty expiration notification for hosts**.
4. In **Minimum Days Threshold Alert**, from the **Warning** list, select the number of days before warranty expiration, that you want to be notified.
5. From the **Critical** list, select the number of days before warranty expiration, that you want to be notified.
6. Click **Apply**.

Firmware Update Repository

In OMIVV, in the **Settings** tab, you can set the location from which the servers can receive firmware updates. This is a global setting.

Firmware repository settings contain the firmware catalog location used to update deployed servers. Following are the locations:

- **Dell (ftp.dell.com)** — Uses the firmware update repository of Dell (ftp.dell.com). The OMIVV downloads selected firmware updates from Dell repository.

  NOTE: OMIVV connects to the Internet to get the catalog and firmware packages applicable for your hosts. Depending on your network settings, configure proxy for the firmware update task to run successfully from Dell online.
- **Shared Network Folder** — Created with Dell Repository Manager. These local repositories should be located on CIFS or NFS file share.

Setting Up the Firmware Update Repository

You can configure the firmware update repository on the OMIVV in the **Settings** tab.

1. In OMIVV, click **Manage** → **Settings**.
2. Under **Appliance Settings**, to the right side of **Firmware Update Repository**, click the **Edit** icon.
3. In the **Firmware Update Repository** dialog box, 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 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 or Linux based file shares. Use the live link to go to Dell Repository Manager.
4. If you selected the **Shared Network Folder** option, 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

   NOTE: You can view the progress of the download in the **Select Update Source** page.
5. When the download is complete, click **Apply**.

OMSA Web Server URL

OMSA link is the URL to launch the OMSA GUI for host servers that have OMSA installed.

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

1. In OMIVV, click **Manage** → **Settings**.
2. Under **vCenter Settings** , to the right side of the OMSA Web Server URL, click **Edit**.
3. In the **OMSA Web Server URL** dialog box, type the URL.
   You must include the full URL including HTTPS and the port number. For example,
   https://10.0.0.1:1311 or https://omsaurl:1311
4. Select **Apply these settings to all vCenters** to apply the OMSA URL to all vCenters.
   If you do not select this check box, the OMSA URL is applied only to one vCenter.

5. From the corresponding host **Summary** tab, check if the link works.
6. Check if the OMSA Console link is functional within the Dell Host Information.

4

Licensing in OpenManage Integration for VMware vCenter

This chapter provides details about licensing in OMIVV. There are no new licensing changes for 3.1.

NOTE: The Licensing for OMIVV does not alter the number of vCenter connection licenses. The maximum number of vCenter licenses is 10. If you want to register multiple vCenters, all vCenters should be part of same SSO. Separate instances of vCenters are not supported in this OMIVV release.

License Types

With version 3.1, there are two types of licenses. An evaluation license and a standard license. These licenses restrict functionality based on time and the number of Dell 11th Generation or newer hosts.

Evaluation License

When the OMIVV version 3.x appliance is powered on for the first time, an evaluation license is automatically installed. This evaluation license allows the OMIVV to operate and manage five Dell hosts (11th Generation and later) and newer hosts without blocking any functionality for the 90 day evaluation period from the first power on. Once a standard license is uploaded, the evaluation license is no longer used.

Standard License

A standard license is purchased from Dell. Different purchase SKU's are used when ordering the license based on the number of Dell 11th Generation or newer servers running VMware ESXi to be managed, and the duration of product support. The license includes product support and appliance updates for a periods of either 3 or 5 years.

Uploading License

When a license is purchased, an email is sent to you containing the license file. The license must be uploaded from the web administration console, accessible by using the ip address of the appliance.

1. Licenses are uploaded using the Upload License link in the vCenter Registration page.
2. After clicking the Upload License link, the Upload License dialog box appears.
3. Browse to the license XML file and click Upload.

   NOTE: The license file might be packaged inside a zip file. Be sure to 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.

4. The Upload License file displays a success message if the license upload is successful.

Options After Uploading Licenses

License file for new purchases

When purchasing a new license, an email is sent from Dell containing the new license file. The license should arrive in a .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 OMIVV version 2.1, OMIVV has the ability to 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 vCenters cannot be increased by stacking, and would require 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 will 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 will continue; 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 uploading a replacement license, if a license was already uploaded with the same entitlement ID it will be replaced.

Enforcement

Appliance Updates

The appliance will not allow updates to newer versions when all licenses are expired. Please obtain and upload a new license prior to attempting to upgrade the appliance.

Evaluation Licenses

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

Adding Hosts to Connection Profiles

When attempting to add a host to a connection profile, if the number of licensed 11th Generation or newer hosts is exceeded and beyond the license number, adding additional hosts is prevented.

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 **Browse for a product** category. In the **Select a product** section, click **Software and Security → Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter 3.1** to access the following documents:

- *OpenManage Integration for VMware vCenter Quick Install Guide for vSphere Client Version 3.1*
- *OpenManage Integration for VMware vCenter for Desktop Client User's Guide Version 3.1*
- *OpenManage Integration for VMware vCenter for Web Client User's Guide Version 3.1*
- *OpenManage Integration for VMware vCenter Release Notes Version 3.1*
- *OpenManage Integration for VMware vCenter Compatibility Matrix Version 3.1*

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.