OpenManage Integration for VMware vCenter version 5.3

Security Configuration Guide

DELLEMC

Notes, cautions, and warnings

(i) **NOTE:** A NOTE indicates important information that helps you make better use of your product.

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

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

Contents

Figures

Tables

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to **https://www.dell.com/support**.

Purpose

This document includes information about security features and capabilities of OpenManage Integration for VMware vCenter (OMIVV).

Audience

This document is intended for individuals who are responsible for managing security for OMIVV.

Revision History

The following table presents the revision history of this document.

Table 1. Revision History

Revision	Date	Description
A00_5.2.0	October 2020	Initial release of the OpenManage Integration for VMware vCenter 5.2 Security Configuration Guide.
A00_5.3.0	March 2021	Added RESTful API related information in the authentication and data security topics.

Related documentation

The complete documentation set for OMIVV is available at **https://www.dell.com/support**. Click **Browse all products**, then click **Software** > **Virtualization Solutions**. Click **OpenManage Integration for VMware vCenter** to access the following documents:

- *OpenManage Integration for VMware vCenter Version 5.3 User's Guide*
- *OpenManage Integration for VMware vCenter Version 5.3 Release Notes*
- *OpenManage Integration for VMware vCenter Version 5.3 Compatibility Matrix*
- *OpenManage Integration for VMware vCenter Version 5.3 API Guide*
- *OpenManage Integration for VMware vCenter Version 5.3 Installation Guide*

You can find the technical artifacts including white papers at https://www.dell.com/support.

Terms used in this document

Table 2. Terms used in this document

Terminology	Description
OMIVV	OpenManage Integration for VMware vCenter
OVF	Open Virtualization Format
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
NFS	Network File System
CIFS	Common Internet File System
OM MP	OpenManage Management pack for vRealize Operations
CMC	Chassis Management Controller (M1000e, FX, VRTX)
OME-M	OpenManage Modular Edition (MX7000)
iDRAC	Integrated Dell Remote Access Controller
SNMP	Simple Network Management Protocol
VM	Virtual Machine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PEM	Privacy-Enhanced Mail
RPM	Red Hat Package Manager
OS	Operating System

Deployment models

You can deploy OpenManage Integration for VMware vCenter (OMIVV) as an OVF in VMware vCenter environment.

Topics:

Open Virtualization Format (OVF) deployment

If you have VMware vSphere virtual machine environment, it is recommended that you deploy OMIVV as an Open Virtualization Format (OVF).

The OVF deployment model includes a pre-configured bundle with the OMIVV software and the Linux operating system that the OMIVV software runs on.

The OVF environment also includes a pre-configured firewall that is tuned to the OMIVV communication requirement with the monitored systems.

The OVF is deployed with an OVF template file. For more information about deploying OMIVV as an OVF, see the *OpenManage Integration for VMware vCenter 5.3 Installation Guide* available at **https://www.dell.com/support**.

Security profiles

OMIVV has a default security profile for secure HTTP access. It is highly recommended to replace the Certificate Authority (CA) signed certificates for the stronger security environments.

Product and Subsystem Security

Topics:

Security controls map

OMIVV performs deployment, inventory, and update of PowerEdge servers using iDRAC and receives SNMP traps from iDRAC.

The User Interface of OMIVV is the appliance administration web page. The OMIVV plugin UI operates from VMware vCenter Client and provides host hardware monitoring and management capabilities.

All system credentials are stored within the OMIVV secure storage.

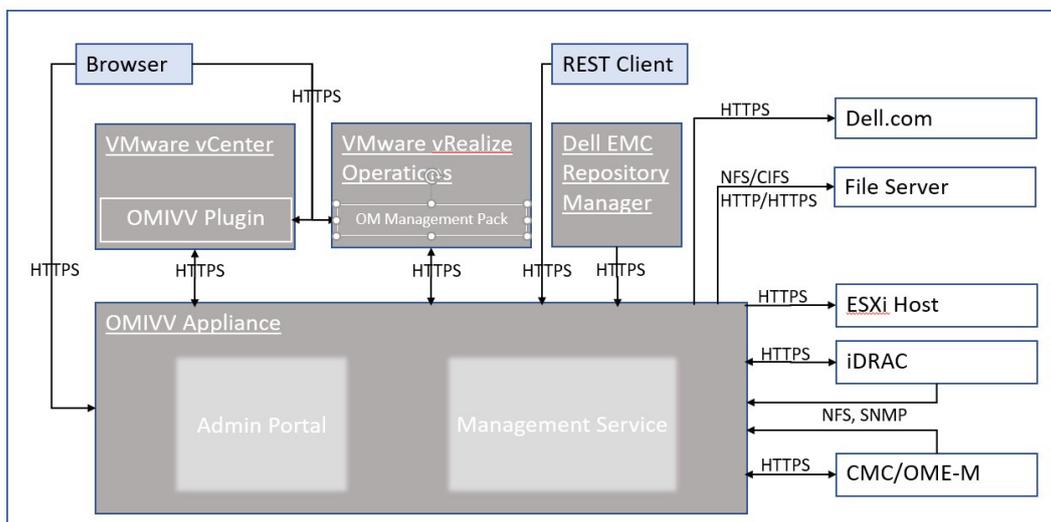The following figure displays the OMIVV security controls map:

Figure 1. Security Controls Map

Authentication

Access control

Access control settings provide protection of resources against unauthorized access. OMIVV plug-in pages can be accessed by VMware vCenter users with appropriate roles and privileges configured in VMware vCenter. OMIVV administration console and RESTFul APIs access is given to OMIVV appliance admin account.

Default user accounts

OMIVV includes the following default user accounts:

● Local user account
● Read only user account
● Root account

Local user account

OMIVV provides a single default local administrative user account. The username of this internal account is admin.

The local administrator has access to all operations in the Dell EMC OMIVV Administration Console only.

The first time that you deploy OMIVV, you are prompted to set the password. Follow the on-screen instruction to set the password.

Read only user account

The OMIVV provides a single default local read only user account. The username of the read only account is readonly.

The administrator can log in to OMIVV using the VM remote console only.

This account can be used during troubleshooting to view critical appliance status and logs.

The first time that you deploy OMIVV, you are prompted to set the password. Follow the on-screen instruction to set the password.

root account

OMIVV appliance has a Operating System root account.

This default account is not accessible. Technical support team uses root account to debug the field issues.

External user accounts

VMware vCenter users can access the OMIVV plugin User Interface elements from vCenter HTML5 Client when the users have appropriate roles and privileges on the vCenter. For more information about roles and privileges, see Required privileges for non-administrator users on page 14.

Login security settings

Failed login behavior

OMIVV includes security settings for when there are multiple unsuccessful authentication occurrences.

Local user account lockout

After 6 consecutive failed attempts to login to the local user account, OMIVV temporarily locks out the user for a period of one minute.

Automatic session timeout

Idle browser session timeout

By default, after 15 minutes of inactivity, the OMIVV session times out and you are automatically logged out.

Authentication types and setup considerations

vCenter user authentication

OMIVV depends on vCenter authentication for access for plug-in pages and RESTful APIs dealing with vCenter operations. The plug-in pages and RESTful APIs dealing with vCenter operations require the privileges that are created by Dell EMC on vCenter during registration.

Register new vCenter server

Prerequisites

Your vCenter account should have the necessary privileges to create a user. For more information about the required privileges, see Required privileges for non-administrator users on page 14.

About this task

You can register the OMIVV appliance after the OMIVV is installed. The OMIVV uses the administrator user account or a non-administrator user account with necessary privileges for vCenter operations. A single OMIVV appliance instance can support 15 vCenter servers (with or without linked mode) and up to 2,000 ESXi hosts.

If you try to register more than 15 vCenters, the following error message is displayed:

Your license allows only <x> vCenters and all are already registered.

To register a new vCenter server, do the following:

Steps

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

      Dell EMC recommends you to register OMIVV with the VMware vCenter using a Fully Qualified Domain Name (FQDN). For all registrations, the hostname of vCenter must be properly resolvable by the DNS server. The following are the recommended practices for using the DNS server:
      - Assign a static IP address and hostname when you deploy an OMIVV appliance with a valid DNS registration. A static IP address ensures that during the system restart, the IP address of the OMIVV appliance remains same.
      - Ensure that OMIVV hostname information is present in both forward and reverse lookup zones in your DNS server.
   b. In the **Description** box, enter a description—optional.
4. Under **vCenter User Account**, perform the following steps:
   a. In the **vCenter User Name** box, enter the username of administrator or a non-administrator username with the required privileges.

b. In the **Password** box, enter the password.

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

d. Select the **Register vSphere Lifecycle Manager** check box.

   Selecting the **Register vSphere Lifecycle Manager** check box allows you to use vSphere Lifecycle Manager feature from vCenter 7.0 and later.

5. Click **Register**.

   The following error message is displayed if vCenter registration fails:

   Could not contact the given vCenter server <x> due to wrong credentials. Check the username and password.

Results

After registering the vCenter server, OMIVV is registered as a vCenter plug-in, and "Dell EMC OpenManage Integration" icon is visible in the vSphere Client from which you can access the OMIVV features.

(i) **NOTE:** For all vCenter operations from OMIVV appliance, OMIVV uses the privileges of the registered user and not the privileges of the user logged-in to VMware vCenter or the OMIVV appliance local accounts. For example, user X with the necessary privileges registers OMIVV with vCenter, and user Y has only the Dell privileges. User Y can now log in to the vCenter and can trigger a firmware update task from OMIVV. While performing the firmware update task, OMIVV uses the privileges of user X to put the host into maintenance mode or reboot the host.

(i) **NOTE:** If you want to upload a customized Certificate Authority (CA)-signed certificate to OMIVV, ensure that you upload the new certificate before vCenter registration. If you upload the new custom certificate after vCenter registration, communication errors are displayed on the vSphere Client. To fix this issue, log out and log in to vCenter. If issue persists, restart the vSphere Client service on the vCenter server.

Register vCenter server using a non-administrative account

Prerequisites

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

About this task

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

Steps

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

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

   For the steps required to create or modify a role and select privileges in the vSphere Client (HTML-5), see the VMware vSphere documentation

2. Assign a user to the newly created role after you define a role and select privileges for the role.

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

   A vCenter Server non-administrator user with the required privileges can now register and/or unregister vCenter, modify credentials, or update the certificate.

3. Register a vCenter server using a non-administrator user with the required privileges.

4. After registration is complete, assign the Dell privileges to the role created or modified in step 1. See Assign Dell privileges to existing role on page 15.

Results

A non-administrator user with the required privileges can now use the OMIVV features with the Dell EMC hosts.

Required privileges for non-administrator users

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

While registering a vCenter server with OMIVV by a non-administrator user, a message is displayed if the following privileges are not assigned:

- Alarms
  - Create alarm
  - Modify alarm
  - Remove alarm
- Extension
  - Register extension
  - Unregister extension
  - Update extension
- Global
  - Cancel task
  - Log event
  - Settings
- Health Update Provider
  - Register
  - Unregister
  - Update
- Host
  - CIM
    - CIM Interaction
- Host.Config
  - Advanced settings
  - Change Settings
  - Connection
  - Maintenance
  - Network configuration
  - Query patch
  - Security profile and firewall
- Inventory
  - Add host to cluster
  - Add standalone host
  - Modify cluster
- Lifecycle Manager: General Privileges
  - Read

  (i) **NOTE:** The vSphere Lifecycle Manager General Privileges are applicable only for vCenter 7.0 and later.

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

(i) **NOTE:** If a vCenter server is registered using non-administrator user to access any OMIVV features, non-administrator user must have Dell privileges. For more information about assigning Dell privileges, see Assign Dell privileges to existing role on page 15.

Assign Dell privileges to existing role

About this task

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

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

Steps

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

   For more information about the available OMIVV roles within vCenter, see Dell Operational role on page 16.

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

vCenter user security

Security roles and permissions

The OpenManage Integration for VMware vCenter stores user credentials in an encrypted format. It does not provide any passwords to client applications to avoid any improper requests. The backup database is fully encrypted by using custom security phrases, and hence data cannot be misused.

By default, users in the Administrators group have all the privileges. The Administrators can use all the functions of the OpenManage Integration for VMware vCenter within VMware vSphere web client. If you want a user with necessary privileges to manage the product, do the following:

1. Create a role with necessary privileges.
2. Register a vCenter server by using the user.
3. Include both the Dell operational role and Dell infrastructure deployment role.

Data integrity

The communication between the OpenManage Integration for VMware vCenter, Administration Console, and vCenter is accomplished by using HTTPS. The OpenManage Integration for VMware vCenter generates a certificate that is used for trusted communication between vCenter and the appliance. It also verifies and trusts the certificate of the vCenter server before communication and the OpenManage Integration for VMware vCenter registration.

A secure Administration Console session has a 15 minutes idle time-out, and the session is only valid in the current browser window and/or tab. If you try to open the session in a new window or tab, a security error is prompted that asks for a valid session. This action also prevents the user from clicking any malicious URL that can attack the Administration Console session.
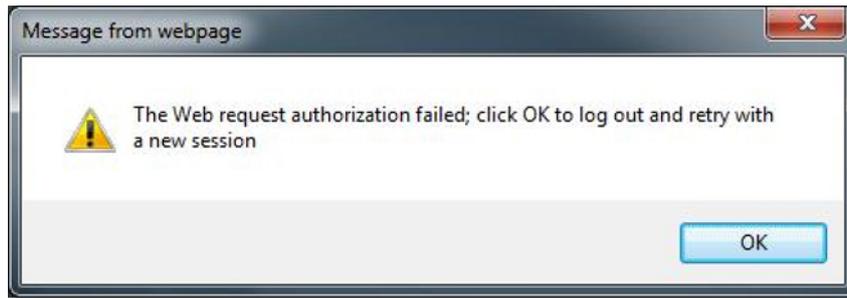
Figure 2. Security error message

Access control authentication, authorization, and roles

To perform vCenter operations, OpenManage Integration for VMware vCenter uses the current user session of vSphere client and the stored administration credentials for the OpenManage Integration. The OpenManage Integration for VMware vCenter uses the vCenter server's built-in roles and privileges model to authorize user actions with the OpenManage Integration and the vCenter managed objects (hosts and clusters).

Dell Operational role

The role contains the privileges/groups to accomplish appliance and vCenter server tasks including firmware updates, hardware inventory, restarting a host, placing a host in maintenance mode, or creating a vCenter server task.

This role contains the following privilege groups:

Table 3. Privilege groups

Group name	Description
Privilege group—Dell.Configuration	Perform Host-related tasks, Perform vCenter-related tasks, Configure SelLog, Configure ConnectionProfile, Configure ClearLed, Firmware Update
Privilege group—Dell.Inventory	Configure inventory, Configure warranty retrieval, Configure readonly
Privilege group—Dell.Monitoring	Configure monitoring, monitor
Privilege group—Dell. Reporting (Not used)	Create a report, Run a report

Dell Infrastructure Deployment role

The role contains the privileges that are related to the hypervisor deployment features.

The privileges this role provides are Configure Host Credential Profile, Assign Identity, and Deploy.

Privilege Group — Dell.Deploy-Provisioning

Configure Host Credential Profile, Assign Identity, Deploy.

About privileges

Every action that is performed by the OpenManage Integration for VMware vCenter is associated with a privilege. The following sections list the available actions and the associated privileges:

- Dell.Configuration.Perform vCenter-related tasks
  - Exit and enter maintenance mode
  - Get the vCenter user group to query the permissions
  - Register and configure alarms, for example enable/disable alarms on the event settings page
  - Post events/alerts to vCenter
  - Configure event settings on the event settings page

- Restore default alerts on the event settings page
- Check DRS status on clusters while configuring alerts/events settings
- Reboot host after performing update or any other configuration action
- Monitor vCenter tasks status/progress
- Create vCenter tasks, for example firmware update task, host configuration task, and inventory task
- Update vCenter task status/progress
- Get host profiles
- Add host to data center
- Add host to cluster
- Apply profile to host
- Get CIM credentials
- Configure hosts for compliance
- Get the compliance tasks status
- Dell.Inventory.Configure ReadOnly
  - Get all vCenter hosts to construct the vCenter tree while configuring connection profiles
  - Check if the host is a Dell server when the tab is selected
  - Get the vCenter's Address/IP
  - Get host IP/Address
  - Get the current vCenter session user based on the vSphere client session ID
  - Get the vCenter inventory tree to display the vCenter inventory in a tree structure.
- Dell.Monitoring.Monitor
  - Get host name for posting the event
  - Perform the event log operations, for example get the event count, or change the event log settings
  - Register, unregister, and configure events/alerts — Receive SNMP traps and post events
- Dell.Configuration.Firmware Update
  - Perform firmware update
  - Load firmware repository and DUP file information on the firmware update wizard page
  - Query firmware inventory
  - Configure firmware repository settings
  - Configure staging folder and perform update by using the staging feature
  - Test the network and repository connections
- Dell.Deploy-Provisioning.Create Template
  - Configure HW Configuration Profile
  - Configure Hypervisor Deployment Profile
  - Configure Connection Profile
  - Assign identity
  - Deploy
- Dell.Configuration.Perform host-related tasks
  - Blink LED, Clear LED
  - Launch iDRAC Console
  - Display and clear SEL log
- Dell.Inventory.Configure Inventory
  - Display system inventory in the Dell Server Management tab
  - Get storage details
  - Get power monitoring details
  - Create, display, edit, delete, and test connection profiles on the connection profiles page
  - Schedule, update, and delete inventory schedule
  - Run inventory on hosts

User and credential management

Preloaded accounts

The following table describes the preloaded OMIVV accounts:

Table 4. Preloaded accounts

User account	Description
OpenManage Integration for VMware vCenter administrator	The default user for OMIVV web application administration.
Read only user.	OMIVV provides a single default local read only user account.
	The administrator can log into OMIVV using the VM remote console only.
	This account can be used during troubleshooting to view critical appliance status and logs.
Linux operating system root	The root operation system account is not accessible. Technical support team uses root account to debug the field issues.

Default credentials

The following table describes the default credentials for the pre-loaded OMIVV accounts.

Table 5. Default credentials

Account	User	Password
OpenManage Integration for VMware vCenter administrator	Admin	Set on first boot after deployment. For more information about changing admin password, see Change OMIVV appliance password on page 18.
Read only user	Read only	Set on first boot after deployment. The readonly user password can be reconfigured after logging in as readonly user using standard Linux password change commands.
Linux operating system root	Root	The OS root password is set when OMIVV is deployed.

Managing credentials

If you are logging in for the first time to Dell EMC administration console, log in as an administrator (the default user name is admin).

(i) **NOTE:** If you forget the administrator password, it cannot be recovered from the OMIVV appliance.

Change OMIVV appliance password

About this task

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

Steps

1. Open the OMIVV web console.
2. In the **OpenManage Integration for VMware vCenter Virtual Appliance Setup** utility, click **Change Admin Password**.
   Complete the instructions on the screen to set the password.

3. In the **Current Password** text box, enter the current admin password.
4. Enter a new password in the **New Password** text box.
5. Retype the new password in the **Confirm New Password** text box.
6. Click **Change Admin Password**.

Authorization

OMIVV appliance supports a single administrative user.

After logging in to OMIVV, administrator can access only the OMIVV appliance configuration features such as:

- Register new vCenter server
- Configure appliance
- Upgrade OMIVV appliance using RPM and backup and restore
- Set up Network Time Protocol servers
- Configure deployment mode
- Generate a Certificate Signing Request (CSR)
- Upload HTTPS certificate
- Set up global alerts
- Generate and download the troubleshooting bundle

Network security

OMIVV appliance uses a preconfigured firewall to enhance security by restricting inbound and outbound network traffic to the TCP and UDP ports. The tables in this section lists the inbound and outbound ports that OMIVV uses.

Network exposure

OpenManage Integration for VMware vCenter uses inbound and outbound ports when communicating with remote systems.

Outbound ports

Outbound ports can be used by OMIVV when connecting to a remote system.

The ports that are listed in the following table are the OMIVV outbound ports.

Table 6. Outbound ports

Port number	Layer 4 Protocol	Service
7	TCP, UDP	ECHO
22	TCP	SSH
25	TCP	SMTP
53	UDP, TCP	DNS
67,68	TCP	DHCP
80	TCP	HTTP
88	TCP, UDP	Kerberos
111	TCP, UDP	ONC RPC
123	TCP, UDP	NTP
161-163	TCP, UDP	SNMP
389	TCP, UDP	LDAP

Table 6. Outbound ports

Port number	Layer 4 Protocol	Service
443	TCP	HTTPS
448	TCP	Data Protection Search Admin REST API
464	TCP, UDP	Kerberos
514	TCP, UDP	rsh
587	TCP	SMTP
636	TCP, UDP	LDAPS
902	TCP	VMware ESXi
2049	TCP, UDP	NFS
2052	TCP, UDP	mountd, clearvisn
3009	TCP	Data Domain REST API
5672	TCP	RabbitMQ over amqp
8443	TCP	MCSDK 8443 is an alternative for 443
9002	TCP	Data Protection Advisor REST API
9443	TCP	Avamar Management Console web service

Inbound ports

The inbound ports that are available to be used by a remote system when connecting to OMIVV.

The ports that are listed in the following table are the OMIVV inbound ports.

Table 7. Inbound ports

Port number	Layer 4 Protocol	Service
22	TCP	SSH
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	RabbitMQ over amqp

Data security

The data that is maintained by OMIVV is stored and secured in internal databases within the appliance and it cannot be accessed from outside.

The data that is in transit through OMIVV is secured by secure communication channel.

(i) **NOTE:** It is recommended that RESTful API users store credentials and data retrieved securely as per your environment restrictions.

Cryptography

OMIVV uses cryptography for the following components:

● Access control
● Authentication

- Digital signatures

Manage certificate

OMIVV uses certificates for secure HTTP access (HTTPS).

By default, OMIVV installs and uses the self-signed certificate for the HTTPS secure transactions.

For stronger security, it is recommended to use the Certificate Authority (CA) signed or custom certificates.

The self-signed certificate is sufficient to establish an encrypted channel between web browsers and the server. The self-signed certificate cannot be used for authentication.

You can use the following types of certificates for OMIVV authentication:

- A self-signed certificate

  OMIVV generates self-signed certificates when the hostname of the appliance changes.

- A certificate that is signed by a trusted certificate authority (CA) vendor.
  (i) **NOTE:** Consider company policies when creating certificates.

Update certificates for registered vCenter servers

About this task

The OpenManage Integration for VMware vCenter uses the OpenSSL API to create the Certificate Signing Request (CSR) by using the RSA encryption standard with a 2048−bit key length.

If the certificate is changed on a vCenter server, use the following tasks to import the new certificate for OMIVV:

Steps

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

Generate a Certificate Signing Request (CSR)

Prerequisites

By default, OMIVV has self-signed certificate. If you need customized Certificate Authority (CA)-signed certificate for OMIVV, it is recommended to upload new certificate before vCenter registration.

About this task

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

Steps

1. On the **APPLIANCE MANAGEMENT** page, click **Generate Certificate Signing Request** in the **HTTPS CERTIFICATES** area.
   A message is displayed stating that if a new request is generated, certificates that is created using the previous CSR can no longer be uploaded to the appliance. To continue with the request, click **Continue**.
2. If you continue with the request, in the **GENERATE CERTIFICATE SIGNING REQUEST** dialog box, enter information about the common name, organization name, locality, state, country, email address, and Subject Alternate Name (SAN), and then click **Continue**.
   (i) **NOTE:** OMIVV does not support multiple values for SAN.
3. Click **Download**, and then save the resulting CSR to an accessible location.

Upload HTTPS certificate

Prerequisites

Ensure that the certificate uses the PEM format.

About this task

You can use the HTTPS certificates for secure communication with OMIVV appliance and host systems or vCenter. To set up this type of secure communication, send the CSR certificate to a signing authority, and then upload the resulting CSR using the admin console. There is also a default certificate that is self-signed and can be used for secure communication—this certificate is unique to every installation.

Steps

1. On the **APPLIANCE MANAGEMENT** page, click **Upload Certificate** in the **HTTPS CERTIFICATES** area.
2. Click **OK** in the **UPLOAD CERTIFICATE** dialog box.
3. To upload the certificate, click **Browse**, and then click **Upload**.
   To check the status, go to **Event Console** of vSphere Client of registered vCenters.

Results

While uploading certificate, OMIVV administration console becomes unresponsive for up to 3 minutes. After upload HTTPs certificate task is complete, close the browser session and access admin portal in a new browser session.

Restore default HTTPS certificate

Steps

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

Results

While restoring certificate, OMIVV administration console becomes unresponsive for up to 3 minutes. After restore default HTTPs certificate task is complete, close the browser session and access admin portal in a new browser session.

Auditing and logging

The admin user can use the OMIVV administration console to generate a troubleshooting bundle with all the relevant logs.

For more information, see Create and download troubleshooting bundle on page 22.

The read only account helps troubleshoot the appliance by allowing the user to read various parameters of the appliance at runtime. For advanced troubleshooting Tech support guides to check specific parameters.

ⓘ **NOTE:** Only OMIVV admin user can perform write operations on the appliance. User auditing is not available in the OMIVV logs. For more information about the vCenter operations performed from the vCenter plugin, see the vCenter audit logs. For RESTful APIs, the Client must be able to handle audit logging.

Create and download troubleshooting bundle

About this task

The troubleshooting bundle contains OMIVV appliance logging information that can be used to help in resolving issues or sent to Technical Support. OMIVV does not log any user sensitive data.

Steps

1. On the **Support** page, click **Create and download troubleshooting bundle**.
   The **Troubleshooting Bundle** dialog box is displayed.

2. In the **Troubleshooting Bundle** dialog box, click **CREATE**.

   Depending on the size of the logs, creating the bundle may take some time.

3. To save the file, click **DOWNLOAD**.

   The Dell EMC OMIVV Administration Console log in page is displayed.

4. Log in to Dell EMC OMIVV Administration Console.

5. Download the troubleshooting bundle. For more information, see

Generate and download the troubleshooting bundle

Prerequisites

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

About this task

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

Steps

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

Serviceability

The support website **https://www.dell.com/support** provides access to licensing information, product documentation, advisories, downloads, and troubleshooting information. This information helps you to resolve a product issue before you contact support team.

Special login is not required to OMIVV for service personnel. If the troubleshooting bundle is not sufficient, the personnel can enable the root user to collect more information.

Ensure that you install security patches and other updates when they are available, including the OMIVV vCenter Operating System update.

Security patches

Periodic OMIVV updates that include security updates, and security only updates released as required.

The updates are cumulative and published on the support and OMIVV users get notifications on the vCenter upon the same.

OMIVV OS update

Periodically, security patches and fixes are released for the OMIVV OS.

These fixes must be installed on existing OVF deployments of OMIVV through an RPM update package. When available, it is highly recommended that you install these security patches and fixes on the OMIVV server through RPM update.

Product code integrity

The OMIVV software installer is signed by Dell. It is recommended that you verify the authenticity of the OMIVV installer signature.

Miscellaneous Configuration and Management

Topics:

*   OpenManage Integration for VMware vCenter (OMIVV) licensing
*   Protect authenticity and integrity
*   Manage backup and restore in OMIVV

OpenManage Integration for VMware vCenter (OMIVV) licensing

OMIVV has two types of licenses:

*   Evaluation license—when the OMIVV appliance is powered on for the first time, an evaluation license is automatically installed. The trial version contains an evaluation license for five hosts (servers) managed by OMIVV. This 90-day trial version is the default license that is supplied when shipped.
*   Standard license—you can purchase any number of host licenses that are managed by OMIVV. This license includes product support and OMIVV appliance updates. The standard license is available for periods of three or five years. Any additional licenses bought extend the period of the existing license. The standard license overwrites an evaluation license.

License duration for a single XML key is calculated based on the sales date of the original order. Any uploaded new licenses will be reflected in the count after the 90 day grace period ends for any prior, expiring licensing.

OMIVV supports up to 15 vCenter instances. When you upgrade from an evaluation license to a full standard license, you receive an email about the order confirmation, and you can download the license file from the Dell Digital Locker. Save the license .XML file to your local system and upload the new license file using the **Administration Console**.

When you purchase a license, the .XML file (license key) is available for download through the Dell Digital Locker at https://www.dell.com/support. If you are unable to download your license keys, contact Dell Support by going to **Contact Order Support** at https://www.dell.com/support to locate the regional Dell Support phone number for your product.

Licensing presents the following information in the OMIVV Administration Console:

*   Maximum vCenter Connection Licenses—up to 15 registered and in-use vCenter connections are enabled.
*   Maximum Host Connection Licenses—the number of host connections that were purchased (with a maximum of 2000 hosts supported for a single OMIVV instance).
*   In Use—the number of vCenter connection or host connection licenses in use. For host connection, this number represents the number of hosts (or servers) that have been inventoried.
*   Available—the number of vCenter connections or host connection licenses available for future use.

When you attempt to add a host to a host credential profile, if the number of licensed hosts exceeds beyond the number of licenses, adding extra hosts is prevented. OMIVV does not support managing the number of hosts more than number of host license is available.

Use the OMIVV RESTful API to get more information about license. For more information, see *OpenManage Integration for VMware API Guide* at https://www.dell.com/support.

(i) **NOTE:** Any active license can be used for OMIVV 5.x versions. Licenses backed up from previous instances of OMIVV, or downloaded again from the Digital Locker can be used for current instances of OMIVV.

Protect authenticity and integrity

To ensure product integrity, the OMIVV installation and update components are signed.

To ensure communication integrity, it is recommended to use CA-signed certificate.

Manage backup and restore in OMIVV

To protect OMIVV from a disaster scenario, it is recommended that you perform backups of OMIVV. If required, you can restore OMIVV from these backups. For more information about backup and restore, see the OMIVV User's Guide available at **https://www.dell.com/support**.