OpenManage Integration for VMware vCenter Version 5.4

Sicherheitskonfigurationshandbuch

October 2021
Rev. A00

DELL EMC

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

Abbildungen

Tabellen

1

Einleitung

Um seine Produktlinien zu verbessern, veröffentlicht Dell EMC regelmäßig neue Software- und Hardwareversionen. Einige in diesem Dokument beschriebene Funktionen werden möglicherweise nicht von allen Versionen der Software oder Hardware unterstützt, die derzeit verwendet wird. In den Versionshinweisen zum Produkt finden Sie aktuelle Informationen zu den Produktfunktionen.

Wenden Sie sich an den technischen Support von Dell EMC, wenn ein Produkt nicht ordnungsgemäß oder nicht wie in diesem Dokument beschrieben funktioniert. Dieses Dokument war zum Veröffentlichungszeitpunkt korrekt. Um sicherzustellen, dass Sie die aktuelle Version dieses Dokuments verwenden, gehen Sie auf **https://www.dell.com/support**.

Zweck

Dieses Dokument enthält Informationen über die Sicherheitsfunktionen von OpenManage Integration for VMware vCenter (OMIVV).

Zielgruppe

Dieses Dokument richtet sich an Personen, die für das Sicherheitsmanagement von OMIVV zuständig sind.

Revisionsverlauf

In der folgenden Tabelle ist der Revisionsverlauf für dieses Dokument dargestellt.

Tabelle 1. Revisionsverlauf

Revision	Date	Beschreibung
A00_5.2.0	Oktober 2020	Erstveröffentlichung des OpenManage Integration for VMware vCenter 5.2 Sicherheitskonfigurationshandbuchs
A00_5.3.0	März 2021	Weitere Informationen zur RESTful API in den Themen „Authentifizierung“ und „Datensicherheit“ hinzugefügt.
A00_5.4.0	Oktober 2021	Keine für diese Version

Zugehörige Dokumentation

Die vollständige Dokumentation für OMIVV finden Sie unter **https://www.dell.com/support**. Klicken Sie auf **Alle Produkte durchsuchen** und klicken Sie dann auf **Software** > **Virtualisierungslösungen**. Klicken Sie auf **OpenManage Integration for VMware vCenter**, um auf die folgenden Dokumente zuzugreifen:

- *OpenManage Integration for VMware vCenter Version 5.4 – Benutzerhandbuch*
- *OpenManage Integration for VMware vCenter Version 5.4 – Versionshinweise*
- *OpenManage Integration for VMware vCenter Version 5.4 – Kompatibilitätsmatrix*
- *OpenManage Integration for VMware vCenter Version 5.4 – API-Handbuch*
- *OpenManage Integration for VMware vCenter Version 5.4 – Installationshandbuch*

Sie finden Sie die technischen Artefakte einschließlich Whitepapers unter https://www.dell.com/support.

2

In diesem Dokument verwendete Begriffe

Tabelle 2. In diesem Dokument verwendete Begriffe

Terminologie	Beschreibung
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 für vRealize Operations Manager
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	Virtuelle Maschine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
PEM	Privacy-Enhanced Mail
RPM	Red Hat Package Manager
Betriebssystem	Betriebssystem

3

Bereitstellungsmodelle

Sie können OpenManage Integration for VMware vCenter (OMIVV) als OVF in der VMware vCenter-Umgebung bereitstellen.

Themen:

Bereitstellung von Open Virtualization Format (OVF)

Wenn Sie über eine VMware vSphere-Umgebung für virtuelle Maschinen verfügen, wird empfohlen, OMIVV als Open Virtualization Format (OVF) bereitzustellen.

Das OVF-Bereitstellungsmodell umfasst ein vorkonfiguriertes Bundle mit der OMIVV-Software und dem Linux-Betriebssystem, auf dem die OMIVV-Software ausgeführt wird.

Die OVF-Umgebung enthält zudem eine vorkonfigurierte Firewall, die für die OMIVV-Kommunikation mit den überwachten Systemen eingestellt ist.

Das OVF wird mit einer OVF-Vorlagendatei bereitgestellt. Weitere Informationen zur Bereitstellung von OMIVV als OVF finden Sie im *Installationshandbuch für OpenManage Integration for VMware vCenter 5.4* , verfügbar unter **https://www.dell.com/support**.

Sicherheitsprofile

OMIVV verfügt über ein Standardsicherheitsprofil für sicheren HTTP-Zugriff. Es wird dringend empfohlen, die von der Zertifizierungsstelle signierten Zertifikate für Umgebungen mit höherer Sicherheit zu ersetzen.

4

Produkt- und Untersystemsicherheit

Themen:

Übersicht über Sicherheitssteuerungen

OMIVV führt die Bereitstellung, Bestandsaufnahme und das Update von PowerEdge-Servern mithilfe von iDRAC aus und empfängt SNMP-Traps vom iDRAC.

Die Benutzeroberfläche von OMIVV ist die Webseite für die Appliance-Administration. Die OMIVV-Plug-in-Benutzeroberfläche arbeitet über den VMware vCenter-Client und bietet Funktionen zum Monitoring und Management von Hosthardware.

Alle Systemzugangsdaten werden innerhalb des sicheren OMIVV-Storage gespeichert.

In der folgenden Abbildung ist eine Übersicht über die OMIVV-Sicherheitssteuerungen dargestellt:

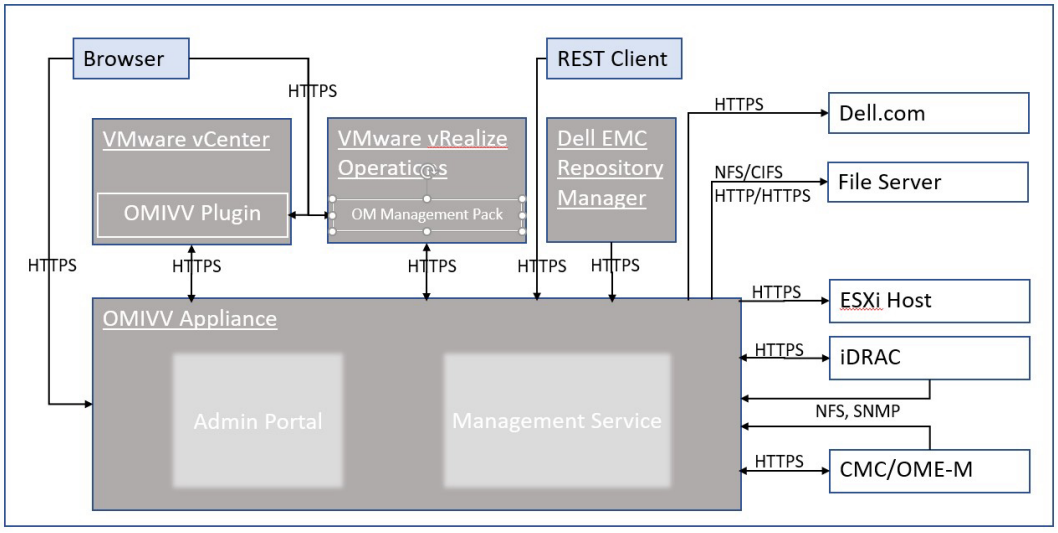

Abbildung 1. Übersicht über Sicherheitssteuerungen

Authentifizierung

Zugriffskontrolle

Zugriffskontrolleinstellungen sorgen für den Schutz von Ressourcen vor unbefugtem Zugriff. VMware vCenter Nutzer mit den entsprechenden Rollen und Berechtigungen, die in VMware vCenter konfiguriert wurden, können auf OMIVV-Plug-in-Seiten zugreifen. Der Zugriff auf die OMIVV-Verwaltungskonsole und RESTful APIs wird nur für Nutzerprofile mit Administratorrechten gewährt.

Standardmäßige Nutzerkonten

OMIVV umfasst die folgenden standardmäßigen Nutzerkonten:

- Lokales Benutzerkonto
- Schreibgeschütztes Nutzerkonto
- Root-Konto

Lokales Benutzerkonto

OMIVV bietet ein einzelnes standardmäßiges, lokales Administratornutzerkonto. Der Nutzername für dieses interne Konto lautet „admin“.

Der lokale Administrator hat nur in der Dell EMC OMIVV-Verwaltungskonsole Zugriff auf alle Vorgänge.

Wenn Sie OMIVV zum ersten Mal bereitstellen, werden Sie aufgefordert, das Kennwort festzulegen. Folgen Sie den Bildschirmanweisungen, um das Kennwort festzulegen.

Schreibgeschütztes Nutzerkonto

OMIVV bietet ein einzelnes standardmäßiges, lokales schreibgeschütztes Nutzerkonto. Der Nutzername des schreibgeschützten Kontos lautet „readonly“.

Der Administrator kann sich nur mit der VM-Remote-Konsole bei OMIVV anmelden.

Dieses Konto kann während des Troubleshootings verwendet werden, um den Status und die Protokolle der kritischen Appliance anzuzeigen.

Wenn Sie OMIVV zum ersten Mal bereitstellen, werden Sie aufgefordert, das Kennwort festzulegen. Folgen Sie den Bildschirmanweisungen, um das Kennwort festzulegen.

Root-Konto

Die OMIVV-Appliance verfügt über ein Betriebssystem-Root-Konto.

Auf dieses Standardkonto kann nicht zugegriffen werden. Das Team für den technischen Support verwendet das Root-Konto zum Debuggen von Problemen.

Externe Nutzerkonten

VMware vCenter-Nutzer können über den vCenter-HTML5-Client auf die OMIVV-Plug-in-Benutzeroberfläche zugreifen, wenn die Nutzer über die entsprechenden Rollen und Berechtigungen in vCenter verfügen. Weitere Informationen über Rollen und Berechtigungen finden Sie unter Erforderliche Berechtigungen für Nicht-Administratornutzer auf Seite 14.

Sicherheitseinstellungen für Anmeldung

Fehlgeschlagene Anmeldung

OMIVV enthält Sicherheitseinstellungen, wenn mehrere Authentifizierungsvorgänge fehlschlagen.

Sperrung des lokalen Nutzerkontos

Nach sechs aufeinanderfolgenden fehlgeschlagenen Anmeldeversuchen für das lokale Nutzerkonto sperrt OMIVV den Nutzer vorübergehend für einen Zeitraum von einer Minute.

Automatisches Sitzungs-Timeout

Timeout bei inaktiver Browsersitzung

Standardmäßig läuft die OMIVV-Sitzung nach 15 Minuten Inaktivität ab und Sie werden automatisch abgemeldet.

Überlegungen zu Authentifizierungsarten und -einrichtung

vCenter-Nutzerauthentifizierung

OMIVV ist für den Zugriff auf Plug-in-Seiten und RESTful APIs von der vCenter-Authentifizierung abhängig. Für die Plug-in-Seiten und RESTful APIs, die die vCenter Operations handhaben, sind die Berechtigungen notwendig, die während der Registrierung von Dell EMC auf vCenter erstellt werden.

Neuen vCenter-Server registrieren

Voraussetzungen

Ihr vCenter-Konto sollte über die erforderlichen Berechtigungen zum Erstellen eines Nutzers verfügen. Weitere Informationen über die erforderlichen Berechtigungen finden Sie unter Erforderliche Berechtigungen für Nicht-Administratornutzer auf Seite 14.

Info über diese Aufgabe

Sie können das OMIVV-Gerät nach der Installation des OMIVV registrieren. Die OMIVV verwendet ein Administrator- oder anderes Nutzerkonto mit den erforderlichen Berechtigungen für vCenter Operations. Eine einzelne OMIVV-Geräteinstanz unterstützt bis zu 15 vCenter Server (mit oder ohne Linked Mode) und bis zu 2.000 ESXi-Hosts.

Wenn Sie versuchen, mehr als 15 vCenter zu registrieren, wird die folgende Fehlermeldung angezeigt:

Ihre Lizenz erlaubt nur <x> vCenter und es sind bereits alle registriert.

Führen Sie folgende Schritte durch, um den neuen vCenter-Server zu registrieren:

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** im rechten Fensterbereich auf **Neuen vCenter-Server registrieren**. Die Seite **NEUES vCENTER REGISTRIEREN** wird angezeigt.
3. Führen Sie im Dialogfeld **NEUES VCENTER REGISTRIEREN** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder den FQDN des Hosts in das Feld **vCenter-Server-IP-Adresse oder Hostname** ein.

      Dell EMC empfiehlt, OMIVV beim VMware vCenter unter Verwendung eines FQDN (Fully Qualified Domain Name) zu registrieren. In allen Registrierungen muss der Hostname von vCenter vom DNS-Server korrekt auflösbar sein. Für DNS-Server werden die folgenden Vorgehensweisen empfohlen:
      - Weisen Sie eine statische IP-Adresse und einen Hostnamen zu, wenn Sie ein OMIVV-Gerät mit einer gültigen DNS-Registrierung bereitstellen. Bei einer statischen IP-Adresse ist sichergestellt, dass die IP-Adresse des OMIVV-Geräts beim Neustart des Systems gleich bleibt.
      - Stellen Sie sicher, dass die OMIVV-Hostnamen-Informationen in der Vorwärts- und Rückwärtssuche Ihres DNS-Servers vorhanden sind.

   b. Geben Sie im Feld **Beschreibung** eine Beschreibung ein – optional.

4. Unter **vCenter Nutzerkonto** führen Sie die folgenden Schritte aus:
   a. Geben Sie im Feld **vCenter Nutzername** den Nutzernamen des Administrators oder eines Nicht-Administrator-Benutzers mit entsprechenden Berechtigungen an.
   b. Geben Sie das Kennwort in das Feld **Kennwort** ein.
   c. Geben Sie das Kennwort zur Bestätigung in das Feld **Kennwort bestätigen** ein.
   d. Aktivieren Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren** .

      Wenn Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren** aktivieren, können Sie die vSphere Lifecycle Manager-Funktion ab vCenter 7.0 aufwärts verwenden.
5. Klicken Sie auf **Registrieren**.

   Die folgende Fehlermeldung wird angezeigt, wenn die vCenter-Registrierung fehlschlägt:

   Es konnte keine Verbindung mit dem angegebenen vCenter-Server <x> aufgrund falscher Zugangsdaten erfolgen. Überprüfen Sie den Nutzernamen und das Kennwort.

Ergebnisse

Nach der Registrierung des vCenter-Servers wird OMIVV als vCenter-Plug-in registriert und das Symbol „Dell EMC OpenManage Integration“ wird im vSphere-Client angezeigt, über den Sie auf die OMIVV-Funktionen zugreifen können.

ANMERKUNG: Für alle vCenter-Vorgänge von der OMIVV-Appliance verwendet OMIVV die Berechtigungen des registrierten Nutzers und nicht die Berechtigungen des bei VMware vCenter angemeldeten Nutzers oder der lokalen Konten der OMIVV-Appliance. Beispiel: Nutzer X mit ausreichender Berechtigung registriert OMIVV mit vCenter und Nutzer Y verfügt nur über Dell Berechtigungen. Nutzer Y kann sich nun bei VCenter anmelden und ein Firmwareupdate von OMIVV auslösen. Während die Firmwareupdateaufgabe durchgeführt wird, nutzt OMIVV die Berechtigungen von Nutzer X, um das Gerät in den Wartungsmodus zu setzten oder den Host neu zu starten.

ANMERKUNG: Wenn Sie ein benutzerdefiniertes, von einer Zertifizierungsstelle signiertes Zertifikat in OMIVV hochladen möchten, stellen Sie sicher, dass Sie das neue Zertifikat vor der vCenter-Registrierung hochladen. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden im vSphere Client Kommunikationsfehler angezeigt. Um dieses Problem zu beheben, melden Sie sich ab und melden Sie sich bei vCenter an. Wenn das Problem bestehen bleibt, starten Sie den vSphere-Client Service auf dem vCenter Server neu.

Registrieren eines vCenter Servers mit einem Konto ohne Administratorrechte

Voraussetzungen

Sie können vCenter Server für die OMIVV Appliance mit vCenter Administrator-Zugangsdaten oder mit einem Nicht-Administrator-Nutzer mit den Dell Berechtigungen registrieren.

Info über diese Aufgabe

Um einen Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen für die Registrierung eines vCenter Servers auszustatten, führen Sie folgende Schritte durch:

Schritte

1. Erstellen Sie eine Rolle oder ändern Sie eine vorhandene Rolle mit den erforderlichen Berechtigungen für die Rolle.

   Weitere Informationen über die Liste der Berechtigungen, die für die Rolle erforderlich sind, erhalten Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Nutzer.

   Die erforderlichen Schritte zum Erstellen oder Ändern einer Rolle und zum Auswählen von Berechtigungen im vSphere Client (HTML5) finden Sie in der Dokumentation zu VMware vSphere.
2. Weisen Sie einen Nutzer zu der neu erstellten Rolle zu, nachdem Sie eine Rolle definiert und Berechtigungen für die Rolle ausgewählt haben.

   Weitere Informationen zum Zuweisen einer Rolle zu Berechtigungen finden Sie in der Dokumentation zu VMware vSphere.

   Ein Nicht-Administrator-Nutzer von vCenter Server mit den erforderlichen Berechtigungen kann jetzt vCenter registrieren und/oder die Registrierung aufheben, Zugangsdaten ändern oder das Zertifikat aktualisieren.
3. Registrieren Sie einen vCenter Server mit einem Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen.

4. Weisen Sie nach Abschluss der Registrierung der in Schritt 1 erstellten oder bearbeiteten Rolle Dell Berechtigungen zu. Informationen dazu finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen auf Seite 15.

Ergebnisse

Jetzt können Nicht-Administrator-Nutzer mit den erforderlichen Berechtigungen die OMIVV-Funktionen mit Dell EMC Hosts nutzen.

Erforderliche Berechtigungen für Nicht-Administratornutzer

Zum Registrieren von OMIVV mit vCenter benötigt ein Nicht-Administratornutzer die folgenden Berechtigungen:

Beim Registrieren eines vCenter Servers mit OMIVV durch einen Nicht-Administrator-Nutzer wird eine Meldung angezeigt, wenn die folgenden Berechtigungen nicht zugewiesen wurden.

- Alarme
  - Erstellen von Alarmen
  - Ändern von Alarmen
  - Entfernen von Alarmen
- Erweiterung
  - Registrieren von Erweiterungen
  - Aufheben der Registrierung von Erweiterungen
  - Aktualisieren von Erweiterungen
- Global
  - Abbrechen von Tasks
  - Protokollereignis
  - Einstellungen
- Funktionszustand-Update-Anbieter
  - Registrieren
  - Registrierung aufheben
  - Aktualisierung
- Host
  - CIM
    - CIM-Interaktion
- Host-Konfig.
  - Erweiterte Einstellungen
  - Einstellungen ändern
  - Verbindung
  - Wartung
  - Netzwerkkonfiguration
  - Abfragen von Patches
  - Sicherheitsprofil und Firewall
- Bestandsaufnahme
  - Hinzufügen von Hosts zu einem Cluster
  - Hinzufügen von eigenständigen Hosts
  - Cluster ändern
- Lifecycle Manager: allgemeine Berechtigungen
  - Lesen

  ANMERKUNG: Die allgemeinen Berechtigungen von vSphere Lifecycle Manager gelten nur für vCenter 7.0 und höher.
- Hostprofil
  - Bearbeiten
  - Ansicht
- Berechtigungen
  - Ändern von Berechtigungen
  - Ändern einer Rolle
- Sitzungen
  - Validieren einer Sitzung
- Task
  - Erstellen

- Aktualisierung

ANMERKUNG: Wenn ein vCenter-Server unter Verwendung eines Nutzers, der kein Administrator ist, registriert wird, um auf OMIVV-Funktionen zuzugreifen, muss der Nutzer, der kein Administrator ist, über Dell Berechtigungen verfügen. Weitere Informationen über das Zuweisen von Dell Berechtigungen finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen auf Seite 15.

Dell Berechtigungen vorhandener Rolle zuweisen

Info über diese Aufgabe

Wenn auf bestimmte Seiten von OMIVV ohne zugewiesene Dell Berechtigungen des angemeldeten Benutzers zugegriffen wird, wird Fehler 2000000 angezeigt.

Sie können zum Zuweisen der Dell Berechtigungen zur Rolle eine vorhandene Rolle bearbeiten.

Schritte

1. Melden Sie sich mit Administratorrechten am vSphere Client (HTML5) an.
2. Erweitern Sie im vSphere Client (HTML5) **Menü** und klicken Sie auf **Administration → Rollen**.
3. Wählen Sie aus der Dropdownliste **Rollenanbieter** einen vCenter Server aus.
4. Wählen Sie in der Liste **Rollen Dell Betrieb** aus und klicken Sie dann auf **BERECHTIGUNGEN**.
5. Um die Dell Berechtigungen zuzuweisen, klicken Sie auf das Bearbeitungssymbol [ ].
   Die Seite **Rolle bearbeiten** wird angezeigt.
6. Klicken Sie im linken Bereich auf **Dell**, wählen Sie dann die folgenden Dell Berechtigungen für die ausgewählte Rolle aus und klicken Sie dann auf **WEITER**:
   - Dell.Configuration
   - Dell.Deploy-Bereitstellung
   - Dell.Inventory
   - Dell.Monitoring
   - Dell.Reporting

   Weitere Informationen zu den verfügbaren OMIVV-Rollen in vCenter finden Sie im Abschnitt Dell Vorgangsrolle auf Seite 16
7. Bearbeiten Sie den Rollennamen und geben Sie falls erforderlich eine Beschreibung für die ausgewählten Rolle ein.
8. Klicken Sie auf **FERTIGSTELLEN**.
   Melden Sie sich ab und dann über das vCenter an. Der Nutzer mit erforderlichen Berechtigungen kann nun die OMIVV-Vorgänge durchführen.

vCenter-Nutzersicherheit

Sicherheitsrollen und Berechtigungen

Das OMIVV speichert Nutzerzugangsdaten in einem verschlüsselten Format. Es stellt keine Kennwörter für Clientanwendungen bereit, um unsachgemäße Anfragen zu vermeiden. Die Datenbanksicherung ist mithilfe benutzerdefinierter Sicherheitsausdrücke vollständig verschlüsselt, deshalb können Daten nicht missbräuchlich verwendet werden.

Als Standardeinstellung besitzen Benutzer in der Administratorgruppe alle Rechte. Die Administratoren können alle Funktionen der OpenManage Integration for VMware vCenter innerhalb des VMware vSphere Webclients benutzen. Wenn ein Benutzer mit erforderlichen Berechtigungen das Produkt verwalten soll, gehen Sie folgendermaßen vor:

1. Erstellen Sie eine Rolle mit erforderlichen Berechtigungen.
2. Registrieren Sie einen vCenter Server mithilfe des Benutzers.
3. Schließen Sie sowohl die operative Dell Rolle als auch die Dell Infrastrukturbereitstellungsrolle ein.

Datenintegrität

Die Kommunikation zwischen OpenManage Integration for VMware vCenter, der Verwaltungskonsole und vCenter erfolgt über HTTPS. OpenManage Integration for VMware vCenter erzeugt ein Zertifikat, das für die vertrauenswürdige Kommunikation zwischen vCenter und

der Appliance verwendet wird. Außerdem überprüft sie das Zertifikat des vCenter-Servers und vertraut ihm vor der Kommunikation und der Registrierung von OpenManage Integration für VMware vCenter.

Bei einer sicheren Verwaltungskonsolen-Sitzung erfolgt nach 15-minütiger Inaktivität ein Timeout und die Sitzung ist nur im aktuellen Browserfenster und/oder in der aktuellen Registerkarte gültig. Wenn Sie versuchen, die Sitzung in einem/einer neuen Fenster oder Registerkarte zu öffnen, wird ein Sicherheitsfehler angezeigt, der nach einer gültigen Sitzung fragt. Diese Aktion verhindert auch, dass der Nutzer auf eine bösartige URL klickt, die die Sitzung der Verwaltungskonsole angreifen kann.

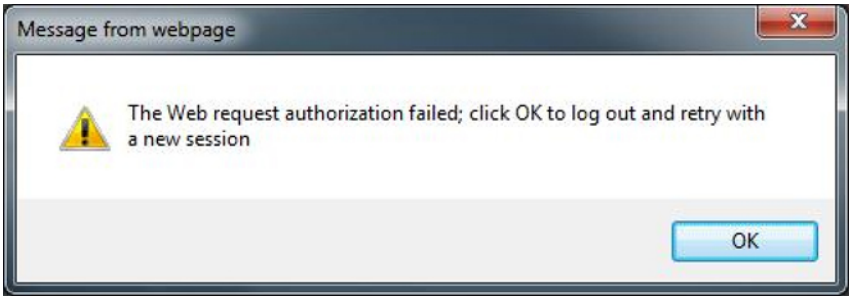

Abbildung 2. Sicherheitsfehlermeldung

Zugriffskontrollauthentifizierung, -autorisierung und -rollen

Um vCenter-Operationen durchzuführen, verwendet OpenManage Integration for VMware vCenter die aktuelle Nutzersitzung des vSphere-Clients und die gespeicherten Administratorzugangsdaten für die OpenManage-Integration. Die OpenManage-Integration für VMware vCenter verwendet das integrierte Rollen- und Berechtigungsmodell des vCenter-Servers, um Benutzeraktionen mit der OpenManage-Integration und den von vCenter verwalteten Objekten (Hosts und Cluster) zu autorisieren.

Dell Vorgangsrolle

Enthält die Berechtigungen/Gruppen zur Ausführung von Geräte- und vCenter Server-Aufgaben einschließlich Firmware-Aktualisierungen, Hardware-Bestandslisten, Neustarten eines Hosts, Versetzen eines Hosts in den Wartungsmodus oder Erstellen einer vCenter Server-Aufgabe.

Diese Rolle umfasst die folgenden Berechtigungsgruppen:

Tabelle 3. Berechtigungsgruppen

Gruppenname	Beschreibung
Berechtigungsgruppe – Dell.Configuration	Ausführen von mit Hosts verknüpften Aufgaben, Ausführen von mit vCenter verknüpften Aufgaben, Konfigurieren von SelLog, Konfigurieren von ConnectionProfile, Konfigurieren von ClearLed, Firmware-Aktualisierung
Berechtigungsgruppe – Dell.Inventory	Konfigurieren der Bestandsaufnahme, Konfigurieren des Serviceabrufs, Konfigurieren von ReadOnly
Berechtigungsgruppe – Dell.Monitoring	Konfigurieren der Überwachung, Überwachung
Berechtigungsgruppe – Dell. Reporting (nicht verwendet)	Erstellen eines Berichts, Ausführen eines Berichts

Dell Infrastrukturbereitstellungsrolle

Diese Rolle umfasst die Berechtigungen, die mit den Hypervisor-Bereitstellungsfunktionen verknüpft sind.

Zu den Berechtigungen dieser Rolle gehören das Konfigurieren des Host-Zugangsdatenprofils, die Identitätszuweisung und die Bereitstellung.

Berechtigungsgruppe – Dell.Deploy- Provisionierung

Konfigurieren des Host-Zugangsdatenprofils, Identitätszuweisung, Bereitstellung.

Informationen zu Berechtigungen

Jede Aktion, die von der OpenManage Integration für VMware vCenter ausgeführt wird, ist einer Berechtigung zugeordnet. In den folgenden Abschnitten sind die verfügbaren Aktionen und die zugehörigen Berechtigungen aufgelistet:

- Dell.Configuration.Perform von mit vCenter verknüpften Aufgaben
  - Beenden und Starten des Wartungsmodus
  - Aufrufen der vCenter-Benutzergruppe zur Abfrage von Berechtigungen
  - Registrieren und Konfigurieren von Alarmen, z. B. Aktivieren/Deaktivieren von Alarmen auf der Seite mit den Ereigniseinstellungen
  - Veröffentlichen von Ereignissen/Warnungen bei vCenter
  - Konfigurieren von Ereigniseinstellungen auf der Seite mit den Ereigniseinstellungen
  - Wiederherstellen von Standardwarnungen auf der Seite mit den Ereigniseinstellungen
  - Überprüfen des DRS-Status auf Clustern während der Konfiguration von Warnungs-/Ereigniseinstellungen
  - Neustarten des Hosts nach Aktualisierungs- oder anderen Konfigurationsmaßnahmen
  - Überwachen des Status/Fortschritts von vCenter-Tasks
  - Erstellen von vCenter-Tasks, z. B. Firmware-Aktualisierungstask, Hostkonfigurationstask und Bestandsaufnahmetask
  - Aktualisieren des Status/Fortschritts von vCenter-Tasks
  - Abrufen von Hostprofilen
  - Hinzufügen von Hosts zu einem Datencenter
  - Hinzufügen von Hosts zu einem Cluster
  - Übernehmen des Profils für einen Host
  - Abrufen von CIM-Anmeldeinformationen
  - Konfigurieren von Hosts für Konformität
  - Abrufen des Status des Konformitätstasks
- Dell.Inventory.Configure ReadOnly
  - Abrufen aller vCenter-Hosts zum Aufbau der vCenter-Struktur während der Konfiguration von Verbindungsprofilen
  - Bei Auswahl der Registerkarte überprüfen, ob der Host ein Dell Server ist
  - Abrufen der Adresse/IP von vCenter
  - Abrufen der Host-IP/Adresse
  - Abrufen des Benutzers der aktuellen vCenter-Sitzung basierend auf der vSphere-Clientsitzungs-ID
  - Abrufen der vCenter-Bestandsaufnahmestruktur, um die vCenter-Bestandsliste in einer Baumstruktur anzuzeigen.
- Dell.Monitoring.Monitor
  - Abrufen des Hostnamens für die Veröffentlichung des Ereignisses
  - Ausführen von Ereignisprotokollierungsvorgängen, z. B. Aufrufen der Ereignisanzahl oder Ändern der Ereignisprotokolleinstellungen
  - Registrieren, Aufheben der Registrierung und Konfigurieren von Ereignissen/Warnungen – Empfangen von SNMP-Traps und Veröffentlichen von Ereignissen
- Dell.Configuration.Firmware Update
  - Ausführen einer Firmware-Aktualisierung
  - Laden von Firmware-Repository- und DUP-Dateninformationen auf der Seite des Assistenten zur Firmware-Aktualisierung
  - Abfragen der Firmware-Bestandsliste
  - Konfigurieren der Firmware-Repository-Einstellungen
  - Konfigurieren des Stagingordners und Ausführen der Aktualisierung unter Verwendung der Stagingfunktion
  - Testen der Netzwerk- und Repository-Verbindungen
- Dell.Deploy-Provisioning Erstellen von Vorlagen
  - HW-Konfigurationsprofil konfigurieren
  - Hypervisor-Bereitstellungsprofil konfigurieren
  - Verbindungsprofil konfigurieren
  - Identität zuweisen
  - Bereitstellen
- Dell.Configuration. Ausführen von mit Hosts verknüpften Tasks
  - LED blinken, LED löschen
  - Starten der iDRAC-Konsole
  - Anzeigen und Löschen des SEL-Protokolls
- Dell.Inventory. Konfigurieren der Bestandsaufnahme
  - Anzeigen der Systembestandsliste auf der Registerkarte zur Dell Serververwaltung
  - Abrufen von Speicherdetails
  - Abrufen von Stromüberwachungsdetails

- Erstellen, Anzeigen, Bearbeiten, Löschen und Testen von Verbindungsprofilen auf der Seite mit den Verbindungsprofilen
- Planen, Aktualisieren und Löschen des Bestandsaufnahmezeitplans
- Ausführen einer Bestandsaufnahme auf Hosts

Nutzer- und Zugangsdatenverwaltung

Vorinstallierte Konten

Die folgende Tabelle beschreibt die vorinstallierten OMIVV-Konten:

Tabelle 4. Vorinstallierte Konten

Nutzerkonto	Beschreibung
OpenManage Integration for VMware vCenter-Administrator	Der Standardnutzer für die OMIVV-Webanwendungsverwaltung
Schreibgeschützter Nutzer	OMIVV bietet ein einzelnes standardmäßiges, lokales schreibgeschütztes Nutzerkonto. Der Administrator kann sich nur mit der VM-Remote-Konsole bei OMIVV anmelden. Dieses Konto kann während des Troubleshootings verwendet werden, um den Status und die Protokolle der kritischen Appliance anzuzeigen.
Linux-Betriebssystem-Root	Auf das Root-Betriebssystemkonto kann nicht zugegriffen werden. Das Team für den technischen Support verwendet das Root-Konto zum Debuggen von Problemen.

Standard-Zugangsdaten

In der folgenden Tabelle werden die Standardzugangsdaten für die vorinstallierten OMIVV-Konten beschrieben.

Tabelle 5. Standard-Zugangsdaten

Account (Konto)	Nutzer	Kennwort
OpenManage Integration for VMware vCenter-Administrator	Admin	Wird nach der Bereitstellung beim ersten Start festgelegt. Für weitere Informationen zum Ändern eines Administratorkennworts siehe Kennwort des OMIVV-Geräts ändern auf Seite 19.
Schreibgeschützter Nutzer	Nur Lesezugriff	Wird nach der Bereitstellung beim ersten Start festgelegt. Das Kennwort für den schreibgeschützten Nutzer kann nach der Anmeldung als schreibgeschützter Nutzer mithilfe von Linux-Standardbefehlen für die Kennwortänderung neu konfiguriert werden.
Linux-Betriebssystem-Root	Root	Die Root-Nutzeranmeldung ist deaktiviert, wenn OMIVV bereitgestellt wird.

Zugangsdaten verwalten

Wenn Sie sich zum ersten Mal bei der Dell EMC Verwaltungskonsole anmelden, melden Sie sich als Administrator an (der Standardnutzername lautet admin).

ANMERKUNG: Ein vergessenes Administratorkennwort kann von der OMIVV-Appliance nicht wiederhergestellt werden.

Kennwort des OMIVV-Geräts ändern

Info über diese Aufgabe

Sie können das Kennwort des OMIVV-Geräts im vSphere-Client unter Verwendung der Konsole ändern.

Schritte

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Admin-Kennwort ändern**.

   Folgen Sie den Anweisungen auf dem Bildschirm, um das Kennwort festzulegen.
3. Geben Sie im Textfeld **Aktuelles Kennwort** das aktuelle Administratorkennwort ein.
4. Geben Sie ein neues Kennwort im Textfeld **Neues Kennwort** ein.
5. Geben Sie das neue Kennwort erneut im Textfeld **Neues Kennwort bestätigen** ein.
6. Klicken Sie auf **Administratorkennwort**.

Autorisierung

Die OMIVV-Appliance unterstützt einen einzigen administrativen Nutzer.

Nach der Anmeldung bei OMIVV kann der Administrator nur auf die Konfigurationsfunktionen der OMIVV-Appliance zugreifen, z. B.:

- Neuen vCenter-Server registrieren
- Appliance konfigurieren
- OMIVV-Appliance durch RPM und Sichern und Wiederherstellen aktualisieren
- Network Time Protocol (NTP)-Server einrichten
- Bereitstellungsmodus konfigurieren
- Zertifikatsignierungsanforderung (CSR) erstellen
- HTTPS-Zertifikat hochladen
- Globale Alarme einrichten
- Erstellen und Herunterladen des Fehlerbehebungsbündels

Netzwerksicherheit

Die OMIVV-Appliance verwendet eine vorkonfigurierte Firewall, um die Sicherheit zu verbessern, indem der eingehende und ausgehende Netzwerkdatenverkehr auf die TCP- und UDP-Anschlüsse beschränkt wird. In der folgenden Tabelle sind die eingehenden und ausgehenden Anschlüsse aufgeführt, über die OMIVV mit Remote-Systemen kommuniziert.

Netzwerkexposition

OpenManage Integration for VMware vCenter verwendet eingehende und ausgehende Anschlüsse für die Kommunikation mit Remote-Systemen.

Ausgehende Anschlüsse

Ausgehende Anschlüsse können von OMIVV zum Herstellen einer Verbindung zu einem Remote-System verwendet werden.

Die in der folgenden Tabelle aufgeführten Anschlüsse sind die ausgehenden OMIVV-Anschlüsse.

Tabelle 6. Ausgehende Anschlüsse

Portnummer	Layer 4-Protokoll	Dienstleistungs-
7	TCP, UDP	ECHO
22	TCP	SSH

Tabelle 6. Ausgehende Anschlüsse (fortgesetzt)

Portnummer	Layer 4-Protokoll	Dienstleistungs-
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
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 über AMQP
8443	TCP	MCSDK 8443 ist eine Alternative für 443
9002	TCP	Data Protection Advisor REST API
9443	TCP	Avamar Management Console Web Service

Eingehende Anschlüsse

Die eingehenden Anschlüsse, die für die Verwendung durch ein Remote-System verfügbar sind, wenn Sie eine Verbindung zu OMIVV herstellen.

Die in der folgenden Tabelle aufgeführten Anschlüsse sind die eingehenden OMIVV-Anschlüsse.

Tabelle 7. Eingehende Anschlüsse

Portnummer	Layer 4-Protokoll	Dienstleistungs-
22	TCP	SSH
80	TCP	HTTP
443	TCP	HTTPS
5671	TCP	RabbitMQ über AMQP

Datensicherheit

Die Daten, die von OMIVV verwaltet werden, werden in internen Datenbanken innerhalb der Appliance gespeichert und gesichert und sind nicht von außen zugänglich.

Die Daten, die über OMIVV übertragen werden, werden durch einen sicheren Kommunikationskanal geschützt.

ANMERKUNG: Es wird empfohlen, die RESTful API-Benutzerzugangsdaten und Daten sicher gemäß ihren Umgebungsbeschränkungen abzurufen.

Kryptografie

OMIVV verwendet Kryptografie für die folgenden Komponenten:

- Zugangskontrolle
- Authentifizierung
- Digitale Signaturen

Aktualisieren des HTTPS-Zertifikats der OMIVV-Appliance

OMIVV verwendet Zertifikate für den sicheren HTTP-Zugriff (HTTPS).

Standardmäßig installiert und verwendet OMIVV das selbstsignierte Zertifikat für die sicheren HTTPS-Transaktionen.

Für eine höhere Sicherheit wird empfohlen, von einer Zertifizierungsstelle signierte oder benutzerdefinierte Zertifikate zu verwenden.

Das selbstsignierte Zertifikat genügt, um einen verschlüsselten Kanal zwischen Webbrowsern und dem Server herzustellen. Das selbstsignierte Zertifikat kann nicht für die Authentifizierung verwendet werden.

Sie können die folgenden Zertifikatarten für die OMIVV-Authentifizierung verwenden:

- Selbstsigniertes Zertifikat

  OMIVV erzeugt selbstsignierte Zertifikate, wenn sich die Hostname der Appliance ändert.

- Ein Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle signiert ist.

ANMERKUNG: Berücksichtigen Sie bei der Erstellung von Zertifikaten die Unternehmensrichtlinien.

Zertifikatsignierungsanforderung (CSR) erstellen

Voraussetzungen

Standardmäßig verfügt OMIVV über ein selbstsigniertes Zertifikat. Wenn Sie ein von einer benutzerdefinierten Zertifizierungsstelle (Certificate Authority, ca) signiertes Zertifikat für OMIVV benötigen, wird empfohlen, vor der vCenter-Registrierung ein neues Zertifikat hochzuladen.

Info über diese Aufgabe

Das Erstellen einer neuen CSR verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden. Um eine CSR zu erstellen, führen Sie die folgenden Schritte aus:

Schritte

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Zertifikatsignierungsanforderung erstellen** im Bereich **HTTPS-ZERTIFIKATE**.
   Eine Meldung zeigt an, dass wenn eine neue Anforderung erzeugt wird, mit dem vorherigen CSR erzeugte Zertifikate nicht mehr auf das Gerät hochgeladen werden. Um mit der Anforderung fortzufahren, klicken Sie auf **Weiter**.
2. Wenn Sie mit der Anfrage fortfahren, geben Sie im Dialogfeld **Zertifikatsignierungsanfrage erstellen** Informationen über den allgemeinen Namen, den Organisationsnamen, den Standort, den Bundesstaat, das Land, die E-Mail-Adresse und den alternativen Antragstellernamen (Subject Alternative Name, SAN) ein, und klicken Sie dann auf **Weiter**.

   ANMERKUNG: OMIVV bietet keine Unterstützung für mehrere Werte für SAN.

3. Klicken Sie auf **Herunterladen** und speichern Sie das resultierende CSR an einem zugänglichen Speicherort.

HTTPS-Zertifikat hochladen

Voraussetzungen

Stellen Sie sicher, dass das Zertifikat das PEM-Format verwendet.

Info über diese Aufgabe

Die HTTPS-Zertifikate werden für die sichere Kommunikation zwischen der OMIVV-Appliance und Hostsystemen oder vCenter verwendet. Um diese Art der sicheren Kommunikation einzurichten, senden Sie das CSR-Zertifikat an eine signierende Zertifizierungsstelle und laden Sie dann das resultierende CSR über die Verwaltungskonsole hoch. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

Schritte

1. Klicken Sie auf der Seite **APPPLIANCE-MANAGEMENT** auf **Zertifikat hochladen** im Bereich **HTTPS-ZERTIFIKATE**.
2. Klicken Sie auf **OK** im Dialogfeld **ZERTIFIKAT HOCHLADEN**.
3. Klicken Sie zum Hochladen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
   Um den Status zu prüfen, rufen Sie die **Ereigniskonsole** des vSphere-Clients registrierter vCenter auf.

Ergebnisse

Während des Hochladens von Zertifikaten reagiert die OMIVV-Verwaltungskonsole bis zu 3 Minuten lang nicht mehr. Schließen Sie nach Abschluss der Aufgabe „HTTPS-Zertifikat hochladen“ die Browsersitzung und greifen Sie auf das Admin-Portal in einer neuen Browsersitzung zu.

ANMERKUNG: Die OMIVV-Appliance-Zertifikatreferenz in registrierten vCentern wird automatisch aktualisiert. Stellen Sie sicher, dass von OMIVV ein Zugriff auf vCenter möglich ist, wenn das Zertifikat in OMIVV hochgeladen wird.

Standardmäßiges HTTPS-Zertifikat wiederherstellen

Schritte

1. Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Standardzertifikat wiederherstellen** im Bereich **HTTPS-ZERTIFIKATE**.
2. Klicken Sie im Dialogfeld **STANDARDMÄSSIGES ZERTIFIKAT WIEDERHERSTELLEN** auf **Anwenden**.

Ergebnisse

Während der Wiederherstellung von Zertifikaten reagiert die OMIVV-Verwaltungskonsole bis zu 3 Minuten lang nicht mehr. Schließen Sie nach Abschluss der Aufgabe „HTTPS-Zertifikat-Standardeinstellungen wiederherstellen“ die Browsersitzung und greifen Sie auf das Admin-Portal in einer neuen Browsersitzung zu.

Aktualisieren von HTTPS-Zertifikaten von registrierten vCenter-Servern

Info über diese Aufgabe

Wenn das Zertifikat auf einem vCenter Server geändert wird, führen Sie die folgenden Schritte durch, um das neue Zertifikat für OMIVV zu importieren:

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im Arbeitsbereich angezeigt.
3. Zum Aktualisieren des Zertifikats für eine vCenter Server-IP-Adresse oder den Hostnamen klicken Sie auf **Aktualisierung**.

Audit und Protokollierung

Der Administratornutzer kann die OMIVV-Verwaltungskonsole verwenden, um ein Troubleshooting-Bundle mit allen relevanten Protokollen zu erstellen.

Weitere Informationen finden Sie unter Troubleshootingbundle erstellen und herunterladen auf Seite 23.

Das schreibgeschützte Konto hilft beim Troubleshooting der Appliance, indem es dem Nutzer ermöglicht, verschiedene Parameter der Appliance während der Laufzeit zu lesen. Für erweitertes Troubleshooting nutzen Sie die Support-Leitfäden zur Überprüfung bestimmter Parameter.

ANMERKUNG: Nur der OMIVV-Admin-Benutzer kann Schreibvorgänge auf der Appliance durchführen. Benutzerüberwachung ist in den OMIVV-Protokollen nicht verfügbar. Weitere Informationen zu den im vCenter Plug-in ausgeführt ein vCenter Operations finden Sie in den vCenter Prüfprotokollen. Für RESTful APIs muss der Client in der Lage sein, die Überprüfungsprotokolle zu verarbeiten.

Troubleshootingbundle erstellen und herunterladen

Info über diese Aufgabe

Das Fehlerbehebungspaket enthält Informationen zur Protokollierung von OMIVV-Geräten, die verwendet werden können, um Probleme zu lösen oder an den technischen Support zu senden. OMIVV protokolliert keine sensiblen Nutzerdaten.

Schritte

1. Klicken Sie auf der Seite **Support** auf **Fehlerbehebungsdatei erstellen und herunterladen**.
   Das Dialogfeld **Fehlerbehebungsdatei** wird angezeigt.
2. Klicken Sie im Dialogfeld **Fehlerbehebungsdatei** auf **ERSTELLEN**.
   Je nach Größe der Protokolle kann die Erstellung der Datei einige Zeit dauern.
3. Klicken Sie auf **DOWNLOAD**, um die Datei zu speichern.
   Die Anmeldeseite für die Dell EMC OMIVV-Verwaltungskonsole wird angezeigt.
4. Melden Sie sich bei der Dell EMC OMIVV-Verwaltungskonsole an.
5. Laden Sie das Troubleshootingbundle herunter.

Erstellen und Herunterladen des Fehlerbehebungsbündels

Voraussetzungen

Um das Fehlerbehebungspaket zu erzeugen, stellen Sie sicher, dass Sie sich beim Administratorportal anmelden.

Info über diese Aufgabe

Das Fehlerbehebungspaket enthält Protokollierungsinformationen von OMIVV, die zur Unterstützung bei der Behebung von Problemen verwendet oder an den technischen Support gesendet werden können.

Schritte

1. Klicken Sie auf der Seite **GERÄTEMANAGEMENT** auf **Fehlerbehebungspaket erstellen**.
2. Klicken Sie auf **Fehlerbehebungspaket herunterladen**.

Betriebsfähigkeit

Die Support-Website **https://www.dell.com/support** bietet Zugriff auf Lizenzierungsinformationen, Produktdokumentation, Ratgeber, Downloads und Troubleshooting-Informationen. Diese Informationen helfen Ihnen bei der Lösung eines Produktproblems, bevor Sie sich an das Support-Team wenden.

Eine spezielle Anmeldung bei OMIVV ist für Servicemitarbeiter nicht erforderlich. Wenn das Troubleshooting-Bundle nicht ausreicht, können Servicemitarbeiter den Root-Nutzer aktivieren, um weitere Informationen zu sammeln.

Stellen Sie sicher, dass Sie Sicherheitspatches und andere Updates installieren, sobald diese verfügbar sind, einschließlich OMIVV-vCenter-Betriebssystem-Updates.

Sicherheitspatches

Regelmäßige OMIVV-Updates, die Sicherheitsupdates enthalten, und nur Sicherheitsupdates, die nach Bedarf veröffentlicht werden.

Die Updates sind kumulativ und werden auf der Support-Webseite veröffentlicht. OMIVV-Nutzer erhalten entsprechende Benachrichtigungen in vCenter.

OMIVV-BS-Update

In regelmäßigen Abständen werden Sicherheitspatches und Korrekturen für das OMIVV-Betriebssystem veröffentlicht.

Diese Korrekturen müssen in vorhandenen OVF-Bereitstellungen von OMIVV über ein RPM-Updatepaket installiert werden. Wenn verfügbar, wird dringend empfohlen, diese Sicherheitspatches und Korrekturen auf dem OMIVV-Server über ein RPM-Update zu installieren.

Produktcode-Integrität

Das Installationsprogramm für die OMIVV-Software wird von Dell signiert. Es wird empfohlen, dass Sie die Echtheit der OMIVV-Installationsprogrammsignatur überprüfen.

5

Sonstige Konfigurations- und Managementeinstellungen

Themen:

OpenManage Integration for VMware vCenter-Lizenzierung (OMIVV)

OMIVV verfügt über zwei Arten von Lizenzen:

- Evaluierungslizenz – Wenn die OMIVV Appliance zum ersten Mal hochgefahren wird, wird automatisch eine Evaluierungslizenz installiert. Die Testversion beinhaltet eine Test-Lizenz für fünf Hosts (Server), die durch OMIVV verwaltet werden. Diese 90-Tage-Testversion ist die Standardlizenz, die mitgeliefert wird.
- Standard Lizenz – Sie können eine beliebige Anzahl von Host-Lizenzen erwerben, die von OMIVV verwaltet werden. Diese Lizenz umfasst Produktunterstützung und Updates der OMIVV-Appliance. Die Standard Lizenz ist für drei oder fünf Jahre verfügbar. Jede zusätzliche erworbene Lizenz verlängert den Zeitraum der bestehenden Lizenz. Die Standardlizenz überschreibt eine Evaluierungslizenz.

Die Lizenzdauer für einen einzelnen XML-Schlüssel wird basierend auf dem Verkaufstermin der ursprünglichen Bestellung berechnet. Alle hochgeladenen neuen Lizenzen werden nach Ablauf der Toleranzperiode von 90 Tagen in der Zählung für eine vorab ablaufende Lizenzierung angezeigt.

Der OMIVV unterstützt bis zu 15 vCenter-Instanzen. Wenn Sie eine Testlizenz auf eine vollwertige Standardlizenz hochstufen, erhalten Sie eine Bestellbestätigung per E-Mail und können die Lizenzdatei im Dell Digital Locker herunterladen. Speichern Sie die XML-Lizenzdatei auf Ihrem lokalen System und laden Sie die neue Lizenzdatei mithilfe der **Verwaltungskonsole** hoch.

Wenn Sie die Lizenzdatei kaufen, können Sie die XML-Datei (Lizenzschlüssel) über Dell Digital Locker unter https://www.dell.com/support herunterladen. Wenn Sie einen Lizenzschlüssel nicht herunterladen können, finden Sie unter **Bestellsupport kontaktieren** auf der Seite https://www.dell.com/support die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt.

Die Lizenzierung enthält die folgenden Informationen in der OMIVV-Verwaltungskonsole:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu 15 registrierte und verwendete vCenter-Verbindungen sind aktiviert.
- Höchstzahl der Host-Verbindungslizenzen – die Anzahl der erworbenen Hostverbindungen (mit maximal 2000 Hosts, die für eine einzige OMIVV-Instanz unterstützt werden).
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern), die in die Bestandsliste aufgenommen wurden.
- Verfügbar – die Anzahl von Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.

Beim Versuch, einen Host zu einem Host-Zugangsdatenprofil hinzuzufügen, wird verhindert, dass weitere Hosts hinzugefügt werden, wenn die Anzahl der lizenzierten Servern über die Lizenzanzahl hinausgeht. OMIVV bietet keine Unterstützung für die Verwaltung einer Anzahl von Hosts, die die Anzahl der verfügbaren Hostlizenzen übersteigt.

Verwenden Sie die OMIVV RESTful API, um weitere Informationen zur Lizenz zu erhalten. Weitere Informationen finden Sie unter *API-Handbuch von OpenManage Integration for VMware vCenter* unter https://www.dell.com/support.

ANMERKUNG: Jede aktive Lizenz kann für OMIVV 5.x-Versionen verwendet werden. Lizenzen, die von vorherigen Instanzen von OMIVV gesichert oder erneut von Digital Locker heruntergeladen wurden, können für aktuelle Instanzen von OMIVV verwendet werden.

Schutz von Authentizität und Integrität

Zur Sicherstellung der Integrität des Produkts sind die OMIVV-Installations- und Updatekomponenten signiert.

Um die Kommunikationsintegrität zu gewährleisten, wird empfohlen, ein von einer Zertifizierungsstelle signiertes Zertifikat zu verwenden.

Backups und Wiederherstellungen in OMIVV verwalten

Zum Schutz von OMIVV vor einem Notfallszenario wird empfohlen, dass Sie Backups von OMIVV durchführen. Falls erforderlich, können Sie OMIVV aus diesen Backups wiederherstellen. Weitere Informationen zum Backup und zur Wiederherstellung finden Sie im OMIVV-Benutzerhandbuch unter **https://www.dell.com/support**.