OpenManage Integration for VMware vCenter Version 5.4

Installationsanleitung

März 2023
Rev. A01

DELL Technologies

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: HINWEIS enthält wichtige Informationen, mit denen Sie Ihr Produkt besser nutzen können.

VORSICHT: ACHTUNG deutet auf mögliche Schäden an der Hardware oder auf den Verlust von Daten hin und zeigt, wie Sie das Problem vermeiden können.

WARNUNG: WARNUNG weist auf ein potenzielles Risiko für Sachschäden, Verletzungen oder den Tod hin.

© 2021- 2023 Dell Inc. oder Ihre Tochtergesellschaften. Alle Rechte vorbehalten. Dell Technologies, Dell und andere Marken sind Marken von Dell Inc. oder ihren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

Inhaltsverzeichnis

1

Einführung

Dieses Handbuch enthält Anweisungen zur Installation und Konfiguration von OpenManage Integration for VMware vCenter (OMIVV). OMIVV wird verwendet, um PowerEdge-Server zu ermitteln, zu überwachen und zu verwalten, auf denen VMware vCenter ausgeführt wird. Zur Durchführung von Bestandsverwaltung, Überwachung und Warnmeldungen, Firmware-Aktualisierungen und Service-Management nach dem erfolgreichen Abschluss der Installation von OMIVV finden Sie weitere Informationen im *OpenManage Integration for VMware vCenter-Benutzerhandbuch* unter **https://www.dell.com/support**.

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.

Eine Softwarelizenz erwerben

Schritte

1. Navigieren Sie zu **Einstellungen** > **Lizenzierung** > **Lizenz kaufen**, oder **Dashboard** > **Lizenz kaufen** oder **Admin Portal** > **vCenter Registrierung** > **Lizenzierung** > **JETZT KAUFEN**.
   Die Supportseite von DellEMC wird angezeigt.
2. Laden Sie die Lizenzdatei herunter und speichern Sie sie an einem bekannten Speicherort.
   Möglicherweise erhalten Sie die Lizenzdatei als gepackte ZIP-Datei. Stellen Sie sicher, dass Sie die Zip-Datei entpacken und laden Sie nur die XML-Lizenzdatei hoch. Die Lizenzdatei wird wahrscheinlich auf Grundlage Ihrer Auftragsnummer benannt (wie beispielsweise 123456789.xml).

Lizenzen verwalten

Lizenzdatei für neue Einkäufe

Wenn Sie eine neue Lizenz bestellen, wird nach der Auftragsbestätigung eine E-Mail von Dell gesendet. Sie können die neue Lizenzdatei im Dell Digital Locker unter **https://www.dell.com/support** herunterladen. Die Lizenz wird Ihnen als XML-Datei zugesendet. Wenn Sie stattdessen eine ZIP-Datei erhalten, extrahieren Sie die XML-Datei, bevor Sie Sie hochladen.

Stacking-Lizenzen

OMIVV kann mehrere Standardlizenzen zur Erhöhung der Anzahl unterstützter Hosts auf die Summe der in den hochgeladenen Lizenzen enthaltenen Hosts stapeln. Eine Evaluierungslizenz kann nicht gestapelt werden. Standardmäßig unterstützt OMIVV bis zu 15 vCenter. Wenn Sie mehr als 15 vCenter verwalten möchten, verwenden Sie mehrere Appliances.

Wenn eine neue Standardlizenz hochgeladen wird, bevor die vorhandene Standardlizenz abläuft, werden die Lizenzen gestapelt. Andernfalls wird, wenn die Lizenz abgelaufen ist und eine neue Lizenz hochgeladen wird, nur die Anzahl der Hosts unterstützt, die in der neuen Lizenz enthalten ist. Wenn Sie bereits mehrere Lizenzen hochgeladen haben, ist die Anzahl unterstützter Hosts die Summe der Hosts in den nicht abgelaufenen Lizenzen zu dem Zeitpunkt, zu dem die letzte Lizenz hochgeladen wurde.

Abgelaufene Lizenzen

Das Hochladen von Lizenzen, bei denen die unterstützte Laufzeit überschritten wurde, welche typischerweise drei oder fünf Jahre ab Kaufdatum beträgt, wird blockiert. Wenn Lizenzen nach dem Hochladen abgelaufen sind, können einige Funktionen möglicherweise nicht ausgeführt werden. Upgrades auf neue Versionen von OMIVV werden jedoch blockiert.

Ersatz von Lizenzen

Sollte ein Problem mit Ihrer Bestellung vorliegen, erhalten Sie eine Ersatzlizenz von Dell EMC. Die Ersatzlizenz enthält die gleiche Berechtigungs-ID wie die vorherige Lizenz. Beim Hochladen einer Ersatzlizenz wird eine bereits mit der gleichen Berechtigungs-ID hochgeladene Lizenz ersetzt.

Erzwingung

Geräte-Aktualisierungen

Das Gerät erlaubt keine Aktualisierungen auf neuere Versionen, wenn alle Lizenzen abgelaufen sind. Erwerben Sie eine neue Lizenz und laden Sie sie vor der Aktualisierung des Geräts hoch.

Testlizenz

Wenn eine Testlizenz abläuft, funktionieren mehrere wichtige Bereiche nicht mehr und es wird eine entsprechende Fehlermeldung angezeigt.

Wichtige Hinweise zu Referenzzwecken

- Ab OMIVV 5.0 wird nur der VMware vSphere Client (HTML5) unterstützt und der vSphere Webclient (Flex) wird nicht unterstützt.
- Für die Verwendung des DNS-Servers gelten die folgenden empfohlenen Vorgehensweisen:
  - OMIVV unterstützt nur IPv4-IP-Adressen. Obwohl sowohl die statische IP-Zuweisung und die DHCP-Zuweisung unterstützt werden, wird empfohlen, eine statische IP-Adresse zuzuweisen. Weisen Sie eine statische IP-Adresse und einen Hostnamen zu, wenn Sie eine OMIVV-Appliance mit einer gültigen DNS-Registrierung bereitstellen. Bei einer statischen IP-Adresse ist sichergestellt, dass die IP-Adresse der OMIVV-Appliance beim Neustart des Systems gleich bleibt.
  - Stellen Sie sicher, dass die OMIVV-Hostnamen-Einträge in der Vorwärts- und Rückwärtssuche Ihres DNS-Servers vorhanden sind.
- Für den OMIVV-Appliancemodus stellen Sie sicher, dass Sie OMIVV im entsprechenden Modus basierend auf Ihrer Virtualisierungsumgebung bereitstellen. Weitere Informationen finden Sie unter Bereitstellungsmodus konfigurieren.
- Konfigurieren Sie das Netzwerk gemäß den Portanforderungen. Weitere Informationen finden Sie unter . Portinformationen

Weitere Informationen zu den DNS-Anforderungen für vSphere finden Sie in den folgenden VMware-Links:

- DNS-Anforderungen für vSphere 6.5 und Platform Services Controller-Appliance
- DNS-Anforderungen für vSphere 6.7 und Platform Services Controller unter Windows

Hardwareanforderungen

OMIVV bietet vollständige Unterstützung für Dell EMC Server mit Unterstützung des vollen Funktionsumfangs für iDRAC Express und Enterprise. Um zu überprüfen, ob Ihre Host-Server berechtigt sind, prüfen Sie die Informationen zu Folgendem in den nachfolgenden Unterabschnitten:

- Unterstützte BIOS- und iDRAC-Versionen
- Unterstützte iDRAC-Versionen (für Bereitstellung sowie Verwaltung)
- Unterstützter Speicher, CPU und Speicherplatz für bereitgestellten Speicher

OMIVV erfordert LAN auf der Hauptplatine oder Netzwerk-Tochterkarte, das auf das Verwaltungsnetzwerk von iDRAC und CMC oder OME Modular-Systemen und das vCenter Verwaltungsnetzwerk zugreifen kann. Weitere Informationen finden Sie unter OMIVV-Gerät konfigurieren und Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs).

Unterstützte BIOS-Versionen

Die folgenden BIOS- und iDRAC-Versionen mit Lifecycle Controller sind für die Aktivierung der Funktionen von OpenManage Integration for VMware vCenter erforderlich.

Es wird empfohlen, das startfähige ISO-Image, das unter Verwendung des Repository Manager oder der Lifecycle-Controller-Plattform erstellt wurde, zum Update Ihrer Server auf eine der folgenden Basisversionen zu verwenden, bevor Sie OMIVV verwenden:

Tabelle 1. Unterstützte BIOS-Version für 12G PowerEdge-Server

Server	Minimale BIOS-Version
M420	1.2.4 oder höher
M520	1.2.6 oder höher
M620	1.2.6 oder höher
M820	1.2.6 oder höher
R220	1.0.3 oder höher
R320	1.2.4 oder höher
R420	1.2.4 oder höher

Tabelle 1. Unterstützte BIOS-Version für 12G PowerEdge-Server (fortgesetzt)

Server	Minimale BIOS-Version
R520	1.2.4 oder höher
R620	1.2.6 oder höher
R720	1.2.6 oder höher
R720xd	1.2.6 oder höher
R820	1.7.2 oder höher
R920	1.1.0 oder höher
T320	1.0.1 oder höher
T420	1.0.1 oder höher
T620	1.2.6 oder höher

Tabelle 2. Unterstützte BIOS-Version für 13G PowerEdge-Server

Server	Minimale BIOS-Version
FC430	1.0.0 oder höher
FC630	1.0.0 oder höher
FC830	1.0.0 oder höher
M630	1.0.0 oder höher
M830	1.0.0 oder höher
R630	1.0.4 oder höher
R730	1.0.4 oder höher
R730xd	1.0.4 oder höher
R430	1.0.4 oder höher
R530	1.0.2 oder höher
R830	1.0.2 oder höher
R930	1.0.2 oder höher
R230	1.0.2 oder höher
R330	1.0.2 oder höher
T630	1.0.2 oder höher
T130	1.0.2 oder höher
T330	1.0.2 oder höher
T430	1.0.2 oder höher

Tabelle 3. Unterstützte BIOS-Version für iDRAC9-basierte PowerEdge-Server

Server	Minimale BIOS-Version
FC640	1.0.0 oder höher
MX740C	1.0.0 oder höher
MX840C	1.0.0 oder höher
M640	1.0.0 oder höher
MX750C	1.0.0 oder höher
R240	1.0.0 oder höher

Tabelle 3. Unterstützte BIOS-Version für iDRAC9-basierte PowerEdge-Server (fortgesetzt)

Server	Minimale BIOS-Version
R250	1.2.5 oder höher
R340	1.0.0 oder höher
R350	1.2.5 oder höher
R940	1.0.0 oder höher
R940xa	1.0.0 oder höher
R740	1.0.0 oder höher
R740xd	1.0.0 oder höher
R740xd2	1.0.0 oder höher
R640	1.0.0 oder höher
R840	1.0.0 oder höher
R440	1.0.0 oder höher
R540	1.0.0 oder höher
R6415	1.0.0 oder höher
R7425	1.0.0 oder höher
R7415	1.0.0 oder höher
R6515	1.0.3 oder höher
R7515	1.0.3 oder höher
R6525	1.0.0 oder höher
R7525	1.2.4 oder höher
R750	1.0.0 oder höher
R650	1.0.0 oder höher
R750xa	1.0.0 oder höher
R750xs	1.2.1 oder höher
R650xs	1.2.1 oder höher
R550	1.2.1 oder höher
R450	1.2.1 oder höher
T140	1.0.0 oder höher
T150	1.2.5 oder höher
T340	1.0.0 oder höher
T350	1.2.5 oder höher
T640	1.0.0 oder höher
T440	1.0.0 oder höher
XR2	2.2.11 oder höher
XR11	1.0.2 oder höher
XR12	1.0.2 oder höher
XE2420	1.0.0 oder höher
XE8545	1.0.0 oder höher

Tabelle 4. Unterstützte BIOS-Version für vSAN Ready Nodes

vSAN Ready Node	Minimale BIOS-Version
R740xd	1.0.0 oder höher
R640	1.0.0 oder höher
R440	1.0.0 oder höher
R6415	1.0.0 oder höher
R7415	1.0.0 oder höher
R7425	1.0.0 oder höher
R6515	1.0.3 oder höher
R7515	1.0.3 oder höher
C6420	1.0.0 oder höher
R840	1.0.0 oder höher
R750	1.0.0 oder höher
R650	1.0.0 oder höher
R7525	1.2.4 oder höher

Unterstützte iDRAC-Versionen mit Lifecycle Controller

Tabelle 5. Unterstützte iDRAC und Lifecycle Controller für die Bereitstellung

Server	iDRAC mit Lifecycle Controller
12G	2.50.50.50 oder höher
13G	2.50.50.50 oder höher
iDRAC9-basierte Server	3.00.00.00 und höher

Tabelle 6. BIOS- und iDRAC-Anforderungen für den Cloud-Server

Modell	BIOS	iDRAC mit Lifecycle Controller
C6320	1.0.2	2.50.50.50 oder höher
C4130	1.0.2	2.50.50.50 oder höher
C6420	1.0.0 oder höher	3.00.00.00 oder höher
C4140	1.0.0 oder höher	3.00.00.00 oder höher
C6525	1.0.0 oder höher	ab Version 3.42.42.42
C6520	1.0.0 oder höher	4.40.21.00 oder höher

Unterstützte Funktionen auf PowerEdge-Servern

Die folgenden Funktionen werden auf den von OpenManage Integration for VMware vCenter verwalteten Hosts unterstützt:

Tabelle 7. Unterstützte Funktionen auf PowerEdge-Servern

Funktionen	12G und 13G	iDRAC9-basierte Server
Hardware-Bestandsaufnahme	J	J
Ereignisse und Alarme	J (SNMP v1 und v2)	J (SNMP v1 und v2)

Tabelle 7. Unterstützte Funktionen auf PowerEdge-Servern (fortgesetzt)

Funktionen	12G und 13G	iDRAC9-basierte Server
Komponentenbezogene Funktionszustandsüberwachung*	J	J
BIOS/Firmwareaktualisierungen#	J	J
Proaktive Hochverfügbarkeit	J	J
Gewährleistungsinformationen	J	J
Verwaltungs-Compliance	J	J
Konfigurations-Compliance	J	J
Automatische/Manuelle Ermittlung von Bare-Metal-Server	J	J
Bare-Metal-Compliance	J	J
Hardwarekonfiguration	J	J
BS-Bereitstellung	J	J
Blinkende Server-LED	J	J
SEL-Protokolle anzeigen/löschen	J	J
iDRAC verknüpfen und starten	J	J
iDRAC-Reset	J	J
Systemsperrmodus	N	J
Systemprofil	J	J
Clusterprofil	J	J
Hostverwaltung mit einheitlicher Gehäuse-IP	N	J@
Support für OEM-Server	J~	J
vSphere Lifecycle Manager	Y ^	Y ^

* In der Cloud mit Modellnummer C6320 wird die Funktionszustandsüberwachung für die Zusatzkarten nicht unterstützt.

In der Cloud mit Modellnummer C6320 werden Firmwareaktualisierungen für die Zusatzkarten nicht unterstützt.

@ Gilt nur für einen MX-Gehäuse-Host. Bestandsaufnahme, Überwachung, proaktive Hochverfügbarkeit und Funktionen zur Firmwareaktualisierung werden unterstützt.

~ Nur für Rack-Server unterstützt

^ Nur für vSphere 7.0 und höher zertifizierte Plattformen

Unterstützte Funktionen für PowerEdge-Gehäuse

Dieses Thema enthält Informationen zu den unterstützten Funktionen auf dem PowerEdge-Gehäuse.

Tabelle 8. Unterstützte Funktionen für modulare Infrastruktur

Funktionen	M1000e	VRTX	FX2s	MX
SNMP-Warnungen	J	J	J	J
Hardware-Bestandsaufnahme	J	J	J	J
CMC oder Managementmodul verknüpfen und starten	J	J	J	J

Tabelle 8. Unterstützte Funktionen für modulare Infrastruktur (fortgesetzt)

Funktionen	M1000e	VRTX	FX2s	MX
Lizenzinformationen	k. A.	J	J	J
Garantie-Informationen	J	J	J	J
Funktionszustandmeldung	J	J	J	J
Gruppenbeziehungsinformationen zur Verwaltung von mehreren Gehäusen	N	N	N	J
Firmware-Aktualisierung	N	N	N	J

Erforderlicher Speicherplatz für bereitgestellten Speicher

Die virtuelle OMIVV-Appliance erfordert mindestens 95 GB Speicherplatz für bereitgestellten Speicher.

Standardmäßige Virtual Appliance-Konfiguration

Das virtuelle OMIVV-Gerät wird mit 8 GB RAM und zwei virtuellen CPUs bereitgestellt (Bereitstellungsmodus „Klein“).

Softwareanforderungen

Stellen Sie sicher, dass die vSphere-Umgebung die Systemanforderungen der virtuellen Appliance sowie die Anforderungen des Schnittstellenzugriffs, der Zeitsynchronisation und der Überwachungsschnittstelle erfüllt. Weitere Informationen über Port-Anforderungen finden Sie unter Portinformationen.

Zur Anzeige von OpenManage Integration for VMware vCenter muss ein System mindestens über eine Bildschirmauflösung von 1024 x 768 und einen Webbrowser verfügen, der die Mindestanforderungen basierend auf dem Betriebssystem erfüllt.

Es wird die Verwendung von Google Chrome für den Zugriff auf die OMIVV-Funktionen empfohlen. OMIVV unterstützt Google Chrome und Mozilla Firefox. Microsoft Internet Explorer wird nicht unterstützt.

Es wird empfohlen, die neueste Version der unterstützten Browser zu verwenden. Informationen zur Unterstützung bestimmter Browserversionen finden Sie in der VMware-Dokumentation für die vCenter-Version, die Sie verwenden.

Voraussetzungen für den VMware vSphere Client (HTML5)

vCenter 6.5 U2 und höher

OpenManage Integration for VMware vCenter bietet Unterstützung für folgende vCenter Server-Versionen:

Tabelle 9. Unterstützte vCenter Serverversionen

vCenter-Version	Client-Unterstützung
6.5 U2	J
6.5 U3	J
6.7	J
6.7 U1	J
6.7 U2	J
6.7 U3	J
7.0	J
7.0 U1	J
7.0 U2	J

Tabelle 9. Unterstützte vCenter Serverversionen (fortgesetzt)

vCenter-Version	Client-Unterstützung
7.0 U3	J

Verwenden Sie den neuesten Patch 13638625 oder höher für vCenter 6.5 U2.

Die OMIVV 5.4 Appliance läuft auf CentOS Version 7.9.

Unterstützte ESXi-Versionen auf verwalteten Hosts

Info über diese Aufgabe

Die folgende Tabelle enthält Informationen über die unterstützten ESXi-Versionen auf verwalteten Hosts:

Tabelle 10. Unterstützte ESXi-Versionen

ESXi Version	12G	13G	iDRAC9-basierte Server
6.0 U3	J	J	N
6.5	J	J	N
6.5 U1	J	J	J
6.5 U2	J	J	J
6.5 U3	J	J	J
6.7	N	J	J
6.7 U1	N	J	J
6.7 U2	N	J	J
6.7 U3	N	J	J
7.0	N	J	J
7.0 U1	N	J	J
7.0 U2	N	J	J
7.0 U3	N	J	J

ANMERKUNG: Der PowerEdge MX-Host wird nur unterstützt, wenn er mit ESXi 6.5 U2 und höher verwendet wird.

Portinformationen

In diesem Abschnitt werden alle Portanforderungen für die Konfiguration der virtuellen Appliance und der verwalteten Nodes aufgeführt.

Tabelle 11. Virtual Appliance

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
53	DNS	TCP	Keine	Ausgang	OMIVV-Appliance zu DNS-Server	DNS-Client	Konnektivität zum DNS-Server oder Auflösen der Hostnamen.
68	DHCP	UDP	Keine	Eingang	DHCP-Server zu OMIVV-Appliance	Dynamische Netzwerkkonfiguration	Um die Netzwerkdetails wie IP, Gateway, Netzmaske und DNS abzurufen.

Tabelle 11. Virtual Appliance (fortgesetzt)

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
69	TFTP	UDP	128 Bit	Ausgang	OMIVV auf iDRAC	Einfache Dateiübertragung	Wird verwendet, um den Bare-Metal-Server auf die erforderliche Mindestversion der Firmware zu aktualisieren.
123	NTP	UDP	Keine	Eingang	NTP zu OMIVV-Appliance	Zeitsynchronisation	Zum Synchronisieren mit einer bestimmten Zeitzone.
162	SNMP-Agent	UDP	Keine	Eingang	iDRAc oder CMC oder OME-Modular zu OMIVV-Appliance	SNMP-Agent (Server)	Für den Empfang von SNMP-Traps von verwalteten Knoten.
80/443	HTTP oder HTTPS	TCP	Keine	Ausgang	OMIVV-Appliance zu Internet	Dell Online-Datenzugriff	Konnektivität zu Online-Gewährleistung (Internet), Firmware und aktuellen RPM-Informationen.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV UI zu OMIVV-Appliance	HTTPS-Server	Von OMIVV angebotene Webdienste. Diese Webdienste werden vom vSphere Client und Dell Admin-Portal genutzt.
443	HTTPS	TCP	128 Bit	Eingang	ESXi-Server zu OMIVV-Appliance	HTTPS-Server	Wird im Betriebssystem-Bereitstellungsprozess für Skripts nach der Installation zur Kommunikation mit der OMIVV-Appliance verwendet.
443	HTTPS	TCP	128 Bit	Eingang	iDRAC zu OMIVV-Appliance	Automatische Ermittlung	Bereitstellungsserver, der für die automatische Ermittlung von verwalteten Knoten verwendet wird.
443	WSMAN	TCP	128 Bit	Ein/Aus	OMIVV-Appliance zu oder von iDRAC	iDRAC-Kommunikation	iDRAC-, CMC- oder OME-Modular-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
445/139	KMU	TCP	128 Bit	Ausgang	OMIVV-Appliance zu CIFS	CIFS-Kommunikation	Für die Kommunikation mit Windows-Freigaben.
2049 /111	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Appliance zu gemanagter Node (iDRAC)	Öffentliche Freigabe	Öffentliche NFS-Freigabe, die von der OMIVV-Appliance für die verwalteten Nodes verfügbar gemacht und für Firmwareupdates- und Betriebssystem-Bereitstellungsprozesse verwendet wird.
4001 bis 4004	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Appliance zu NFS	Öffentliche Freigabe	Diese Ports müssen offen gehalten werden zur Ausführung der statd, quotd, lockd, und mountd Dienstleistungen durch den V2 und V3-Protokolle der NFS-Server.
Benutzer definierte	Beliebig	UDP/TCP	Keine	Ausgang	OMIVV-Appliance zu Proxyserver	Proxy	Für die Kommunikation mit dem Proxyserver

Tabelle 12. Gemanagte Nodes (iDRAC)

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
162	SNMP	UDP	Keine	Ausgang	OMIVV-Appliance zu gemanagter Node (iDRAC)	Hardware-Ereignisse	Asynchrone SNMP-Traps, die von iDRAC gesendet werden. Dieser Port muss über iDRAC geöffnet werden.
443	WSMAN	TCP	128 Bit	Eingang	OMIVV-Appliance zu gemanagter Node (iDRAC)	iDRAC-Kommunikation	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über iDRAC geöffnet werden.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV-Appliance zu gemanagter Node (iDRAC)	HTTPS-Server	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über iDRAC geöffnet werden.

Weitere Informationen über die iDRAC und CMC Portinformationen finden Sie im *Integrated Dell Remote Access Controller-Benutzerhandbuch* und im *Dell Chassis Management Controller Benutzerhandbuch* unter **https://www.dell.com/support**.

Weitere Informationen über die OME Modular Portinformationen finden Sie im *Dell EMC OME-Modular Benutzerhandbuch* unter **https://www.dell.com/support**.

Dell Online Ziel-URL

Tabelle 13. Dell Online Ziel-URL

Funktion	Ziel-URL
Garantiedetails	https://apigtwb2c.us.dell.com
Garantieschlüssel	https://downloads.dell.com/catalog/CatalogIndex.gz
Firmware-Aktualisierung	https://downloads.dell.com
RPM-Upgrade	https://linux.dell.com

2

OMIVV installieren und konfigurieren

Voraussetzungen

Stellen Sie sicher, dass alle Anforderungen erfüllt sind und Sie das benötigte VMware vCenter ausführen. Weitere Informationen finden Sie unter Hardwareanforderungen und Softwareanforderungen.

Info über diese Aufgabe

Die folgenden Schritte fassen das allgemeine Installations- und Konfigurationsverfahren für die OMIVV zusammen:

Schritte

1. Laden Sie die Datei *DellEMC_OpenManage_Integration_<version number>.<build number>.zip* von der Dell Supportwebsite unter **https://www.dell.com/support** herunter. Weitere Informationen zum Herunterladen von OMIVV finden Sie unter OpenManage Integration for VMware vCenter herunterladen.
2. Navigieren Sie zu dem Speicherort, an dem Sie die Datei heruntergeladen haben, und extrahieren Sie den Inhalt.
3. Stellen Sie mithilfe des vSphere Client (HTML5) eine Open Virtualization Format(OVF)-Datei bereit, die die OMIVV-Appliance enthält. Siehe Bereitstellen der OMIVV-OVF.
4. Nachdem Sie eine OVF bereitgestellt haben, legen Sie die Zeitzone, das aktuelle Datum und die Uhrzeit fest. Weitere Informationen finden Sie unter Konfigurieren des Network Time Protocol (NTP) und Einstellen der lokalen Zeitzone.
5. Konfigurieren Sie die Netzwerkeinstellungen. Weitere Informationen finden Sie unter OMIVV-Gerät konfigurieren.
6. Laden Sie die Lizenzdatei hoch. Weitere Informationen zur Lizenzierung finden Sie unter Hochladen einer Lizenz auf die OMIVV-Verwaltungskonsole.
7. Stellen Sie den Bereitstellungsmodus gemäß der Anforderung ein. Weitere Informationen finden Sie unter Bereitstellungsmodus konfigurieren.
8. Registrieren Sie die OMIVV-Appliance über die Verwaltungskonsole beim vCenter Server. Informationen dazu finden Sie unter Neuen vCenter Server registrieren.
9. Schließen Sie die Appliance-Konfigurationseinstellungen ab. Weitere Informationen finden Sie unter OMIVV-Gerät konfigurieren.

Themen:

Voraussetzungs-Checkliste

Bevor Sie mit der Produktinstallation beginnen, stellen Sie Folgendes sicher:

- Überprüfen Sie, ob Sie über Nutzername und Kennwort für OMIVV verfügen, um auf den vCenter-Server zuzugreifen. Der Nutzer hat möglicherweise eine Administratorrolle mit allen erforderlichen Berechtigungen oder einen Nicht-Administratornutzer mit den erforderlichen Berechtigungen. Weitere Informationen über die Liste der Berechtigungen, die für die Ausführung von OMIVV erforderlich sind, erhalten Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Nutzer.
- Stellen Sie sicher, dass Sie über das Root-Kennwort für 6.5 U3 und ältere ESXi-Hostsysteme oder Active Directory-Anmeldeinformationen mit Administratorrechten auf dem Host verfügen.

- Überprüfen Sie, ob Sie über den Nutzernamen und das Kennwort verfügen, der bzw. das mit iDRAC Express oder Enterprise assoziiert ist und über Administratorrechte auf dem iDRAC verfügt.
- Sie haben Administratorrechte in iDRAC.
- Die einfache 2FA- und Smart Card-Anmeldung sind in iDRAC für iDRAC9-basierte Server deaktiviert.
- Überprüfen Sie, ob der vCenter-Server ausgeführt wird.
- Bestimmen Sie den Speicherort des OMIVV-Installationsverzeichnisses.
- Die OMIVV und der vCenter-Server müssen sich im gleichen Netzwerk befinden.
- Es besteht eine Route zwischen den vCenter-, OMIVV- und den iDRAC-Netzwerken, wenn vCenter, OMIVV und iDRAC sich in verschiedenen Netzwerken befinden. Dies gilt nur, wenn die OMIVV-Appliance nicht mit zwei NICs konfiguriert ist.
- Die VMware vSphere-Umgebung muss die Systemanforderungen der virtuellen Appliance sowie die Anforderungen des Portzugriffs, der Zeitsynchronisierung und des Überwachungsports erfüllen.
- Stellen Sie sicher, dass Sie den Test für den Host über die iDRAC Webschnittstelle zur Verwaltung der OMIVV-Schlüsselfunktionen aktivieren.

ANMERKUNG: Das virtuelle Gerät fungiert als reguläre virtuelle Maschine. Jede Unterbrechung oder jedes Herunterfahren wirkt sich auf die allgemeine Funktion des virtuellen Geräts aus.

OpenManage Integration for VMware vCenter herunterladen

Voraussetzungen

Halten Sie die Service-Tag-Nummer Ihres Dell EMC PowerEdge-Servers bereit. Es wird empfohlen, dass Sie die Service-Tag-Nummer für den Zugriff auf dem gesamten Support auf der Dell Support-Website verwenden. Dadurch wird sichergestellt, dass Sie die entsprechende Version der Software für Ihre Plattform herunterladen.

So laden Sie OMIVV herunter:

Schritte

1. Gehen Sie zu **https://www.dell.com/support**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Geben Sie die Service-Tag-Nummer Ihres Dell EMC PowerEdge-Servers ein und wählen Sie anschließend die Suche aus.
   - Wählen Sie **Alle Produkte durchsuchen** > **Servers** > **PowerEdge** aus.
3. Wählen Sie das entsprechende Modell Ihres PowerEdge-Servers aus.
4. Auf der Support-Seite Ihres Servers wählen Sie **Treiber und Downloads** aus.
5. Aus der Liste **Betriebssystem** wählen Sie die entsprechende Version von VMware ESXi aus.
6. Wählen Sie aus der Liste **KategorieSystemverwaltung** aus.
   Die unterstützte Version von OMIVV wird angezeigt.
7. Klicken Sie auf **Herunterladen** oder aktivieren Sie das Kontrollkästchen, um die Software zu Ihrer Download-Liste hinzuzufügen.

Bereitstellen von OMIVV OVF mit dem vSphere Client (HTML5)

Voraussetzungen

Stellen Sie sicher, dass Sie die Produkt-Zip-Datei (*DellEMC_OpenManage_Integration_<version number>.<build number>.zip*) von **https://www.dell.com/support** heruntergeladen haben.

Schritte

1. Navigieren Sie zu den Speicherorten, von denen Sie OMIVV heruntergeladen haben, und doppelklicken Sie auf **DellEMC_OpenManage_Integration.exe**, um die Datei zu extrahieren.

   Die unterstützte Client-Betriebssystem-Version zum Extrahieren und Ausführen der Exe-Datei ist Windows 7 SP1 und höher.

   Die unterstützte Serverbetriebssystemversion zum Extrahieren und Ausführen der Exe-Datei ist Windows 2008 R2 und höher.

2. Akzeptieren Sie die **Endbenutzer-Lizenzvereinbarung** und speichern Sie die .ovf-Datei.
3. Kopieren oder verschieben Sie die .ovf-Datei an einen Speicherort, auf den der VMware vSphere-Host, auf den Sie die Appliance laden, zugreifen kann.
4. Starten Sie den **VMware vSphere Client (HTML5)**.
5. Wählen Sie im **VMware vSphere Client** einen Host aus und klicken Sie im Hauptmenü auf **Maßnahmen** > **OVF-Vorlage bereitstellen**.

   Sie können auch mit der rechten Maustaste auf den **Host** klicken und **OVF-Vorlage bereitstellen** auswählen.

   Daraufhin wird der **OVF-Vorlagen-Bereitstellungsassistent** angezeigt.
6. Navigieren Sie zum Fenster **Eine OVF-Vorlage auswählen** und führen Sie folgende Schritte durch:
   a. Wählen Sie zum Herunterladen des OVF-Pakets aus dem Internet **URL** aus.
   b. Wenn Sie das OVF-Paket auf Ihrem lokalen System auswählen möchten, dann wählen Sie **Lokale Datei** aus und klicken Sie auf **Dateien auswählen**.
   c. Wählen Sie die Dateien (.mf, .ovf und .vmdk) aus.
   d. Klicken Sie auf **Weiter**.
   Das Fenster **Name und Verzeichnis anzeigen** wird angezeigt.

   ANMERKUNG: Wenn das OVF-Paket auf einer Netzwerkfreigabe gespeichert ist, kann der Installationsprozess zwischen 10 und 30 Minuten dauern. Für eine schnellstmögliche Installation wird empfohlen, die OVF-Datei auf einem lokalen Laufwerk zu hosten.
7. Führen Sie im Fenster **Name und Verzeichnis auswählen** folgende Schritte aus:
   a. Geben Sie im Feld **Name der virtuellen Maschine** den Namen der Vorlage ein. Der Benutzername kann aus bis zu 80 Zeichen bestehen.
   b. Wählen Sie aus der Liste **Speicherort für die virtuelle Maschine auswählen** einen Speicherort aus, um die Vorlage bereitzustellen.
   c. Klicken Sie auf **Weiter**.
   Es wird das Fenster **Compute-Ressourcen auswählen** angezeigt.
8. Wählen Sie aus der Liste **Compute-Ressourcen auswählen** die Zielrechner-Ressource aus und klicken Sie auf **Weiter**.

   Es ist zwingend erforderlich, die Ziel-Rechenressource auszuwählen, um fortzufahren. Die Kompatibilitätsprüfung wird durchgeführt, um zu überprüfen, ob die Ziel-Rechenressource ausgewählt ist oder nicht.

   Das Fenster **Details überprüfen** wird mit den folgenden Informationen angezeigt:
   - **Herausgeber**: die Herausgeberdaten
   - **Download-Größe**: Die Größe der OVF-Vorlage in Gigabytes
   - **Größe auf Festplatte**: Details über breite und schlanke Bereitstellungen
9. Klicken Sie auf **Weiter**.
   Das Fenster **Speicher auswählen** wird angezeigt.
10. Führen Sie im Fenster **Speicher auswählen** die folgenden Schritte aus:
    a. Wählen Sie aus der Dropdown-Liste **Formatieren des virtuellen Laufwerks** eines der folgenden Formate aus:
       - Thick Provision (Lazy Zeroed)
       - Thick Provision (Eager Zeroed)
       - Thin Provision (Schlanke Bereitstellung)

       Es wird empfohlen, dass Sie „Thick Provision (Eager Zeroed)“ auswählen.
    b. Wählen Sie aus der Drop-Down-Liste **VM-Speicher-Richtlinie** eine Richtlinie aus.
    c. Klicken Sie auf **Weiter**.
    Das Fenster **Netzwerke auswählen**, das Einzelheiten über die Quelle und Zielnetzwerke enthält, wird angezeigt.
11. Wählen Sie im Fenster **Netzwerke auswählen** das Zielnetzwerk für jedes Quellnetzwerk aus und klicken Sie auf **Weiter**.

    Zur Verwaltung der Dell EMC-Server in ihrer vSphere-Umgebung benötigt OMIVV Zugriff auf das vSphere-Netzwerk (vCenter und ESXi-Verwaltungsnetzwerk) und das Out-of-band-Netzwerk (iDRAC, CMC und Dell EMC OpenManage Enterprise Modular (OME-Modular)).

    Wenn das vSphere-Netzwerk und das Out-of-band-Netzwerk in Ihrer Umgebung als separates isoliertes Netzwerk verwaltet werden, benötigt OMIVV Zugriff auf beide Netzwerke. In diesem Fall muss die OMIVV-Appliance mit zwei Netzwerkadaptern konfiguriert werden. Wenn Sie über das vSphere-Netzwerk auf das Out-of-band-Netzwerk zugreifen können, konfigurieren Sie keinen Netzwerkadapter für die OMIVV-Appliance. Weitere Informationen zum Konfigurieren von zwei Netzwerkadaptern finden Sie unter Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs).

    - Out-of-band-Netzwerk: Das Verwaltungsnetzwerk, an das iDRAC, CMC und OME-Modular angeschlossen sind.
    - vSphere-Netzwerk: Das Verwaltungsnetzwerk, mit dem ESXi-Hosts, vCenter und PSCs verbunden sind.

12. Überprüfen Sie im Fenster **Für Fertigstellung bereit** die ausgewählten Optionen für die OVF-Bereitstellungsaufgabe und klicken Sie auf **Fertigstellen**.
    Der Bereitstellungsjob wird ausgeführt und zeigt den Status der Fertigstellung an, in dem Sie den Fortschritt der Aufgabe verfolgen können.
13. Schalten Sie die virtuelle Maschine ein.

    ANMERKUNG: Nachdem Sie ein OVF bereitgestellt haben, müssen Sie vor der Registrierung bei OMIVV zwingend das aktuelle Datum und die aktuelle Uhrzeit festlegen.

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.

Bereitstellungsmodus konfigurieren

Info über diese Aufgabe

Stellen Sie für jeden der genannten Bereitstellungsmodi sicher, dass Sie genügend Speicherressourcen für das OMIVV-Gerät zurückstellen, indem Sie Reservierungen verwenden. In der Dokumentation zu vSphere finden Sie die Schritte zum Reservieren von Speicherressourcen.

Stellen Sie sicher, dass die folgenden Systemvoraussetzungen für die erforderlichen Bereitstellungsmodi erfüllt sind, indem Sie diese Ressourcen der virtuellen OMIVV-Maschine zuweisen:

Tabelle 14. Systemanforderungen für Bereitstellungsmodi

Bereitstellungsmodi	Anzahl der Hosts	Anzahl der CPUs	Speicher (GB)	Mindestspeichergröße
Klein	Bis zu 250	2	8	95 GB
Mittel	Bis 500	4	16	95 GB
Groß	Bis zu 1000	8	32	95 GB
Extragroßer Modus	Bis zu 2.000	12	32	95 GB

ANMERKUNG: Die MX-Gehäuse-Firmwareaktualisierungsfunktion wird nur in den Bereitstellungsmodi „Mittel“, „Groß“ und „Extragroß“ unterstützt.

Sie können einen geeigneten Bereitstellungsmodus auswählen, um OMIVV so zu skalieren, dass es der Anzahl der Knoten in Ihrer Umgebung entspricht.

Um das OpenManage Management Pack for vRealize Operations (vROPS) in OMIVV zu integrieren, ist der minimale Bereitstellungsmodus **Medium**.

Schritte

1. Scrollen Sie auf der Seite **GERÄTEMANAGEMENT** hinunter zu **Bereitstellungsmodus**.
   Die Konfigurationswerte des Bereitstellungsmodus wie **Klein**, **Mittel**, **Groß** und **Extragroß** werden angezeigt. Standardmäßig ist dieser Wert auf **Klein** gesetzt.
2. Um einen Bereitstellungsmodus basierend auf einer Umgebung zu bearbeiten, klicken Sie auf **Bearbeiten**.
3. Stellen Sie im **Bearbeiten**-Modus sicher, dass die Voraussetzungen erfüllt sind, und wählen Sie den gewünschten Bereitstellungsmodus aus.
4. Klicken Sie auf **Anwenden**.
   Die zugewiesene CPU und der Speicher werden mit der erforderlichen CPU und dem Speicher für die Einstellung des Bereitstellungsmodus verglichen.
   - Wenn die Überprüfung fehlschlägt, wird eine Fehlermeldung angezeigt.
   - Wenn die Überprüfung erfolgreich ist, wird das OMIVV-Gerät neu gestartet und der Bereitstellungsmodus geändert, nachdem Sie die Änderung bestätigt haben.

- Wenn der erforderliche Bereitstellungsmodus bereits eingestellt ist, wird eine Meldung angezeigt.

5. Wenn der Bereitstellungsmodus geändert wird, müssen Sie die Änderungen bestätigen. Die OMIVV-Appliance wird anschließend neu gestartet, damit der Bereitstellungsmodus aktualisiert wird.

Ergebnisse

ANMERKUNG: Während das OMIVV-Gerät gestartet wird, wird die zugewiesene Systemressource mit dem eingestellten Bereitstellungsmodus verglichen und dahingehend geprüft. Wenn die zugewiesenen Systemressourcen unter dem Bereitstellungsmodus liegen, wird das OMIVV-Gerät nicht bis zur Anzeige der Anmeldeseite gestartet. Zum Starten des OMIVV-Geräts muss es heruntergefahren, die Systemressourcen auf die vorhandene Einstellung des Bereitstellungsmodus aktualisiert und das OMIVV-Gerät wieder eingeschaltet werden.

Bereitstellungsmodus zurückstufen

Schritte

1. Melden Sie sich bei der Administratorkonsole an.
2. Ändern Sie den Bereitstellungsmodus im erforderlichen Maße.
3. Fahren Sie das OMIVV-Gerät herunter und ändern Sie die Systemressourcen im erforderlichen Maße.
4. Schalten Sie das OMIVV-Gerät ein.

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.

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.

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 Betriebsrolle** im OMIVV-Sicherheitskonfigurationsleitfaden.
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.

Schreibgeschützte Benutzerrolle

Es gibt einen Nutzer ohne Rechte mit der Bezeichnung „schreibgeschützt“ mit Shell-Zugriff für Diagnosezwecke. Der Nutzer mit schreibgeschützter Rolle verfügt über eingeschränkte Rechte zum Ausführen einiger Befehle.

Neuen vCenter Server registrieren

Schritte

1. Öffnen Sie die **Verwaltungskonsole** von einem unterstützten Browser aus.

   Um die **Administrationskonsole** zu öffnen, starten Sie einen Webbrowser und geben Sie `https://<ApplianceIP or Appliance hostname or FQDN>` ein.

   Die IP-Adresse ist die IP-Adresse der Appliance-VM und nicht die IP-Adresse des ESXi-Hosts. Sie können über die oben in der Konsole angezeigte URL auf die Verwaltungskonsole zugreifen.
   Beispiel: `Https://10.210.126.120` oder `Https://myesxihost`
   Die URL unterscheidet nicht zwischen Groß- und Kleinschreibung.
2. Geben Sie im Anmeldefenster der **OMIVV-Verwaltungskonsole** das Kennwort ein und klicken Sie dann auf **Anmelden**.

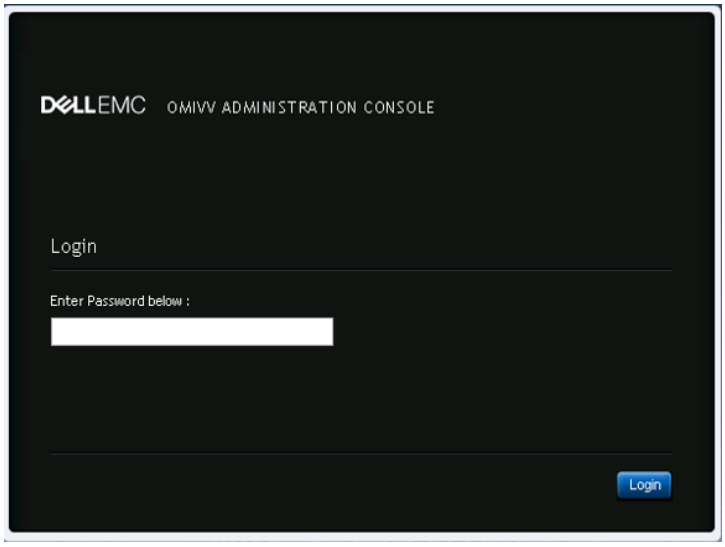


Abbildung 1. Verwaltungskonsole

Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, die EULA zu akzeptieren.

3. Führen Sie auf der Seite **Dell EMC Endnutzer-Lizenzvereinbarung** die folgenden Schritte aus:
   a. Lesen Sie die Bedingungen und Bestimmungen und aktivieren Sie dann das Kontrollkästchen **Ich akzeptiere die Bedingungen in der Lizenzvereinbarung**.
   b. Klicken Sie auf **Akzeptieren**.

   Weitere Informationen zu den Telemetrie-EULA erhalten Sie, indem Sie auf **Dell EMC Telemetrie-EULA** klicken.

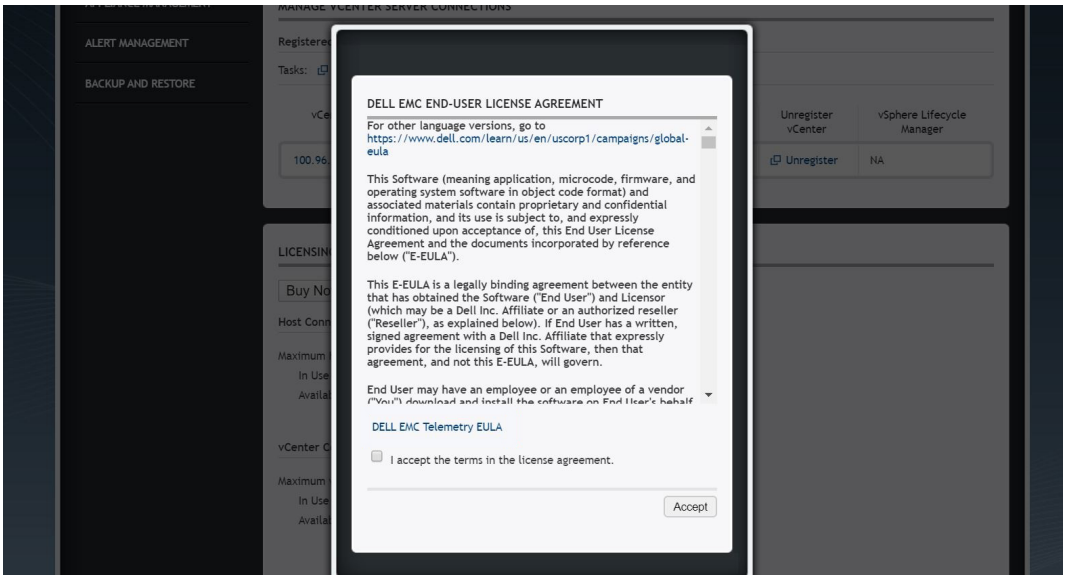


Abbildung 2. Dell EMC Endnutzer-Lizenzvereinbarung

4. Klicken Sie im Fenster **vCenter-Registrierung** auf **Neuen vCenter Server registrieren**.

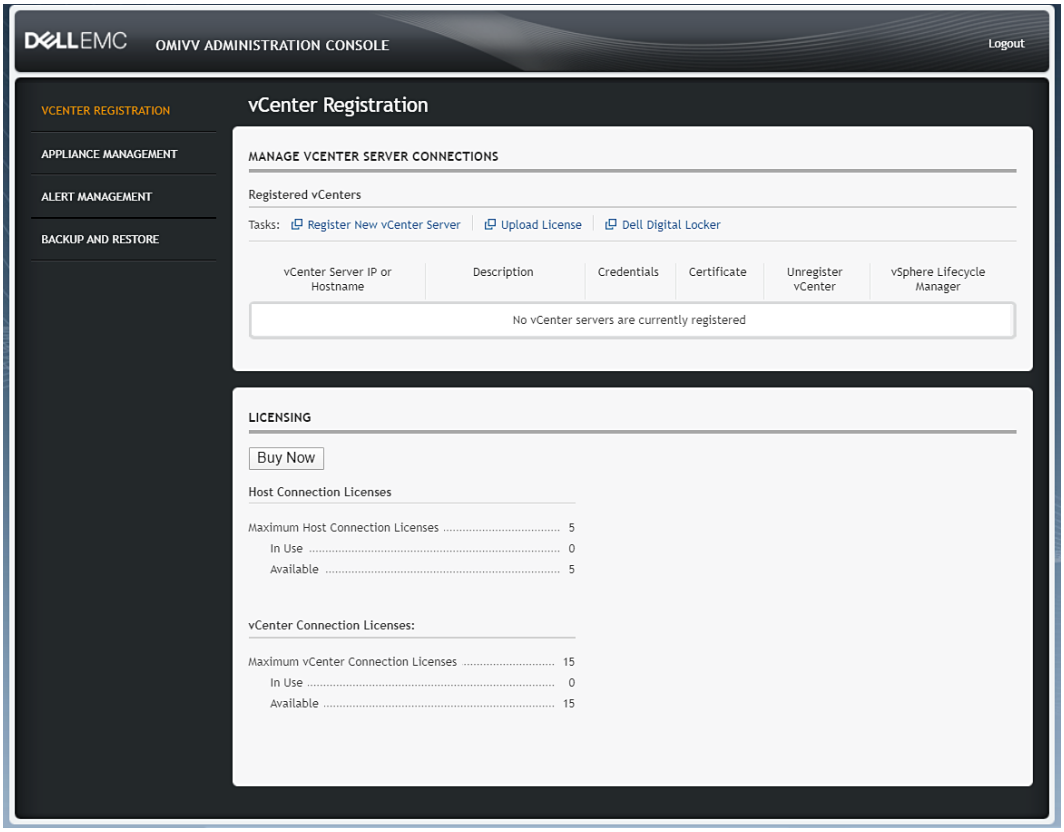


Abbildung 3. vCenter-Registrierung

5. Führen Sie im Fenster **Neuen vCenter Server registrieren** die folgenden Unterschritte aus:
   a. Geben Sie unter **vCenter-Name**im Textfeld **vCenter Server-IP oder -Hostname** die IP-Adresse oder den FQDN des Servers ein.

      ANMERKUNG: Es wird empfohlen, OMIVV beim VMware vCenter unter Verwendung eines FQDN (Fully Qualified Domain Name) zu registrieren. Achten Sie darauf, dass der Hostname des vCenter vom DNS-Server für FQDN-basierte Registrierungen korrekt aufgelöst werden kann.

   b. Geben Sie eine Beschreibung in das Textfeld **Beschreibung** ein. Die Beschreibung ist optional.
   c. Geben Sie im Feld **vCenter Nutzername** unter **vCebter Nutzerkonto** den Nutzernamen des Administrators oder eines Nicht-Administrator-Benutzers mit ausreichenden Berechtigungen an.

      Geben Sie den **Nutzernamen** als `Domäne\Nutzer` oder `Domäne/Nutzer` oder `Nutzer@Domäne` ein. OMIVV verwendet für die Verwaltung von vCenter das Administratorkonto oder ein Nutzerkonto mit den erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Registrieren eines vCenter Servers mit einem Konto ohne Administratorrechte.
   d. Geben Sie das Kennwort in das Feld **Kennwort** ein.
   e. Geben Sie das Kennwort im Feld **Kennwort bestätigen** erneut ein.
   f. Aktivieren Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren (vCenter 7.0 und höher)**. Wenn Sie das Kontrollkästchen **vSphere Lifecycle Manager registrieren** aktivieren, können Sie die vSphere Lifecycle Manager-Funktion ab vCenter 7.0 aufwärts verwenden.

      Sie können den Status von vSphere Lifecycle Manager nach Abschluss der vCenter-Registrierung ändern (registrieren oder deregistrieren). Weitere Informationen finden Sie unter Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole und Aufheben der Registrierung von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole.
6. Klicken Sie auf **Registrieren**.

   Sobald OMIVV registriert ist, wird das OMIVV-Symbol auf der Startseite des vSphere Client (HTML5) angezeigt.

   Informationen zum Überprüfen der Installation finden Sie unter Installation überprüfen.

   ANMERKUNG: OpenManage Integration for VMware vCenter unterstützt derzeit bis zu 2.000 Hosts für den extragroßen Bereitstellungsmodus mit einer einzigen vCenter-Instanz oder mehrere vCenter-Server mithilfe des Linked Mode.
7. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie die OMIVV-Testversion verwenden, können Sie das OMIVV-Symbol anzeigen.
- Bei der Vollversion des Produkts kann die Lizenzdatei vom Dell Digital Locker unter **https://www.dell.com/support**heruntergeladen werden und Sie können diese Lizenz in Ihre virtuelle Appliance importieren. Klicken Sie zum Importieren der Lizenzdatei auf **Lizenz hochladen**. Weitere Informationen zum Hochladen einer Lizenz finden Sie unter Hochladen einer Lizenz auf die OMIVV-Verwaltungskonsole.

Ergebnisse

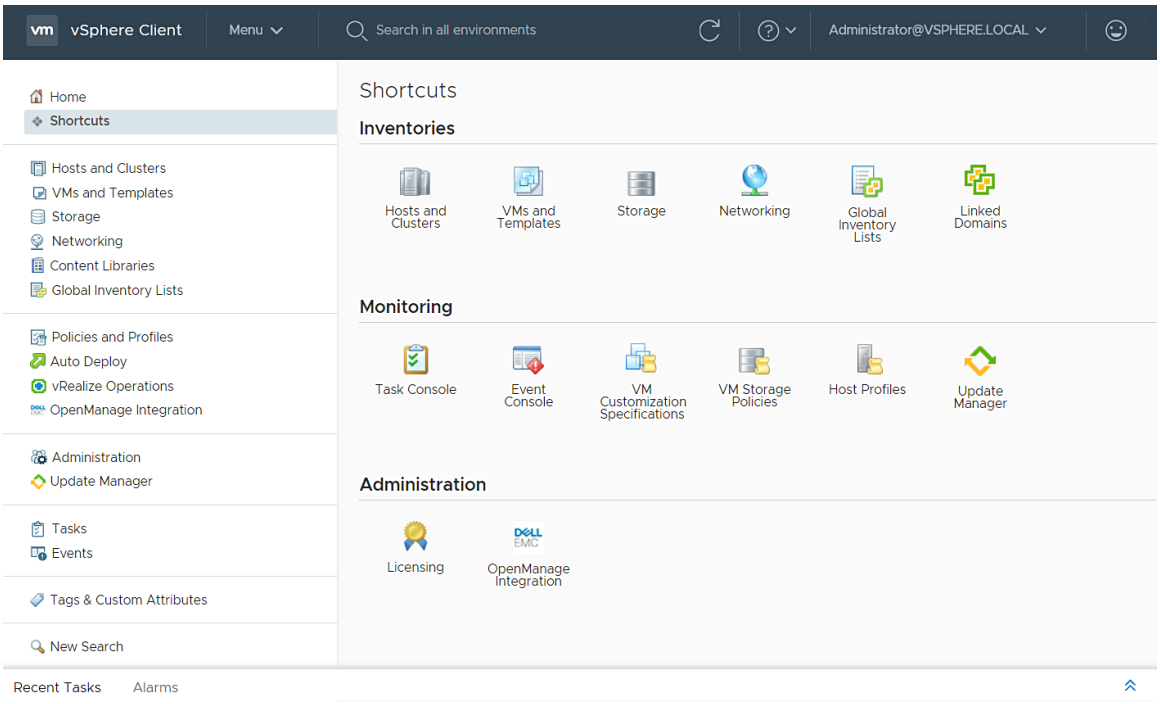


Abbildung 4. OpenManage Integration for VMware vCenter wurde erfolgreich zum vCenter hinzugefügt

Beispiel

Für alle vCenter Operations verwendet OMIVV die Berechtigungen eines registrieren Nutzers und nicht die Berechtigungen eines angemeldeten Nutzers.

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 das Firmwareupdate durchgeführt wird, nutzt OMIVV die Berechtigungen von Nutzer X, damit das Gerät in den Wartungsmodus versetzt werden kann oder der Host erneut gestartet werden kann.

Installation überprüfen

Info über diese Aufgabe

Die folgenden Schritte stellen Sie sicher, dass die OMIVV-Installation erfolgreich war:

Schritte

1. Schließen Sie alle vSphere Client-Fenster und öffnen Sie einen neuen vSphere Client (HTML5).
2. Stellen Sie sicher, dass vCenter mit OMIVV kommunizieren kann, indem Sie einen Ping-Befehl vom vCenter Server zur IP-Adresse oder dem Hostnamen der virtuellen Appliance senden.
3. Erweitern Sie in vSphere Client **Menü** und klicken Sie auf **Administration** > **Lösungen** > **Client Plug-ins**.

   Weitere Informationen über die Zugriffsbeschränkungen für die Seite **Plug-in-Verwaltung** oder **Client-Plug-ins** finden Sie in der VMware Dokumentation.
4. Überprüfen Sie auf der Seite **Client-Plug-ins** die Version und stellen Sie sicher, dass OMIVV installiert und aktiviert ist.

   Wenn OMIVV nicht aktiviert ist, warten Sie einige Zeit ab und melden Sie sich dann bei vCenter ab und wieder an.
5. Um zu bestätigen, dass das OMIVV-Symbol im vSphere Client (HTML5) angezeigt wird, erweitern Sie im vSphere Client **Menü**.

Das Symbol OpenManage Integration wird angezeigt.

Hochladen einer Lizenz auf die OMIVV-Verwaltungskonsole

Voraussetzungen

Stellen Sie sicher, dass Ihre Lizenzen im Dell Digital Locker unter https://www.dell.com/support zum Herunterladen bereit sind. Wenn Sie mehr als eine Lizenz bestellt haben, werden sie möglicherweise separat zu unterschiedlichen Zeitpunkten geliefert. Sie können den Status anderer Lizenzelemente unter „Bestellstatus“ auf https://www.dell.com/support prüfen. Die Lizenzdatei steht im .XML-Format zur Verfügung.

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**.
   Die registrierten vCenter-Server werden im Arbeitsbereich angezeigt.
4. Klicken Sie auf **Lizenz hochladen**.
5. Klicken Sie im Dialogfeld **LIZENZ HOCHLADEN** auf **Durchsuchen**, um zur Lizenzdatei zu navigieren, und klicken Sie auf **Upload**.

   ANMERKUNG: Wenn Sie die Lizenzdatei ändern oder bearbeiten, funktioniert die Lizenzdatei (XML-Datei) nicht. Sie können die XML-Datei (Lizenzschlüssel) über Dell Digital Locker herunterladen. Wenn Sie einen Lizenzschlüssel nicht herunterladen können, wenden Sie sich an den Dell Support. Die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt finden Sie unter „Technischen Support kontaktieren“ auf https://www.dell.com/support.

Registrieren von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole

Voraussetzungen

Die vCenter Version muss 7.0 oder höher sein.

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** unter **vSphere Lifecycle Manager** auf **Registrieren**.
   Das Dialogfeld **VSPHERE LIFECYCLE MANAGER REGISTRIEREN** <vCenter Name> wird angezeigt.
3. Klicken Sie auf **vSphere Lifecycle Manager registrieren**.
   Die Bestätigungsmeldung wird angezeigt, die auf die erfolgreiche Registrierung von vSphere Lifecycle Manager hinweist.

   Informationen zum Verwaltung von Clustern mithilfe von vSphere Lifecycle Manager finden Sie im OMIVV-Benutzerhandbuch unter **https://www.dell.com/support**.

Aufheben der Registrierung von vSphere Lifecycle Manager in der Dell EMC Verwaltungskonsole

Voraussetzungen

Die vCenter Version muss 7.0 oder höher sein.

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Klicken Sie auf der Seite **VCENTER-REGISTRIERUNG** unter **vSphere Lifecycle Manager** auf **Registrierung aufheben**.
   Das Dialogfeld **VSPHERE LIFECYCLE MANAGER-REGISTRIERUNG AUFHEBEN** <vCenter Name> wird angezeigt.
3. Klicken Sie auf **Registrierung aufheben**.

Die Bestätigungsmeldung wird angezeigt, die auf die erfolgreiche Deregistrierung von vSphere Lifecycle Manager hinweist. Die **DellEMC-OMIVV** wird aus der Liste **Hardware Support Manager** im vSphere Lifecycle Manager entfernt. Dies hat keine Auswirkungen auf die OMIVV-Funktionalität.

Informationen zum Verwaltung von Clustern mithilfe von vSphere Lifecycle Manager finden Sie im OMIVV-Benutzerhandbuch unter **https://www.dell.com/support**.

Registrierung von Dell OpenManage Integration for VMware vCenter aufheben

Voraussetzungen

Stellen Sie sicher, dass Sie die Registrierung der OMIVV vom vCenter Server nicht aufheben, wenn ein Job für die Bestandsaufnahme-/Gewährleistung oder ein Bereitstellungsauftrag ausgeführt wird.

Info über diese Aufgabe

Um Dell OpenManage Integration for VMware vCenter zu deinstallieren, müssen Sie die Registrierung von OMIVV auf dem vCenter Server unter Verwendung der Administrationskonsole aufheben.

Schritte

1. Navigieren Sie zu https://<Appliance-IP oder Hostname>.
2. Klicken Sie auf der Seite **VCENTER REGISTRIERUNG** in der Tabelle **vCenter Server IP- oder Hostname** auf **Registrierung aufheben**.

   ANMERKUNG: Achten Sie darauf, das richtige vCenter auszuwählen, da OMIVV mehr als einem vCenter zugeordnet sein kann.

3. Klicken Sie zur Bestätigung der Aufhebung der Registrierung auf den ausgewählten vCenter Server auf das Dialogfeld **VCENTER REGISTRIERUNG AUFHEBEN** und anschließend auf **Registrierung aufheben**.

   ANMERKUNG: Nachdem Sie die Registrierung von OMIVV aufgehoben haben, melden Sie sich am vSphere Client (HTML5) ab und wieder an. Wenn das OMIVV-Symbol weiterhin angezeigt wird, führen Sie die folgenden Schritte aus:

   - Navigieren Sie für VMware vCenter-Server-Appliance zu `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`. Rufen Sie für Windows vCenter die folgenden Ordner in der vCenter-Appliance auf und überprüfen Sie, ob die alten Daten der älteren Version vorhanden sind – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` Ordner in der vCenter-Appliance und überprüfen Sie, ob die alten Daten, wie z. B. com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX vorhanden sind.
   - Löschen Sie den Ordner, der der früheren OMIVV-Version entspricht, manuell und starten Sie die vSphere Client Services für vSphere Client (HTML5) und Webclient (Flex) neu.

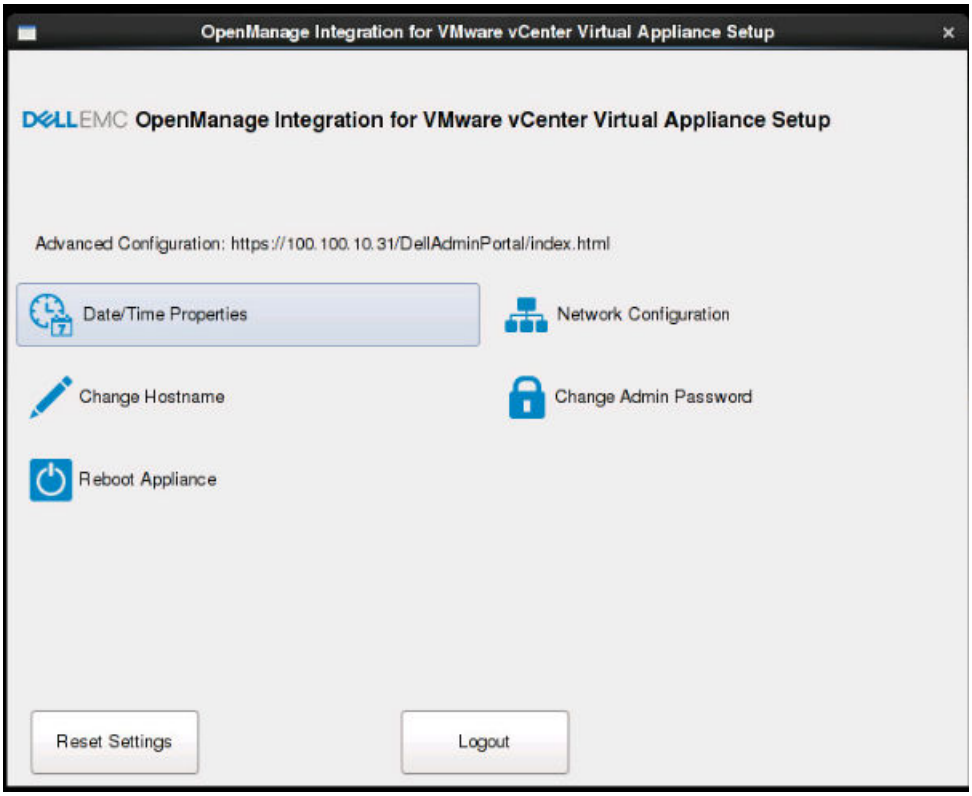
OMIVV-Gerät konfigurieren

Schritte

1. Schalten Sie die virtuelle Maschine ein.
2. Klicken Sie im rechten Fensterbereich auf **Web-Konsole starten**.
3. Melden Sie sich als Administrator an (der Standardnutzername ist `admin`).
4. Wenn Sie sich zum ersten Mal anmelden, befolgen Sie die Anweisungen auf dem Bildschirm, um das Kennwort festzulegen (Admin- und ReadOnly-Nutzer).

   ANMERKUNG: Ein vergessenes Administratorkennwort kann von der OpenManage Integration for VMware vCenter-Appliance nicht wiederhergestellt werden.

5. Zum Konfigurieren der OMIVV-Zeitzoneninformationen klicken Sie auf **Datum/Uhrzeit-Eigenschaften**.



ANMERKUNG: Wenn das OMIVV-Gerät keine IP-Adresse aus dem Netzwerk abrufen kann (DHCP), wird `0.0.0.0` als IP-Adresse angezeigt. Um dies zu beheben, müssen Sie die statische IP manuell konfigurieren.

a. Aktivieren Sie auf der Registerkarte **Datum und Uhrzeit** das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren**. Das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren** ist nur aktiviert, wenn NTP über das Admin-Portal erfolgreich konfiguriert wurde. Weitere Informationen zum Konfigurieren von NTP finden Sie unter Einrichten von NTP-Servern (Network Time Protocol).

b. Klicken Sie auf **Zeitzone**, wählen Sie die entsprechende Zeitzone aus und klicken Sie dann auf **OK**.

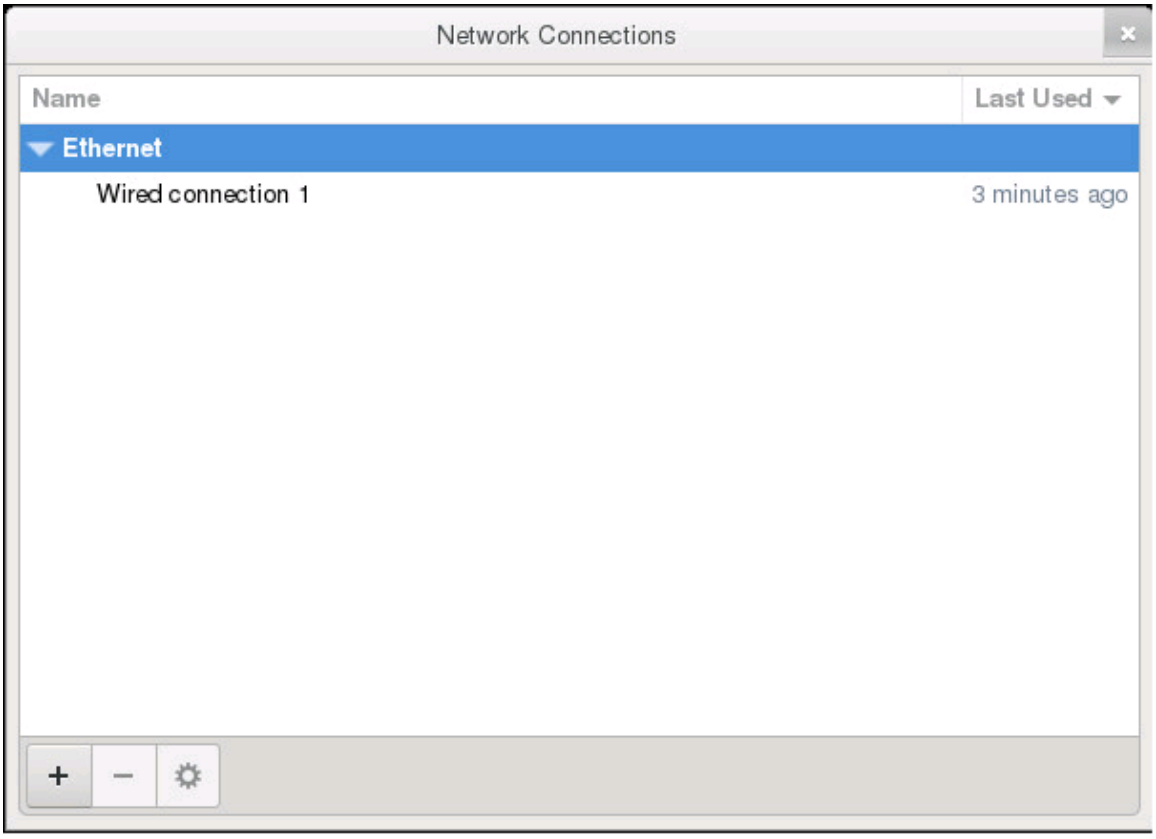
6. Um das Netzwerk des OMIVV-Geräts zu konfigurieren, klicken Sie auf **Netzwerkkonfiguration**.

   Zur Verwaltung der Dell EMC Server in Ihrer vSphere-Umgebung benötigt OMIVV Zugriff auf das vSphere-Netzwerk (vCenter und ESXi-Verwaltungsnetzwerk) und das Out-of-band-Netzwerk (iDRAC, CMC und OME-Modular).

   Wenn das vSphere-Netzwerk und das Out-of-band-Netzwerk in Ihrer Umgebung als separates isoliertes Netzwerk verwaltet werden, benötigt OMIVV Zugriff auf beide Netzwerke. In diesem Fall muss das OMIVV-Gerät mit zwei Netzwerkadaptern konfiguriert werden. Es wird empfohlen, beide Netzwerke im Rahmen der Erstkonfiguration zu konfigurieren.

   Wenn Sie über das vSphere-Netzwerk auf das Out-of-band-Netzwerk zugreifen können, konfigurieren Sie keine zwei Netzwerkadapter für das OMIVV-Gerät. Weitere Informationen zum Konfigurieren einer zweiten Netzwerkkarte finden Sie unter Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs).

7. Wählen Sie **Kabelgebundene Verbindung 1** aus und klicken Sie auf  .



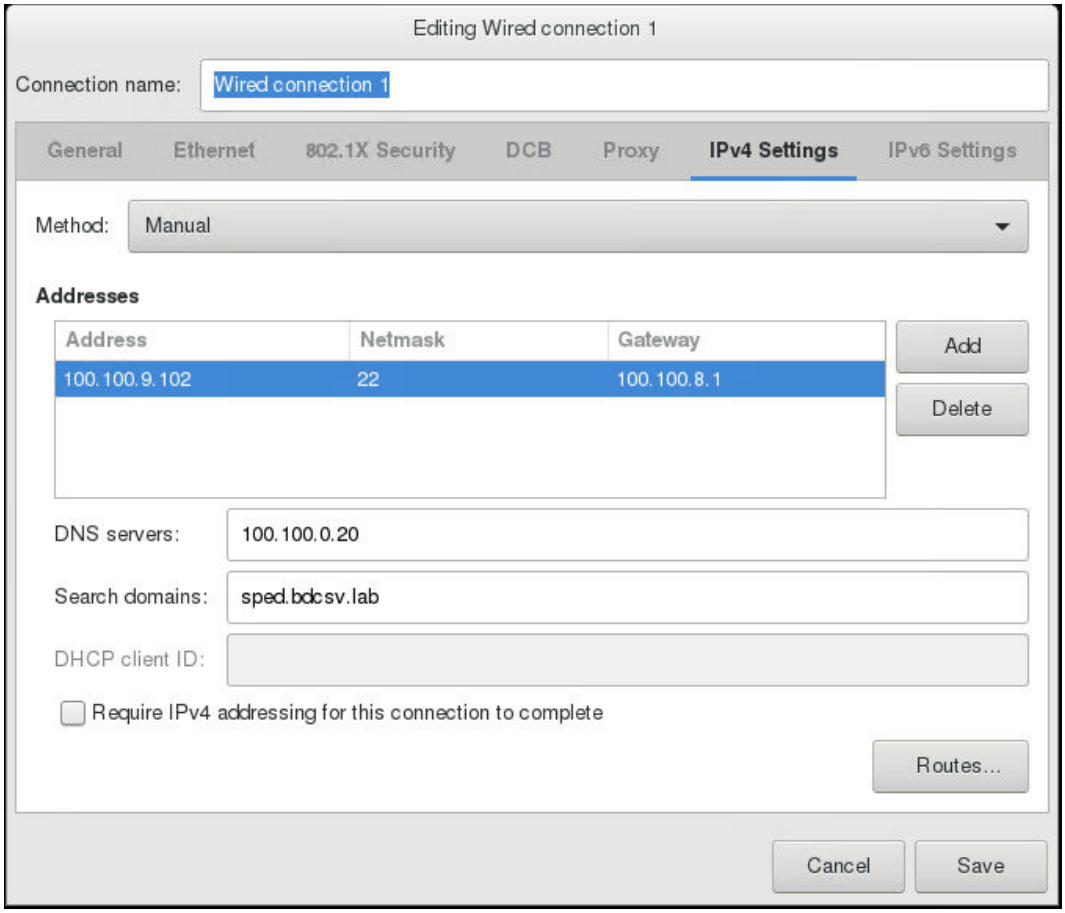
a. Klicken Sie auf die Registerkarte **IPv4-Einstellungen**, wählen Sie **Manuell** aus dem Dropdown-Menü **Methode** und klicken Sie auf **Hinzufügen**.

   ANMERKUNG: Wenn Sie Automatisch (DHCP) wählen, geben Sie keine IP-Adresse ein, da das OMIVV-Gerät die IP-Adresse beim nächsten Neustart automatisch vom DHCP-Server erhält.

b. Geben Sie eine gültige IP-Adresse, eine Netzmaske (im CIDR-Format (Classless Inter-Domain Routing)) und Gateway-Informationen ein.
   Wenn Sie im Feld **Netzmaske** eine IP-Adresse eingeben, wird diese automatisch in das entsprechende CIDR-Format umgewandelt.

c. Geben Sie die DNS-Server-IP und die zu suchenden Domänen jeweils in die Felder **DNS-Server** und **Domänen suchen** ein.

d. Aktivieren Sie das Kontrollkästchen **IPv4-Adressierung zum Abschließen dieser Verbindung erforderlich** und klicken Sie auf **Speichern**.



ANMERKUNG:

Nachdem Sie das OMIVV-Gerät mit einer statischen IP-Adresse konfiguriert haben, wird die OMIVV-Terminal-Hilfsprogramm-Seite manchmal nicht sofort aktualisiert, um die aktualisierte IP anzuzeigen. Um dieses Problem zu beheben, verlassen Sie das OMIVV-Terminal-Dienstprogramm und melden Sie sich erneut an.

8. Klicken Sie zum Ändern des Hostnamens des OMIVV-Geräts auf **Hostnamen ändern**.
   a. Geben Sie einen gültigen Hostnamen ein und klicken Sie auf **Hostnamen aktualisieren**.

   ANMERKUNG: Wenn bei der OMIVV-Appliance bereits vCenter-Server registriert sind, heben Sie die Registrierung auf und registrieren Sie alle vCenter-Instanzen erneut. Weitere Informationen finden Sie Verwalten der Aufhebung der Registrierung und der erneuten Registrierung.

9. Starten Sie das System neu.

Konfigurieren der OMIVV-Appliance mit zwei Netzwerkschnittstellen-Controllern (NICs)

Zur Verwaltung der Dell EMC Server in Ihrer vSphere-Umgebung benötigt OMIVV Zugriff auf das vSphere-Netzwerk (vCenter und ESXi-Verwaltungsnetzwerk) und das Out-of-band-Netzwerk (iDRAC, CMC und OME-Modular). Wenn das vSphere-Netzwerk und das Out-of-band-Netzwerk in Ihrer Umgebung als separates isoliertes Netzwerk verwaltet werden, benötigt OMIVV Zugriff auf beide Netzwerke. In diesem Fall muss die OMIVV-Appliance mit zwei NICs konfiguriert werden. Wenn auf das Out-of-band-Netzwerk über das vSphere-Netzwerk zugegriffen werden kann, sollten Sie keine zwei NICs für die OMIVV-Appliance konfigurieren.

Voraussetzungen

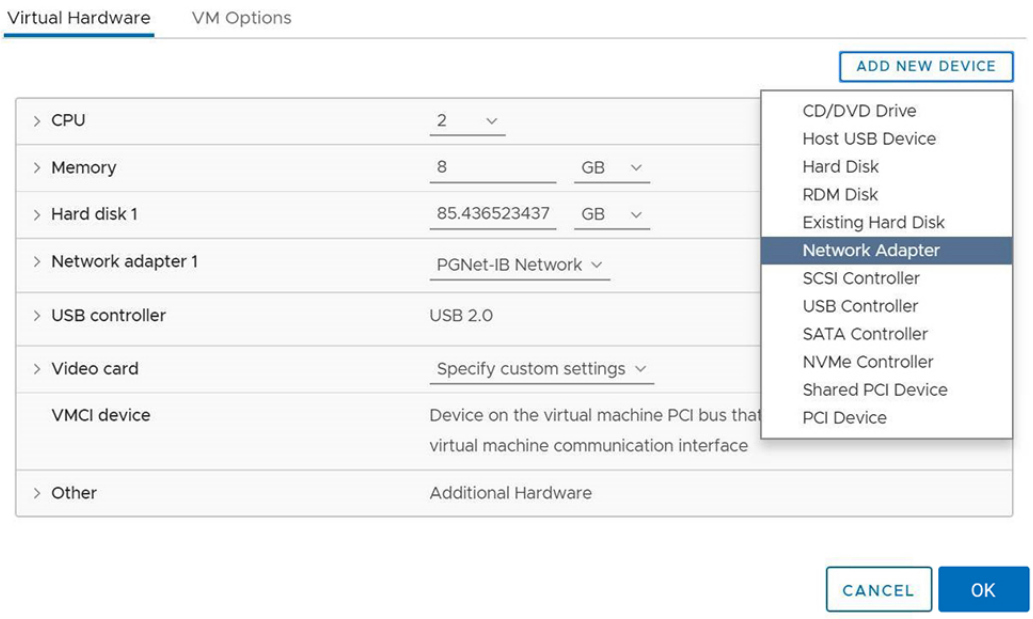
Stellen Sie sicher, dass Sie über die folgenden Informationen sowohl für das Out-of-band-Netzwerk als auch für das vSphere-Netzwerk verfügen:

- IP-Adresse, Netzmaske (im CIDR-Format) und Gateway der Appliance (falls statisch)

- Standard-Gateway: Es ist zwingend erforderlich, das Standard-Gateway nur für ein Netzwerk mit einer Internetverbindung zu konfigurieren. Es wird empfohlen, das vSphere-Netzwerk als Standardgateway zu verwenden.
- Routing-Anforderungen (Netzwerk-IP, Netzmaske und Gateway): Für andere externe Netzwerke, die weder direkt noch über das Standard-Gateway erreichbar sind, konfigurieren Sie die statischen Routen.
- DNS-Anforderungen: OMIVV unterstützt DNS-Konfiguration nur für ein Netzwerk. Weitere Informationen zur DNS-Konfiguration finden Sie unter Schritt 9 (b) in diesem Thema.

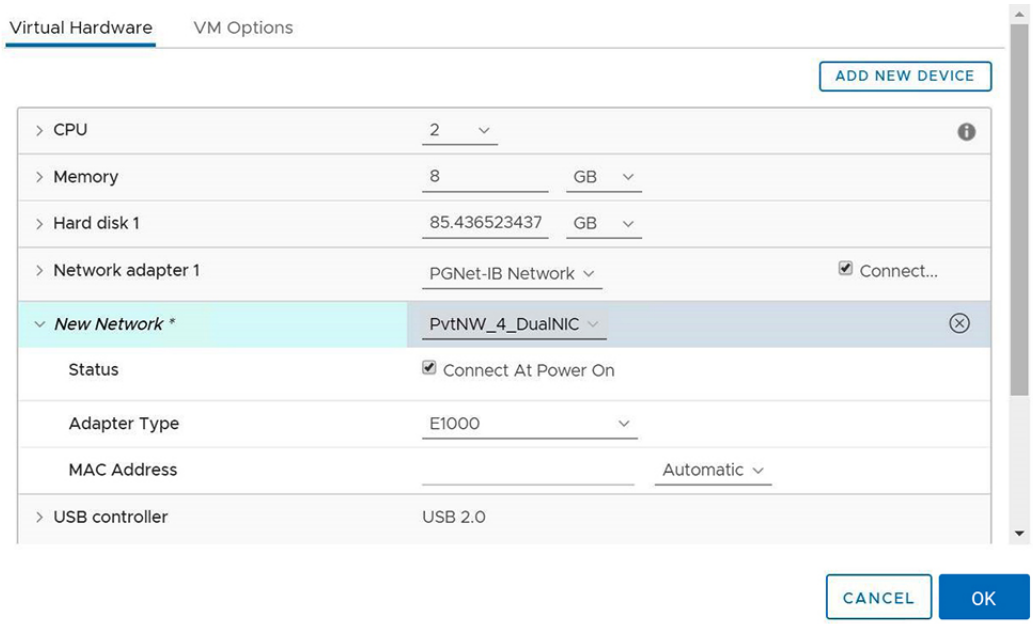
Schritte

1. Schalten Sie die OMIVV-Appliance aus.
2. Bearbeiten Sie die VM-Einstellungen mit dem vSphere Client (HTML5) und fügen Sie den zusätzlichen Netzwerkadapter hinzu. Um die VM-Einstellungen zu bearbeiten, klicken Sie mit der rechten Maustaste auf die VM und klicken Sie dann auf **Einstellungen bearbeiten**.
3. Klicken Sie auf **NEUES GERÄT HINZUFÜGEN** und wählen Sie **Netzwerkadapter** aus.



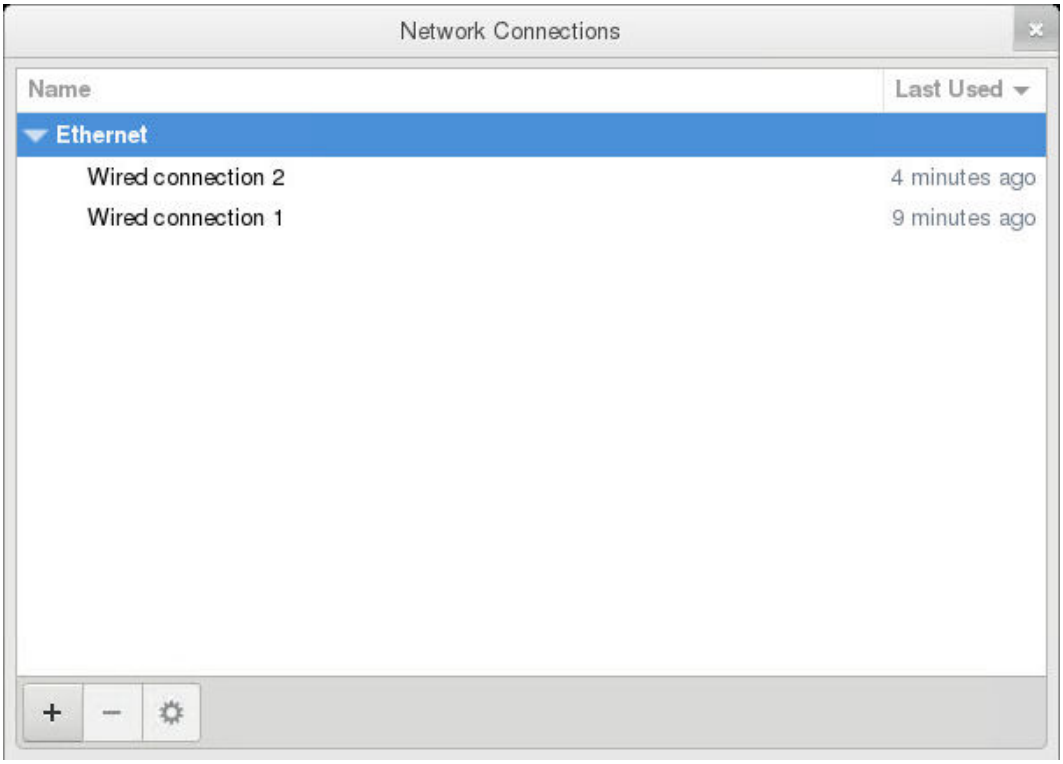
   a. Wählen Sie das entsprechende Netzwerk für den NIC aus und markieren Sie dann das Kontrollkästchen **Beim Einschalten verbinden**.
   b. Wählen Sie im Drop-Down-Menü den **VMXNET3**-Adapter aus.

      ANMERKUNG: OMIVV unterstützt den VMXNET3-NIC-Typ.



4. Schalten Sie das OMIVV-Appliance ein. Melden Sie sich als Administrator an (der Standardnutzername ist Admin) und drücken Sie dann die **Eingabetaste**.
5. Wählen Sie im Hilfsprogramm **OpenManage Integration for VMware vCenter – Einrichtung einer virtuellen Appliance Netzwerkkonfiguration**.

   Auf der Seite **Netzwerkverbindungen** werden zwei NICs angezeigt.

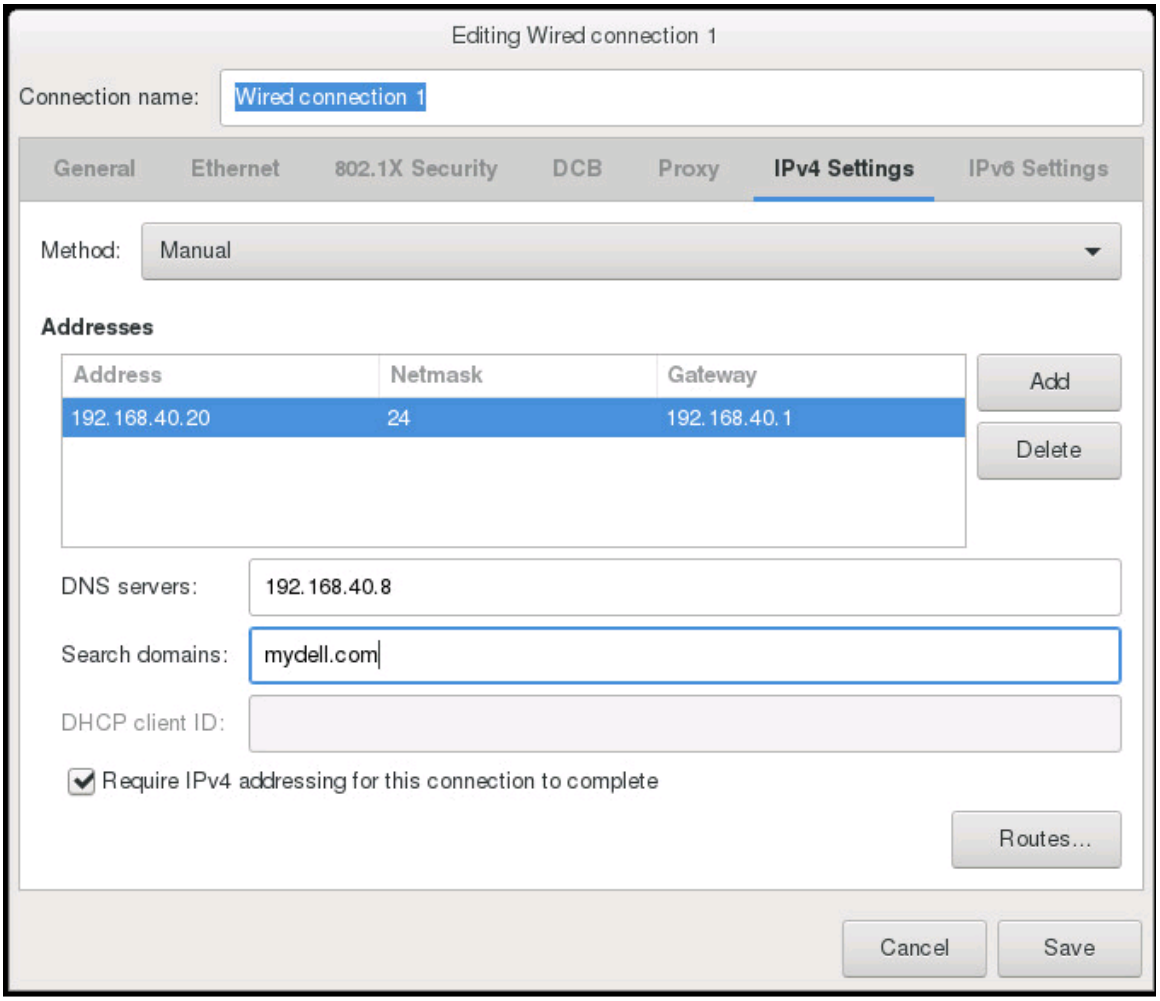


WARNUNG: Verwenden Sie „+“ nicht, um eine neue Netzwerkschnittstelle hinzuzufügen. Um einen NIC hinzuzufügen, muss „Einstellungen bearbeiten“ für vSphere verwendet werden.

6. Wählen Sie die NIC aus, die Sie konfigurieren möchten, und klicken Sie auf  .
7. Um die richtige NIC zu identifizieren, verwenden Sie die auf der Registerkarte **Ethernet** angezeigte MAC-ID und vergleichen Sie sie dann mit der im vSphere Client (HTML5) angezeigten MAC-ID.

Achten Sie darauf, dass Sie die auf der Registerkarte **Ethernet** angegebene Standard-MAC-Adresse nicht ändern.

8. Klicken Sie auf die Registerkarte **Allgemein** und aktivieren Sie das Kontrollkästchen **Automatische Verbindung zu diesem Netzwerk herstellen, wenn es verfügbar ist**.
9. Klicken Sie auf die Registerkarte **IPv4-Einstellungen** und gehen Sie wie folgt vor:



a. Wählen Sie **Manuell** oder **Automatisch (DHCP)** aus der Dropdown-Liste **Methode**.
b. Wenn Sie die Methode **Manuell** auswählen, klicken Sie auf **Hinzufügen** und geben Sie dann die gültige IP-Adresse, Netzmaske (im CIDR-Format) und Gateway-Details ein. Es wird empfohlen, die statische IP-Adresse für den Fall zu verwenden, dass Sie die Priorität der DNS-Server (primäre und sekundäre DNS-Einträge) steuern möchten.

   Typischerweise werden die vSphere-Elemente eines Rechenzentrums, wie vCenter- und ESXi-Hosts, über den Hostnamen oder FQDN verwaltet. iDRAC, CMC und OME-Modular werden über IP-Adressen verwaltet. In diesem Fall wird empfohlen, die DNS-Einstellungen nur für das vSphere-Netzwerk zu konfigurieren.

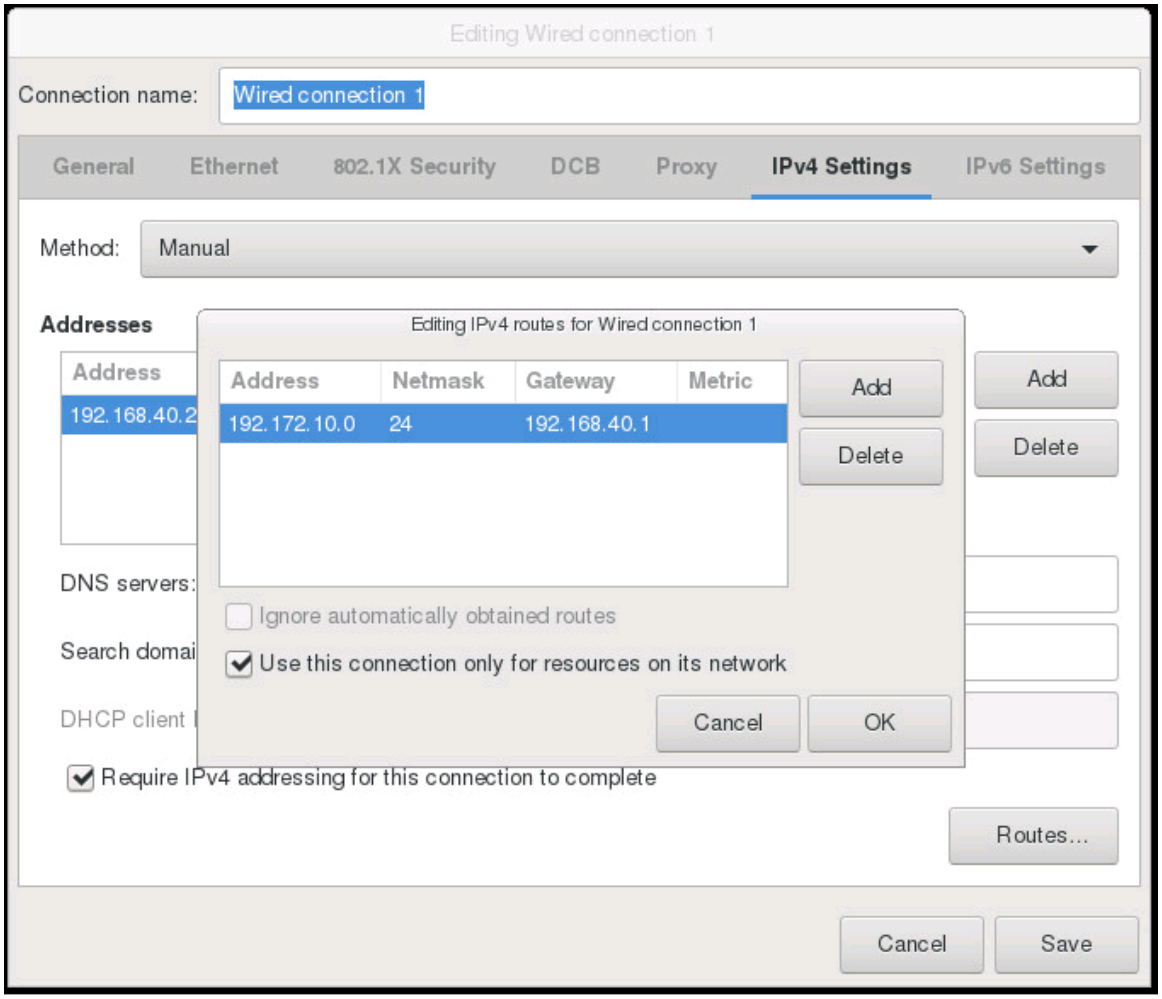
   Wenn sowohl das vSphere-Netzwerk als auch das iDRAC-Verwaltungsnetzwerk über den Hostnamen oder FQDN verwaltet werden, muss der DNS-Server so konfiguriert werden, dass er den Hostnamen oder FQDN für beide Netzwerke auflöst. Weitere Informationen finden Sie in der CentOS-Dokumentation.

   ANMERKUNG: Der zuletzt konfigurierte DNS-Server wird zum primären DNS, unabhängig davon, für welches Netzwerk der DNS konfiguriert ist.

c. Geben Sie die DNS-Server-IP und die zu suchenden Domänen in die Felder **DNS-Server** und **Domänen suchen** ein.
d. Aktivieren Sie das Kontrollkästchen **IPv4-Adressierung zum Abschließen dieser Verbindung erforderlich** und klicken Sie auf **SPEICHERN**.
e. Wenn Sie dieses Netzwerk nicht als Standardnetzwerk (Gateway) verwenden möchten, klicken Sie auf **Routen**, und aktivieren Sie dann das Kontrollkästchen **Diese Verbindung nur für Ressourcen in ihrem Netzwerk verwenden**.

   ANMERKUNG: Das Hinzufügen mehrerer Netzwerke als Standardgateways kann zu Netzwerkproblemen führen, sodass OMIVV-Funktionen beeinträchtigt sind.

f. Wenn Sie über die bekannten Gateways zu einem externen Netzwerk gelangen möchten, klicken Sie auf der gleichen Seite auf **Hinzufügen** und fügen Sie dann die Netzwerk-IP-Adresse, die Netzmaske (im CIDR-Format) und die Gateway-Details hinzu.



In der Regel erfordert das Netzwerk, das Sie als Standard-Gateway konfiguriert haben, keine manuelle Routingkonfiguration, da das Gateway die Erreichbarkeit gewährleisten kann. Bei Netzwerken, für die das Standard-Gateway nicht konfiguriert ist (für die das Kontrollkästchen **Diese Verbindung nur für Ressourcen in ihrem Netzwerk verwenden** aktiviert wurde), kann jedoch eine manuelle Routingkonfiguration erforderlich sein. Da das Standard-Gateway nicht so konfiguriert ist, dass dieses Netzwerk externe Netzwerke erreicht, sind manuelle Routingkonfigurationen erforderlich.

ANMERKUNG: Eine falsche Routingonfiguration kann dazu führen, dass die Netzwerkschnittstelle unvermittelt nicht mehr reagiert. Achten Sie darauf, die Routing-Einträge entsprechend zu konfigurieren.

g. Klicken Sie auf **OK**.

10. Klicken Sie auf **Speichern**. Zum Konfigurieren einer anderen NIC wiederholen Sie die Schritte 6–10.
11. Navigieren Sie zu **OpenManage Integration for VMware vCenter – Einrichtung einer virtuellen Appliance** und klicken Sie auf **Appliance neu starten**. Die Netzwerkkonfiguration ist erst nach einem Neustart der OMIVV-Appliance abgeschlossen.

    Nachdem die Appliance erfolgreich neu gestartet wurde, funktionieren die NICs gemäß der Konfiguration. Der Status von NICs kann eingesehen werden, indem Sie sich als **schreibgeschützter** Nutzer anmelden und die folgenden Befehle ausführen: `ifconfig`, `ping` und `route -n`.

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**.

Konfigurieren des Network Time Protocol (NTP) und Einstellen der lokalen Zeitzone

Schritte

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Datum/Uhrzeit-Eigenschaften**.

   Geben Sie die NTP-Details in die Admin-Konsole ein. Weitere Informationen finden Sie unter Einrichten von NTP-Servern (Network Time Protocol).
3. Wählen Sie auf der Registerkarte **Datum und Uhrzeit Datum und Uhrzeit über das Netzwerk synchronisieren**.
   Das **NTP-Server**-Feld wird angezeigt.
4. Zum Hinzufügen einer weiteren NTP-Server-IP oder eines Hostnamens klicken Sie auf die Schaltfläche **Hinzufügen**, und drücken Sie die **Tabulatortaste**.
5. Klicken Sie auf **Zeitzone**, und wählen Sie dann die entsprechende Zeitzone aus. Klicken Sie dann Sie auf **OK**.

   Der Kommunikationsfehler tritt auf, wenn die Zeitzonen von vCenter und OMIVV voneinander abweichen. Legen Sie die gleiche Zeitzone zwischen OMIVV und vCenter fest.

Einrichten von NTP-Servern (Network Time Protocol)

Info über diese Aufgabe

Sie können das NTP zum Synchronisieren der Uhren der OMIVV-Geräte mit der Uhr eines NTP-Servers verwenden.

Schritte

1. Klicken Sie in der Verwaltungskonsole auf der Seite **GERÄTE-MANAGEMENT** auf **Bearbeiten** im Bereich **NTP-Einstellungen**.
2. Wählen Sie **Aktiviert** aus. Geben Sie den Hostnamen oder die IP-Adresse eines bevorzugten und eines sekundären NTP-Server ein und klicken Sie auf **Anwenden**.
3. Nachdem Sie NTP konfiguriert haben, starten Sie die Terminalkonsole und aktivieren Sie das Kontrollkästchen **Datum und Uhrzeit über das Netzwerk synchronisieren**.

   Der Kommunikationsfehler tritt auf, wenn die Zeitzonen von vCenter und OMIVV voneinander abweichen. Legen Sie die gleiche Zeitzone zwischen OMIVV und vCenter fest.

Ergebnisse

Es kann etwa 10 Minuten dauern, bis die OMIVV-Uhr mit dem NTP-Server synchronisiert ist.

ANMERKUNG: Wenn die OMIVV-Verwaltungskonsole eine lange Zeit in Anspruch nimmt, um Informationen zu laden, stellen Sie sicher, dass die NTP-Einstellungen korrekt sind und der NTP-Server über die virtuelle OMIVV-Maschine erreichbar ist.

Hostnamen des OMIVV-Geräts ändern

Schritte

1. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Hostname ändern**.

ANMERKUNG: Wenn irgendwelche vCenter-Server beim OMIVV-Gerät registriert sind, heben Sie die Registrierung auf und registrieren Sie alle vCenter-Instanzen erneut.

2. Geben Sie einen aktualisierten Hostnamen ein.
   Geben Sie den Domänennamen im folgendem Format an: *<Hostname>*.
3. Klicken Sie auf **Hostnamen aktualisieren**.
   Der Hostname des Geräts wird aktualisiert und die Hauptmenü-Seite wird angezeigt.
4. Um das Gerät neu zu starten, klicken Sie auf **Neustart des Geräts**.

Ergebnisse

ANMERKUNG: Stellen Sie sicher, dass Sie alle Referenzen auf das virtuelle Gerät in Ihrer Umgebung manuell aktualisieren, wie z. B. Bereitstellungsserver in iDRAC und Dell EMC Repository Manager (DRM).

Neustart des OMIVV-Geräts durchführen

Schritte

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Gerät neu starten**.
3. Um das Gerät neu zu starten, klicken Sie auf **Ja**.

OMIVV-Appliance auf werkseitige Einstellungen zurücksetzen

Schritte

1. Öffnen Sie die OMIVV-Webkonsole.
2. Klicken Sie im Dienstprogramm **OpenManage Integration for VMware vCenter – Einrichtung eines virtuellen Geräts** auf **Einstellungen zurücksetzen**.
   Die folgende Meldung wird angezeigt:

   ```
   All the settings in the appliance will be Reset to Factory Defaults and the appliance will be rebooted. Do you still wish to continue?
   ```

3. Um das Gerät zurückzusetzen, klicken Sie auf **Ja**.
   Wenn Sie auf **Ja** klicken, wird das OMIVV-Gerät auf die Werkseinstellungen zurückgesetzt und alle anderen Einstellungen und vorhandenen Daten werden gelöscht.

   Nachdem die Zurücksetzung auf die Werkseinstellungen abgeschlossen ist, registrieren Sie die vCenters erneut bei dem OMIVV-Gerät.

Ergebnisse

ANMERKUNG: Wenn das OMIVV-Gerät auf die Werkseinstellungen zurückgesetzt wird, werden alle Aktualisierungen an der Netzwerkkonfiguration beibehalten. Diese Einstellungen werden nicht zurückgesetzt.

Neukonfigurieren von OMIVV nach dem Upgrade der registrierten vCenter-Version

Info über diese Aufgabe

Nach einer Aktualisierung eines registrierten vCenters führen Sie die folgenden Aufgaben aus:

- Für Nicht-Administratornutzer
  1. Weisen Sie Nicht-Administratornutzern bei Bedarf zusätzliche Berechtigungen zu. Informationen dazu finden Sie unter Erforderliche Berechtigungen für Nicht-Administratornutzer.

     Weisen Sie die zusätzlichen Berechtigungen zum Beispiel zu, wenn Sie eine Aktualisierung von vCenter 6.0 auf vCenter 6.5 durchführen.

2. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
3. Wenn es sich beim registrierten vCenter um Version 7.0 oder höher handelt, aktivieren Sie vSphere Lifecycle Manager in der OMIVV-Verwaltungskonsole.

- Für Administratornutzer:
  1. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
  2. Wenn es sich beim registrierten vCenter um Version 7.0 oder höher handelt, aktivieren Sie die vSphere Lifecycle Manager OMIVV-Administrationskonsole.

Wiederherstellen von OMIVV nach der Aufhebung der Registrierung

OMIVV wiederherstellen, nachdem die Registrierung einer früheren Version von OMIVV aufgehoben wurde

Info über diese Aufgabe

Sollten Sie die Registrierung des OMIVV-Plugins nach einem Backup einer früheren Datenbankversion aufgehoben haben, führen Sie die folgenden Schritte durch, bevor Sie mit der Migration fortfahren:

ANMERKUNG: Durch das Aufheben der Registrierung des Plug-ins werden alle Anpassungen, die auf den registrierten Alarmen implementiert wurden, und Funktionszustandsaktualisierungen von Dell für PHA-Cluster entfernt. Die folgenden Schritte stellen die benutzerdefinierten Einstellungen nicht wieder her. Sie registrieren aber erneut die Alarme mit ihren Standardeinstellungen.

ANMERKUNG: Es wird empfohlen, die Identität (IP oder FQDN) der älteren OMIVV-Appliance für die neue OMIVV-Appliance beizubehalten.

ANMERKUNG: Wenn die IP-Adresse für die neue Appliance sich von der IP-Adresse der älteren Appliance unterscheidet, kann die Funktion „Proaktive HA“ möglicherweise nicht ordnungsgemäß ausgeführt werden. Deaktivieren und aktivieren Sie in einem solchen Fall die PHA für alle Cluster, in denen der Dell Host vorhanden ist.

Schritte

Führen Sie die Aufgaben 3 bis 9 aus, die unter OMIVV-Appliance durch Sichern und Wiederherstellen aktualisieren aufgeführt sind.

Verwalten der Aufhebung der Registrierung und der erneuten Registrierung

Voraussetzungen

Es wird empfohlen, vor dem Aufheben der Registrierung ein Backup durchzuführen.

Info über diese Aufgabe

ANMERKUNG: Durch das Aufheben der Registrierung des Plug-ins werden alle Anpassungen, die auf den registrierten Alarmen implementiert wurden, und Funktionszustandsaktualisierungen von Dell für PHA-Cluster entfernt. Die folgenden Schritte stellen die benutzerdefinierten Einstellungen nicht wieder her. Sie registrieren aber erneut die Alarme mit ihren Standardeinstellungen.

Schritte

1. Erstellen Sie ein Backup von OMIVV.
2. Heben Sie die Registrierung für vCenter in OMIVV auf.
3. Führen Sie alle geplanten Konfigurationsänderungen aus. Beispiel: Änderungen am Hostnamen oder neue Konfigurationen.
4. Starten Sie die OMIVV-Appliance neu,
5. Stellen Sie die Backupdatei wieder her. Weitere Informationen finden Sie unter OMIVV-Appliance durch Sichern und Wiederherstellen aktualisieren.

3

OMIVV-Appliance und Repository-Speicherort aktualisieren

Voraussetzungen

- Um sicherzustellen, dass alle Daten geschützt sind, führen Sie vor dem Aktualisieren der OMIVVAppliance eine Sicherung der OMIVV-Datenbank aus. Informationen dazu finden Sie unter Backups und Wiederherstellungen verwalten.
- Die OMIVV-Appliance benötigt eine Internetverbindung, um verfügbare Aktualisierungsmechanismen anzuzeigen und die RPM-Aktualisierung durchzuführen. Stellen Sie sicher, dass die OMIVV-Appliance über eine Internetverbindung verfügt. Wenn Sie ein Proxy-Netzwerk auf Basis der Netzwerk-Umgebungseinstellungen benötigen, aktivieren Sie die Proxy-Einstellungen und geben Sie die Proxydaten ein. Siehe das Thema im Benutzerhandbuch – Einrichten des HTTP-Proxy.
- Stellen Sie sicher, dass **Repository-Pfad aktualisieren** gültig ist.
- Stellen Sie sicher, dass Sie sich von allen vSphere Client (HTML5)-Sitzungen an den registrierten vCenter-Servern abmelden.
- Stellen Sie vor der Anmeldung an einem registrierten vCenter Server sicher, dass Sie alle Geräte gleichzeitig unter der gleichen vCenter Linked Mode-Umgebung aktualisieren. Andernfalls werden möglicherweise inkonsistente Informationen in den OMIVV-Instanzen angezeigt.

Schritte

1. Im Abschnitt **GERÄTEAKTUALISIERUNG** der Seite **GERÄTEVERWALTUNG** überprüfen Sie die aktuelle und verfügbare OMIVV-Version.

   Für die verfügbare Version des OMIVV-Appliance werden die entsprechenden RPM- und OMIVV-Aktualisierungsmechanismen mit einem Häkchen angezeigt [✔].

   Im Folgenden werden die verfügbaren Optionen des Aktualisierungsmechanismus dargestellt. Sie können eine dieser Optionen für den Aktualisierungsmechanismus durchführen:

Option	Beschreibung
1	Wenn ein Häkchen neben RPM angezeigt wird, können Sie eine RPM-Aktualisierung von der vorhandenen Version auf die neueste verfügbare Version durchführen. Informationen dazu finden Sie unter OMIVV-Appliance über RPM aktualisieren (mit Internet).
2	Wenn ein Häkchen neben OVF angezeigt wird, können Sie eine Sicherungskopie der OMIVV-Datenbank von der vorhandenen Version erstellen und die Wiederherstellung in der neuesten verfügbaren Applianceversion ausführen. Informationen dazu finden Sie unter OMIVV-Appliance durch Sichern und Wiederherstellen aktualisieren.
3	Wenn ein Häkchen neben RPM und OVF angezeigt wird, können Sie eine der genannten Optionen zur Aktualisierung Ihrer Appliance ausführen. In diesem Szenario ist die empfohlene Option die RPM-Aktualisierung.

2. Zur Aktualisierung der OMIVV-Appliance führen Sie die genannten Aufgaben für die Upgrade-Mechanismen durch, je nach Version von OMIVV.

Themen:

- OMIVV-Appliance über RPM aktualisieren (mit Internet)
- OMIVV-Appliance über RPM aktualisieren (per Intranet)
- Backups und Wiederherstellungen verwalten

OMIVV-Appliance über RPM aktualisieren (mit Internet)

Voraussetzungen

Stellen Sie sicher, dass Sie ein Upgrade auf eine Version des Geräts durchführen, die größer als die aktuelle ist.

Es wird empfohlen, einen Snapshot der Appliance zu erstellen, bevor Sie das Upgrade der OMIVV-Appliance durchführen.

Schritte

1. Aktivieren Sie auf der Seite **GERÄTEMANAGEMENT** die Option „Proxy“ entsprechend Ihren Netzwerkeinstellungen und rufen Sie bei Bedarf die Proxy-Einstellungen auf. Siehe das Thema .

   Für die verfügbare Version des OMIVV-Geräts werden die entsprechenden RPM- und OMIVV-Aktualisierungsmechanismen mit einem Häkchen angezeigt [✔].

2. Zum Aktualisieren des OMIVV-Plug-ins von einer vorhandenen Version auf die verfügbare Version führen Sie einen der folgenden Schritte durch:
   - Für die Aktualisierung unter Verwendung von RPM, das unter **Repository-Pfad aktualisieren** verfügbar ist, stellen Sie sicher, dass **Repository-Pfad aktualisieren** auf folgenden Pfad eingestellt ist: https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/

   Klicken Sie andernfalls im Fenster **Gerätemanagement** im Bereich **Geräteaktualisierung** auf **Bearbeiten**, um den Pfad im Textfeld **Aktualisierungs-Repository-Pfad** in https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ zu ändern, und klicken Sie auf **Übernehmen**.

3. Vergleichen Sie die verfügbare OMIVV-Geräteversion und die aktuelle OMIVV-Geräteversion.
4. Klicken Sie unter **Geräteeinstellungen** auf **Virtuelles Gerät aktualisieren**, um die Aktualisierung des OMIVV-Geräts zu übernehmen.
5. Klicken Sie im Dialogfeld **GERÄTEAKTUALISIERUNG** auf **Aktualisieren**.
   Nachdem Sie auf **Aktualisieren** geklickt haben, werden Sie vom Fenster der **VERWALTUNGSKONSOLE** abgemeldet.
6. Schließen Sie den Internet-Browser.

   Während des Upgrade-Vorgangs wird das Gerät ein- oder zweimal neu gestartet. Nachdem der Geräte-RPM aktualisiert wurde, stellen Sie sicher, dass Sie den Browser-Cache leeren, bevor Sie sich beim Dell Administratorportal anmelden.

   Nach Abschluss der RPM-Aktualisierung wird der Anmeldebildschirm in der OMIVV Konsole angezeigt. Öffnen Sie einen Browser, geben Sie den Link*https:\\<ApplianceIP|Hostname>* ein und navigieren Sie zum Bereich **GERÄTEAKTUALISIERUNG**. Prüfen Sie, ob die Versionen der verfügbaren und aktuellen OMIVV-Geräte gleich sind.

   Alle Anpassungen, die auf den eingetragenen Dell Alarmen und dem Dell Funktionszustand-Update-Anbieter für PHA-Cluster durchgeführt werden, werden nach dem RPM-Upgrade auf die Standardeinstellung zurückgesetzt.

OMIVV-Appliance über RPM aktualisieren (per Intranet)

Voraussetzungen

Erstellen Sie eine HTTP-, HTTPS- oder NFS-Freigabe.

Stellen Sie sicher, dass die HTTP- oder HTTPS-Freigabe Dateinamen unterstützt, die Sonderzeichen wie ++ oder Leerzeichen enthalten.

OMIVV unterstützt:

- HTTP-Freigabe in Version 5.0 und höher
- HTTPS-Freigaben in Version 5.1 und höher
- NFS-Freigaben in Version 5.2 und höher

Schritte

1. Laden Sie das Paket RPM.zip herunter, das Sie unter https://www.dell.com/support finden.
2. Entpacken Sie RPM.zip und kopieren Sie die Dateien und Ordner vom Entpackungsort auf die HTTP- bzw. HTTPS-Freigabe.

3. Klicken Sie auf der Seite **APPLIANCEVERWALTUNG** im Bereich **APPLIANCEAKTUALISIERUNG** auf **Bearbeiten** und geben Sie den Pfad der Freigabe unter **Repository-Pfad aktualisieren** ein.

   Das Format des Update-Repository-Pfads für HTTP ist `http://<IP or hostname>/<path to RepoConfig.xml>`.

   Das Format des Update-Repository-Pfads für HTTPS ist `https://<IP or hostname>/<path to RepoConfig.xml>`.

   Das Format des Update-Repository-Pfads für NFS ist `<IP or hostname>:/<path to RepoConfig.xml>`.

4. Klicken Sie auf **Anwenden**.
5. Vergleichen Sie die verfügbare OMIVV-Applianceversion und die aktuelle OMIVV-Applianceversion.
6. Klicken Sie unter **Applianceeinstellungen** auf **Virtuelle Appliance aktualisieren**, um die Aktualisierung der OMIVV-Appliance zu übernehmen.
7. Klicken Sie im Dialogfeld **APPLIANCEAKTUALISIERUNG** auf **Aktualisieren**.
   Nachdem Sie auf **Aktualisieren** geklickt haben, werden Sie vom Fenster der **OMIV VERWALTUNGSKONSOLE** abgemeldet.

   Es kann je nach Netzwerkgeschwindigkeit in etwa 40 Minuten dauern, bis die Aktualisierung abgeschlossen ist.
8. Schließen Sie den Webbrowser.
   Nachdem die Applianceaktualisierung abgeschlossen ist, stellen Sie sicher, dass Sie den Browser-Cache leeren, bevor Sie sich bei der **OMIV VERWALTUNGSKONSOLE** anmelden.

Backups und Wiederherstellungen verwalten

Info über diese Aufgabe

Mit der Verwaltungskonsole können Sie Sicherungs- und Wiederherstellungsaufgaben durchführen.

- Backup und Wiederherstellung konfigurieren
- Automatische Backups planen
- Sofortiges Backup durchführen
- Datenbank aus einem Backup wiederherstellen
- Sicherungs- und Wiederherstellungseinstellungen zurücksetzen

Führen Sie folgende Schritte in OMIVV durch, um die Seite **EINSTELLUNGEN ZU BACKUP UND ZUR WIEDERHERSTELLUNG** über die Verwaltungskonsole aufzurufen:

Schritte

1. Navigieren Sie zu `https:\\<ApplianceIP|hostname>`.
2. Geben Sie im **Anmelde**-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.

Backup und Wiederherstellung konfigurieren

Die Backup- und Wiederherstellungsfunktion dient zum Sichern der OMIVV-Datenbank an einem Remote-Speicherort (NFS und CIFS), von dem aus sie später wiederhergestellt werden kann. Die Profile, Konfiguration und Host-Informationen sind im Backup enthalten. Wir empfehlen, das Sie zum Schutz gegen Datenverlust automatische Backups planen.

Info über diese Aufgabe

Die folgenden Einstellungen werden nicht gespeichert und wiederhergestellt:

- Profile
- Bestandsaufnahmedetails für den Host
- OMIVV-Lizenz
- In OMIVV konfigurierte vCenter Geräteeinstellungen
- HTTP- oder HTTPS-Proxy
- Bereitstellungsmodus
- Erweiterte Überwachung
- Warnungsverwaltung
- Sichern und Wiederherstellen
- PHA-Aktivierung über Dell Anbieter

Die folgenden Einstellungen werden nicht gespeichert und wiederhergestellt:

- Konfiguration auf der virtuellen Konsole (z. B. Netzwerkkonfiguration, Zeitkonfiguration und Kennwort)
- In vCenter veröffentlichte Warnmeldungen und Aufgaben
- In vCenter durchgeführte Änderungen der Warnmeldungen
- Zertifikate
- Auf der Dell EMC Verwaltungskonsole konfigurierte allgemeine Einstellungen
- NTP-Einstellungen
- Anpassen oder Einstellen von Fehlerbedingungen für PHA

Schritte

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Bearbeiten**.
2. Führen Sie im markierten Bereich **EINSTELLUNGEN UND DETAILS** die folgenden Schritte aus:
   a. Geben Sie in **Sicherungsverzeichnis** den Pfad der Sicherungsdateien an.
   b. Geben Sie unter **Nutzername** den Nutzernamen ein.
   c. Geben Sie in **Kennwort** das Kennwort ein.
   d. Geben Sie das Verschlüsselungskennwort in das Feld **Kennwort für die Verschlüsselung von Backups** ein.
      Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: @[]{}_+,-.:=.
   e. Geben Sie das Verschlüsselungskennwort im Feld **Kennwort bestätigen** erneut ein.
   f. Zum Validieren des Backup-Speicherorts und zum Verschlüsseln des Backup-Kennworts klicken Sie auf **Test**.
3. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.
4. Konfigurieren Sie den Backup-Zeitplan. Weitere Informationen finden Sie unter Planen von automatischen Backups.

Nächste Schritte

Konfigurieren Sie nach diesem Verfahren einen Backup-Zeitplan.

NFS-Anforderungen

Die folgenden Einstellungen sind für OMIVV bei der Konfiguration von NFS erforderlich:

- Stellen Sie sicher, dass Sie über Leseberechtigungen für die Durchführung von Wiederherstellungs- und Schreibberechtigungen für das Backup verfügen.
- Konfigurieren Sie für die Windows-basierte NFS-Freigabe Folgendes:
  - Klicken Sie im Ordner „Eigenschaften“ auf **Sicherheit** und stellen Sie sicher, dass **Jeder** über die folgenden Berechtigungen verfügt:
    - Berechtigung zum vollständigen Zugriff für Backup und Wiederherstellung
    - Lesen und ausführen, lesen, ändern und Auflisten der Ordnerinhaltsberechtigungen für RPM-Upgrade.
  - Klicken Sie in den Ordnereigenschaften auf **NFS-Freigabe** und klicken Sie dann auf **Verwalten der NFS-Freigabe**.

    Das Fenster **Erweiterte NFS-Freigabe** wird angezeigt.

    - Wählen Sie den **Anonymen Zugriff zulassen** aus und legen Sie dann die Werte für UID und GID auf 91 fest.
    - Wählen Sie **Unix-Zugriff durch nicht zugeordneten Benutzer zulassen**aus.
- In einer Linux-basierten NFS-Freigabe erstellt und liest OMIVV Datei mit UID 53. Stellen Sie sicher, dass das als NFS-Freigabe exportierte Linux-Verzeichnis Lese-, Schreib- und Ausführungsrechte für UID 53 über Nutzer-Squash bei NFS-Konfiguration oder zugeordneten Nutzer mit UID 53 hat.

Automatische Backups planen

Info über diese Aufgabe

Weitere Informationen zum Konfigurieren des Backup-Speicherorts und des Berechtigungsnachweises finden Sie unter Konfigurieren von Backup und Wiederherstellung.

Schritte

1. Auf der Seite **EINSTELLUNGEN FÜR BACKUP UND WIEDERHERSTELLUNG** klicken Sie auf **Bearbeiten automatisch geplanter Backup**.

Die relevanten Felder sind aktiviert.

2. Klicken Sie auf **Aktiviert**, um Backups zu aktivieren.
3. Aktivieren Sie die Kontrollkästchen **Tage, an denen ein Backup durchgeführt werden soll** für die Tage, an denen eine Backup-Aufgabe durchgeführt werden soll.
4. Geben Sie die Zeit in dem Format SS: MM in **Uhrzeit für Backup (24 Stunden, SS: MM)** ein.
   Das Feld **Nächster Backup** wird mit dem Datum und der Uhrzeit für den nächsten geplanten Backup ausgefüllt.
5. Klicken Sie auf **Anwenden**.

Sofortiges Backup durchführen

Schritte

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Jetzt sichern**.
2. Aktivieren Sie im Dialogfeld **JETZT SICHERN** das Kontrollkästchen **Speicherort und Verschlüsselungskennwort aus den Sicherungseinstellungen verwenden**, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
3. Geben Sie die Werte für **Sicherungsverzeichnis**, **Nutzername**, **Kennwort** und **Kennwort für Verschlüsselung** ein.
   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: @[]{}_+,-.:=. Es gibt keine Längenbeschränkung für ein Passwort.
4. Klicken Sie auf **Sichern**.

OMIVV-Datenbank aus Backup wiederherstellen

Voraussetzungen

Nach der Wiederherstellung von OMIVV von einer früheren Version gilt Folgendes:

- 11G-Server werden nicht unterstützt. Nur 12G-Server oder spätere Generationen bleiben nach der Wiederherstellung erhalten.
- Hardware Profile und Bereitstellungsvorlagen werden nicht unterstützt. Es wird empfohlen, das Systemprofil für die Bereitstellung zu verwenden.
- Bereitstellungsaufgaben, die auf 11G-Servern geplant sind und/oder Hardwareprofil-basierte Bereitstellungsvorlagen verwenden, werden abgebrochen.
- Alle 11G-Server werden aus den Berechtigungsprofilen entfernt und verbrauchte Lizenzen werden freigegeben.
- Repository-Profile verwenden nur 64-Bit-Pakete.

  ANMERKUNG: Wenn Sie Backups und Wiederherstellungen von 4.x auf 5.x durchführen, wird beim Namen des Clusterprofils ein Warnsymbol angezeigt, da OMIVV das 32-Bit-Firmware-Bundle in 5.x nicht unterstützt. Um die neuesten Änderungen für das Clusterprofil zu verwenden, bearbeiten Sie das Clusterprofil.
- Firmwareupdates-Jobs, die auf 11G-Servern geplant sind, werden abgebrochen.

Stellen Sie sicher, dass der richtige Bereitstellungsmodus konfiguriert ist, bevor Sie den Wiederherstellungsvorgang durchführen.

Schritte

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUM BACKUP UND ZUR WIEDERHERSTELLUNG** auf **Jetzt wiederherstellen**.
2. Geben Sie im Dialogfeld **JETZT WIEDERHERSTELLEN** einen Pfad für den **Dateispeicherort** zusammen mit der Datei backup .gz im CIFS oder NFS-Format ein.
3. Geben Sie den **Nutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.
   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: @[]{}_+,-.:=.
4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
   Bei einer Wiederherstellung wird das OMIVV-Gerät nach Abschluss der Wiederherstellung neu gestartet. Informationen zum Überprüfen der Installation finden Sie unter .

   Schließen Sie nach Abschluss der Wiederherstellung den Browser und löschen Sie den Browser-Cache, bevor Sie sich beim Admin-Portal anmelden.

Sicherungs- und Wiederherstellungseinstellungen zurücksetzen

Info über diese Aufgabe

Mithilfe der Funktion zum Zurücksetzen von Einstellungen können Sie Einstellungen auf den unkonfigurierten Status zurücksetzen.

Schritte

1. Klicken Sie auf der Seite **EINSTELLUNGEN ZUR SICHERUNG UND WIEDERHERSTELLUNG** auf **Einstellungen zurücksetzen**.
2. Klicken Sie im Dialogfeld **Einstellungen zurücksetzen** auf **Anwenden**.

OMIVV-Appliance durch Sichern und Wiederherstellen aktualisieren

Voraussetzungen

Es wird empfohlen, Cluster oder Hosts, die von OMIVV verwaltet werden, nach dem Backup und vor der Wiederherstellung der Backupdatei nicht zu ändern oder zu entfernen. Wenn die von OMIVV verwalteten Cluster oder Hosts geändert oder entfernt werden, konfigurieren Sie nach der Wiederherstellung die Profile (z. B. Host-Zugangsdatenprofil, Clusterprofil), die mit diesen Clustern und Hosts verknüpft sind.

Heben Sie die Registrierung des OMIVV-Plug-ins von vCenter nicht auf. Durch das Aufheben der Registrierung des Plug-ins von vCenter wird der Dell Funktionszustand-Update-Anbieter für proaktive HA-Cluster entfernt, die durch das OMIVV-Plug-in auf vCenter registriert sind.

Es wird empfohlen, einen Snapshot der Appliance zu erstellen, bevor Sie das Upgrade der OMIVV-Appliance durchführen.

Info über diese Aufgabe

Führen Sie die folgenden Schritte aus, um die OMIVV-Appliance von einer älteren Version auf die aktuelle Version zu aktualisieren:

Schritte

1. Sichern Sie die Daten früherer Versionen.
2. Deaktivieren Sie die ältere OMIVV-Appliance im vCenter.
3. Stellen Sie die neue OpenManage Integration-Appliance OVF bereit.
4. Starten Sie die neue OpenManage Integration-Appliance.
5. Richten Sie das Netzwerk und die Zeitzone für die neue Appliance ein.

   ANMERKUNG: Es wird empfohlen, die Identität (IP oder FQDN) der älteren OMIVV-Appliance für die neue OMIVV-Appliance beizubehalten.

6. Im Lieferumfang der OMIVV-Appliance ist ein Standardzertifikat enthalten. Wenn Sie ein nutzerdefiniertes Zertifikat für Ihre Appliance möchten, aktualisieren Sie dasselbe. Siehe Zertifikatsignierungsanforderung (CSR) erstellen und HTTPS-Zertifikat hochladen. Andernfalls überspringen Sie diesen Schritt.
7. Stellen Sie die Datenbank auf dem neuen OMIVV-Appliance wieder her. Siehe Wiederherstellen der OMIVV-Datenbank aus einem Backup.
8. Überprüfen der Appliance. Weitere Informationen finden Sie unter Installation überprüfen.
9. Nach dem Upgrade wird empfohlen, die Bestandsaufnahme auf allen Hosts erneut durchzuführen, die das OMIVV-Plug-in verwaltet.

   Die Einstellungen für Ereignisse und Alarme werden nach der Wiederherstellung der Appliance nicht aktiviert. Sie können die Einstellungen für Ereignisse und Alarme über die Registerkarte **Einstellungen** erneut aktivieren.

   Wenn Sie ein Upgrade von einer früheren Version von OMIVV auf die verfügbare Version durchführen, werden alle geplanten Jobs weiterhin ausgeführt.

   Alle Anpassungen, die auf den eingetragenen Dell Alarmen und dem Dell Funktionszustand-Update-Anbieter für PHA-Cluster durchgeführt werden, werden nach dem Backup- und Wiederherstellungsvorgang auf die Standardeinstellungen zurückgesetzt.

   Nach dem Backup und der Wiederherstellung von einer früheren OMIVV-Version auf eine neuere OMIVV-Version führen Sie die folgenden Aufgaben durch, wenn eines der folgenden Probleme auftritt:
   - 200000-Meldung
   - Dell EMC Logo fehlt.
   - OMIVV-UI reagiert nicht.
   - OMIVV-Plug-in wird nicht von vCenter entfernt.
   - Das SSL-Zertifikat ist ungültig.

   Auflösung:

   - Starten Sie die vSphere Client Services für vSphere Client (HTML5) und vSphere Webclient (Flex) auf dem vCenter Server neu.
   - Wenn das Problem weiterhin besteht:

- Navigieren Sie für VMware vCenter-Server-Appliance zu `/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity`. Rufen Sie für Windows vCenter die folgenden Ordner in der vCenter-Appliance auf und überprüfen Sie, ob die alten Daten der älteren Version vorhanden sind – `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity` Ordner in der vCenter-Appliance und überprüfen Sie, ob die alten Daten, wie z. B. com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X.0.0.XXX vorhanden sind.
- Löschen Sie den Ordner, der der früheren OMIVV-Version entspricht, manuell und starten Sie die vSphere Client Services für vSphere Client (HTML5) und Webclient (Flex) neu.

Wenn die IP-Adresse für die neue Appliance sich von der IP-Adresse der älteren Appliance unterscheidet, führen Sie Folgendes durch:

- Die proaktive HA funktioniert möglicherweise nicht ordnungsgemäß. Deaktivieren und aktivieren Sie in einem solchen Fall die proaktive HA für alle Cluster, in denen der Dell EMC Host vorhanden ist.
- Konfigurieren Sie das Trap-Ziel für die SNMP-Traps, sodass es auf die neue Appliance verweist. Die Identitätsänderung wird durch Ausführung der Bestandsaufname auf diesen Hosts korrigiert. Während der Ausführung der Bestandsaufnahme auf Hosts werden diese Hosts, falls die SNMP-Traps nicht auf die neue IP verweisen, als „nicht konform“ aufgelistet. Informationen zur Behebung von Problemen mit der Host-Compliance finden Sie im Abschnitt Verwaltungs-Compliance im Benutzerhandbuch.

4

Konfigurieren der OMIVV-Appliance mithilfe des Assistenten für die Erstkonfiguration

Nachdem Sie die grundlegende Installation von OMIVV und die Registrierung der vCenter abgeschlossen haben, wird automatisch erstmals der Erstkonfigurationsassistent angezeigt, wenn Sie auf das OMIVV-Symbol klicken.

Sie können den Assistenten für die Erstkonfiguration auch mithilfe der folgenden Schritte starten:

- **Einstellungen** > **Erstkonfigurationsassistent** > **ERSTKONFIGURATIONSASSISTENT STARTEN**
- **Dashboard** > **Schnellverweise** > **ERSTKONFIGURATIONSASSISTENT STARTEN**

ANMERKUNG: Die Benutzeroberfläche ist bei beiden Methoden ähnlich.

ANMERKUNG: Wenn Sie bei der Durchführung OMIVV-bezogener Aufgaben nach dem Ändern der DNS-Einstellungen einen Webkommunikationsfehler erhalten, löschen Sie den Browser-Cache, melden Sie sich vom vSphere Client (HTML5) ab und melden Sie sich dann erneut an.

Unter Verwendung des Assistenten für die ursprüngliche Konfiguration können Sie die folgenden Aufgaben anzeigen und ausführen:

- vCenter auswählen
- Host-Zugangsdatenprofil erstellen Weitere Informationen finden Sie unter Host-Zugangsdatenprofil erstellen.
- Konfigurieren von Ereignissen und Alarmen. Weitere Informationen finden Sie unter Konfigurieren von Ereignissen und Alarmen.
- Planen Sie Bestandsaufnahme-Jobs. Weitere Informationen finden Sie unter Einen Bestandsaufnahme-Job planen.
- Gewährleistungsabfrage-Job planen Weitere Informationen finden Sie unter Gewährleistungsabfrage-Jobs planen.

Themen:

Erstkonfiguration

Info über diese Aufgabe

Nachdem Sie die grundlegende Installation von OMIVV und die Registrierung der vCenter abgeschlossen haben, wird automatisch erstmals der Erstkonfigurationsassistent angezeigt, wenn Sie auf das OMIVV-Symbol klicken.

Wenn Sie den Assistenten für die Erstkonfiguration später starten möchten, navigieren Sie zu:

- **Einstellungen** > **Erstkonfigurationsassistent** > **ERSTKONFIGURATIONSASSISTENT STARTEN**
- **Dashboard** > **Schnellverweise** > **ERSTKONFIGURATIONSASSISTENT STARTEN**

Schritte

1. Lesen Sie auf der **Willkommen**-Seite die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
2. Wählen Sie auf der Seite **vCenter auswählen** im Drop-Down-Menü **vCenter** ein bestimmtes vCenter oder **Alle registrierten vCenter** aus und klicken Sie dann auf **WEITER**.

   ANMERKUNG: Wenn mehrere vCenter Server als Bestandteil der gleichen vCenter Linked Mode-Umgebung mit derselben OMIVV-Appliance registriert sind und Sie die Konfiguration eines einzelnen vCenters ausgewählt haben, müssen Sie Schritt 2 wiederholen, bis Sie jedes vCenter konfiguriert haben.
3. Klicken Sie auf der Seite **Host-Zugangsdatenprofil erstellen** auf **HOST-ZUGANGSDATENPROFIL ERSTELLEN**. Weitere Informationen zum Erstellen eines Host-Zugangsdatenprofils finden Sie unter Host-Zugangsdatenprofil erstellen.

   Nachdem Hosts zu einem Host-Zugangsdatenprofil hinzugefügt wurden, wird die IP-Adresse von OMIVV automatisch als SNMP-Trap-Ziel für den iDRAC des Hosts festgelegt. OMIVV aktiviert den WBEM-Service und deaktiviert ihn dann nach dem Abrufen der iDRAC-IP-Adresse für Hosts, auf denen ESXi 6.5 und höher ausgeführt wird.

OMIVV verwendet den WBEM-Service, um den ESXi-Host und die iDRAC-Beziehungen ordnungsgemäß zu synchronisieren. Wenn die Konfiguration des SNMP-Trap-Ziels und/oder das Aktivieren des WBEM-Service für bestimmte Hosts fehlschlägt, werden diese Hosts als „nicht konform“ geführt. Informationen zum Anzeigen und Beheben der Nichtübereinstimmung finden Sie im Abschnitt Management-Compliance im Benutzerhandbuch.

4. Führen Sie auf der Seite **Zusätzlichen Einstellungen konfigurieren** die folgenden Schritte aus:
   a. Planen Sie Bestandsaufnahme-Jobs. Weitere Informationen zum Planen von Bestandsaufnahme-Jobs finden Sie unter Einen Bestandsaufnahme-Job planen.
   b. Serviceabfrage-Job planen Weitere Informationen zum Planen von Serviceabfrage-Jobs finden Sie unter Gewährleistungsabfrage-Jobs planen.

      Wenn Sie den Zeitplan für die Bestandsaufnahme ändern möchten, navigieren Sie zu **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Bestandsaufnahme-Abruf** oder **Jobs** > **Bestand** > **Hosts-Bestandaufnahme**.

      Wenn Sie den Zeitplan für den Gewährleistungsabruf ändern möchten, navigieren Sie zu **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Gewährleistungsabruf** oder **Jobs** > **Gewährleistung**.
   c. Konfigurieren von Ereignissen und Alarmen. Informationen zum Konfigurieren von Ereignissen und Alarmen finden Sie unter Konfigurieren von Ereignissen und Alarmen.
   d. Um einzelne Einstellungen anzuwenden, klicken Sie separat auf die Schaltfläche **Anwenden** und klicken Sie dann auf **Weiter**.

      Es wird dringend empfohlen, alle zusätzlichen Einstellungen zu aktivieren. Wenn keine der zusätzlichen Einstellungen angewendet werden, wird eine Meldung angezeigt, die darauf hinweist, dass alle zusätzlichen Einstellungen obligatorisch sind.
5. Lesen Sie auf der Seite **Weitere Schritte** die Anweisungen und klicken Sie dann auf **BEENDEN**.

   Es wird empfohlen, Ihre OMIVV-Hosts mit einer Konfigurations-Baseline zu verknüpfen, da Ihnen dies ermöglicht, die Konfigurationsänderungen in Hosts und zugehörigen Clustern aufmerksam zu überwachen. Die Konfigurations-Baseline kann für jedes Cluster erstellt werden, sobald die Hosts erfolgreich von OMIVV verwaltet werden. Gehen Sie wie folgt vor, um eine Konfigurations-Baseline zu erstellen:
   - Repository-Profil für Firmware und Treiber erstellen: Auf diese Weise können Sie Baseline-Firmware- und Treiberversionen definieren.
   - Systemprofil erstellen: Hier können Sie Baseline-Hardwarekonfigurationen für Hosts definieren.
   - Clusterprofil erstellen: Um eine erfolgreiche Baseline zu erstellen, wählen Sie Cluster aus und ordnen Sie Firmware, Treiber und Hardwarekonfigurationen zu.
   - Die in einem PowerEdge MX-Gehäuse mit einem deaktivierten iDRAC IPv4 vorhandenen Hosts müssen über ein Gehäuse-Anmeldeinformationsprofil verwaltet werden.

Host-Zugangsdatenprofil erstellen

Voraussetzungen

Wenn die Anzahl der hinzugefügten Hosts die Lizenzgrenze überschreitet, kann kein Host-Zugangsdatenprofil erstellt werden.

Bevor Sie die Active Directory (AD)-Anmeldeinformationen mit einem Host-Zugangsdatenprofil verwenden, stellen Sie Folgendes sicher:

- Das Nutzerkonto ist in AD vorhanden.
- Der iDRAC oder der Host müssen für die AD-basierte Authentifizierung konfiguriert sein.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Compliance und Bereitstellung** > **Host-Zugangsdatenprofil**.
2. Klicken Sie auf der Seite **Host-Zugangsdatenprofil** auf **NEUES PROFIL ERSTELLEN**.
3. Lesen Sie auf der Seite des Assistenten **Host-Zugangsdatenprofil** die Anweisungen und klicken Sie dann auf **ERSTE SCHRITTE**.
4. Führen Sie auf der Seite **Name und Zugangsdaten** folgende Schritte aus:
   a. Geben Sie den Profilnamen und die Beschreibung an. Die Beschreibung ist optional.
   b. Wählen Sie in der Liste **vCenter-Name** eine Instanz von vCenter aus, auf der Sie das Host-Zugangsdatenprofil erstellen möchten.
   c. Geben Sie im Bereich **iDRAC-Zugangsdaten** die lokalen iDRAC-Zugangsdaten oder die AD-Zugangsdaten ein.
      - Gehen Sie wie folgt vor, um die lokalen Zugangsdaten für iDRAC einzugeben:
        - Geben Sie den Nutzernamen im Feld **Nutzername** ein. Der Nutzername ist auf 16 Zeichen beschränkt.

          Informationen zur Definition von Nutzernamen finden Sie im *iDRAC-Benutzerhandbuch*, das unter https://www.dell.com/support verfügbar ist.
        - Geben Sie das Kennwort ein.

Weitere Informationen zu den empfohlenen Zeichen in Nutzernamen und Kennwörtern finden Sie im *iDRAC Benutzerhandbuch*, das unter https://www.dell.com/support verfügbar ist.

- Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
- Um die Zugangsdaten für einen iDRAC einzugeben, der bereits für AD konfiguriert und aktiviert ist, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.

  ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware und die Bereitstellung eines Betriebssystems (BS).

  - Geben Sie den Nutzernamen im Feld **Active Directory-Nutzername** ein.

    Geben Sie den Nutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Nutzername ist auf 256 Zeichen beschränkt. Informationen zu Nutzernamen-Einschränkungen finden Sie in der **Dokumentation zum Microsoft Active Directory**.

  - Geben Sie das Kennwort ein.

    Die AD-Anmeldeinformationen können für den iDRAC und den Host dieselben oder unterschiedlich sein.

d. Geben Sie im **Host Root**-Bereich die lokalen Host-Zugangsdaten oder AD-Zugangsdaten ein.

Der Standardnutzername lautet root.

- Um die lokalen Host-Zugangsdaten einzugeben, führen Sie die folgenden Schritte durch:
  - Geben Sie das Kennwort ein.

    Das Host-Kennwort ist nur für Hosts erforderlich, auf denen ESXi 6.5 U3 und frühere Versionen ausgeführt werden.

    Um diesen Schritt für ESXi 6.7 und neuere Versionen zu überspringen, stellen Sie sicher, dass das Kontrollkästchen **Host-Zugangsdaten verwenden** deaktiviert ist. Wenn für einen Host, auf dem ESXi 6.7 oder höher ausgeführt wird, ein Kennwort eingegeben wurde, wird das Kennwort ignoriert.

    Für Hosts, auf denen ESXi 6.7 oder höherausgeführt werden, wird empfohlen, keine Zugangsdaten für ESXi einzugeben. OMIVV kann die iDRAC mit dem ESXi-Host verbinden, selbst wenn falsche Host-Zugangsdaten eingegeben wurden.

- Um die Zugangsdaten für Hosts einzugeben, die bereits für AD konfiguriert und aktiviert sind, aktivieren Sie das Kontrollkästchen **Active Directory verwenden**.
  - Geben Sie den Nutzernamen im Feld **Active Directory-Nutzername** ein. Geben Sie den Nutzernamen in einem dieser Formate ein: `domain\username` oder `username@domain`. Der Nutzername ist auf 256 Zeichen beschränkt. Informationen zu Nutzernamen-Einschränkungen finden Sie in der **Dokumentation zum Microsoft Active Directory**.
  - Geben Sie das Kennwort ein.
- Um das Host-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, markieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.

5. Klicken Sie auf **Weiter**.
   Die Seite **Zugeordnete Gehäuse** wird angezeigt.
6. Klicken Sie auf der Seite **zugeordnete Hosts** zum Hinzufügen oder Entfernen von Hosts auf **HOSTS HINZUFÜGEN/ENTFERNEN**.
   Die Seite **Hosts hinzufügen oder entfernen** wird angezeigt.
   a. Erweitern Sie auf der Seite **Hosts hinzufügen oder entfernen** die Strukturansicht, wählen Sie die Hosts aus oder entfernen Sie sie und klicken Sie dann auf **OK**.

   ANMERKUNG: Fügen Sie keine PowerEdge MX-Server mit deaktiviertem iDRAC-IPv4 zu einem Host-Zugangsdatenprofil hinzu. Diese Server werden mit einem Gehäuse-Zugangsdatenprofil verwaltet.

7. Um die Verbindung zu testen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **TEST STARTEN**.
   Es wird empfohlen, dass Sie die Verbindung für alle konfigurierten Hosts testen.
   Während der Testverbindung aktiviert OMIVV den WBEM-Service und deaktiviert ihn dann nach dem Abrufen der iDRAC-IP-Adresse für Hosts, auf denen ESXi 6.5 und höher ausgeführt wird.

   ANMERKUNG: Nach der Eingabe gültiger Zugangsdaten kann es vorkommen, dass der Testverbindungsvorgang für den Host fehlschlägt und eine Meldung angezeigt wird, die darauf hinweist, dass ungültige Zugangsdaten eingegeben wurden. Dieses Problem tritt auf, wenn ESXi den Zugriff blockiert. Bei mehreren Anmeldeversuchen am ESXi mit den falschen Zugangsdaten wird Ihr Zugang zu ESXi 15 Minuten lang gesperrt. Warten Sie 15 Minuten und versuchen Sie den Vorgang erneut.

- Um den Testverbindungsprozess zu beenden, klicken Sie auf **TEST ABBRECHEN**.

Sie können die Ergebnisse der Testverbindung im Bereich **TESTERGEBNISSE** anzeigen.

8. Klicken Sie auf **Fertigstellen**.

Einen Bestandsaufnahme-Job planen

Info über diese Aufgabe

Um die neuesten Bestandsdaten auf OMIVV anzuzeigen, müssen Sie einen Bestandsaufnahme-Job regelmäßig planen, um sicherzustellen, dass die Bestandsinformationen der Hosts oder des Gehäuses auf dem neuesten Stand sind. Es wird empfohlen, den Bestandsaufnahme-Job wöchentlich auszuführen.

ANMERKUNG: Das Gehäuse wird im OMIVV-Kontext verwaltet. Es gibt keinen Kontext von vCenter in der Gehäuseverwaltung. Nachdem die geplante Host-Bestandsaufnahme abgeschlossen ist, wird die Gehäuse-Bestandsaufnahme für alle mit OMIVV verwalteten Gehäuse ausgelöst.

ANMERKUNG: Die Einstellungen auf dieser Seite werden jedes Mal auf den Standardwert zurückgesetzt, wenn der Konfigurationsassistent aufgerufen wird. Wenn Sie zuvor schon einen Zeitplan für die Bestandsaufnahme konfiguriert haben, stellen Sie sicher, dass Sie den vorherigen Zeitplan auf dieser Seite vor Abschluss der Assistentenfunktionen replizieren, damit der vorherige Zeitplan nicht durch die Standardeinstellungen außer Kraft gesetzt wird.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter Einstellungen** > **Zeitplan Datenabruf** > **Bestandsaufnahme-Abruf**.
2. Aktivieren Sie das Kontrollkästchen **Abruf von Bestandsaufnahmedaten aktivieren (empfohlen)**.

   Wenn in einer vCenter Linked Mode-Umgebung mit mehreren vCenter Servern der Zeitplan für einzelne vCenter unterschiedlich ist und Sie die Option **Alle registrierten vCenter** auswählen, um den Bestandsaufnahme-Zeitplan zu aktualisieren, wird auf der Seite „Bestandsaufnahme-Zeitplaneinstellungen“ der Standardzeitplan angezeigt.
3. Wählen Sie den Tag und die Uhrzeit für den Abruf von Bestandsaufnahmedaten aus und klicken Sie auf **ANWENDEN**.

   ANMERKUNG: Wenn Sie in einer vCenter Linked Mode-Umgebung mit mehreren vCenter Servern den Bestandsaufnahme-Zeitplan für **Alle registrierten vCenter** aktualisieren, überschreibt die Aktualisierung die Einstellungen für den individuellen vCenter Bestandsaufnahme-Zeitplan.

Gewährleistungsabfrage-Jobs planen

Voraussetzungen

1. Um den Autorisierungsschlüssel zu aktualisieren, stellen Sie sicher, dass Sie Zugriff auf den Index-Katalog (`https://downloads.dell.com/catalog/CatalogIndex.gz`) haben.
2. Um einen Servicebericht zu erhalten, stellen Sie sicher, dass Sie Zugriff auf `https://apigtwb2c.us.dell.com` haben.
3. Stellen Sie sicher, dass die Bestandsaufnahme erfolgreich auf Hosts und Gehäusen ausgeführt wird.
4. Um die Servicefunktionen von OMIVV zu verwenden, müssen Sie über eine Internetverbindung verfügen. Wenn Ihre Umgebung einen Proxy für das Internet benötigt, stellen Sie sicher, dass Sie die Proxyeinstellungen im Admin-Portal konfigurieren.

Info über diese Aufgabe

Hardware-Serviceinformationen werden von Dell Online abgerufen und von OMIVV angezeigt. Nur die Service-Tag-Nummer wird gesendet und nicht von Dell Online gespeichert.

In einer vCenter Linked Mode-Umgebung mit mehreren vCenter Servern wird die Gehäusegewährleistung automatisch bei jedem vCenter ausgeführt, wenn die Gewährleistung für ein beliebiges vCenter ausgeführt wird. Jedoch wird der Service nicht automatisch hinzugefügt, wenn er nicht zum Gehäuse-Zugangsdatenprofil hinzugefügt wird.

ANMERKUNG: Die Einstellungen auf dieser Seite werden jedes Mal auf den Standardwert zurückgesetzt, wenn der Konfigurationsassistent aufgerufen wird. Wenn Sie zuvor schon einen Serviceabfrage-Job konfiguriert haben, stellen Sie sicher, dass Sie den vorherigen Zeitplan auf dieser Seite vor Abschluss der Assistentenfunktionen replizieren, damit der vorherige Zeitplan nicht durch die Standardeinstellungen außer Kraft gesetzt wird.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter-Einstellungen** > **Planung für Routinejobs** > **Serviceabfrage**.
2. Aktivieren Sie das Kontrollkästchen **Abruf von Servicedaten aktivieren (empfohlen)**.

   Wenn in einer vCenter Linked Mode-Umgebung mit mehreren vCenter Servern der Zeitplan für einzelne vCenter unterschiedlich ist und Sie die Option **Alle registrierten vCenter** auswählen, um den Gewährleistungs-Zeitplan zu aktualisieren, wird auf der Seite „Gewährleistungs-Zeitplaneinstellungen“ der Standardzeitplan angezeigt.
3. Wählen Sie den Tag und die Uhrzeit für den Abruf von Servicedaten aus und klicken Sie auf **ANWENDEN**.

   ANMERKUNG: Wenn Sie in einer vCenter Linked Mode-Umgebung mit mehreren vCenter Servern den Gewährleistungs-Zeitplan für **Alle registrierten vCenter** aktualisieren, überschreibt die Aktualisierung die Einstellungen für den individuellen vCenter Gewährleistungs-Zeitplan.

Konfigurieren von Ereignissen und Alarmen

Voraussetzungen

- Aktivieren Sie SNMP-Ereignisse auf der Seite iDRAC-Einstellungen für alle von OMIVV verwalteten Hosts.
- Zum Empfangen von Ereignissen von den Servern müssen Sie sicherstellen, dass das SNMP-Trap-Ziel in iDRAC festgelegt ist. OMIVV unterstützt SNMP v1- und v2-Warnmeldungen.
- Stellen Sie vor der Aktivierung von Hosts und Gehäuse- und MPR-Warnungen sicher, dass Sie die Ereignisanzeigeebene auf „Alle Ereignisse veröffentlichen“ oder „Nur kritische Ereignisse und Warnungsereignisse veröffentlichen“ oder „Nur Ereignisse veröffentlichen“ festlegen.
- Um die Alarme für alle Hosts und Ihr Gehäuse zu erhalten, legen Sie die Ereignisanzeigenebene auf „Alle Ereignisse veröffentlichen“, „Nur kritische Ereignisse und Warnereignisse veröffentlichen“ oder „Nur Ereignisse im Zusammenhang mit Virtualisierung anzeigen“.
- Stellen Sie sicher, dass für alle Hosts, die unter Verwendung von OMIVV verwaltet werden, die Option **Memory Page Retire Warnung für alle Hosts aktivieren** aktiviert ist, um MPR-Warnmeldungen für alle Hosts zu erhalten.

  Legen Sie darüber hinaus die Ereignisanzeigenebene auf „Alle Ereignisse übermitteln“, „Nur kritische Ereignisse und Warnereignisse veröffentlichen“ oder „Nur Ereignisse im Zusammenhang mit Virtualisierung anzeigen“ fest.
- Stellen Sie sicher, dass Sie die gleiche Zeitzone zwischen OMIVV und vCenter festlegen. Wenn die Zeitzonen unterschiedlich sind, kann es zu Verzögerungen bei der Veröffentlichung von Alarmen kommen.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **vCenter-Einstellungen** > **Ereignisse und Alarme**.
2. Führen Sie die folgenden Schritte aus, um MPR-Alarme (Memory Page Retire) zu aktivieren:
   a. Klicken Sie auf **MPR-Alarme für alle Hosts aktivieren**.

      Das Dialogfeld **MPR-Alarm aktivieren** wird angezeigt.
   b. Klicken Sie zum Übernehmen der Änderungen auf **WEITER**.
   c. Klicken Sie auf **ANWENDEN**, um die Änderungen zu speichern.

      Weitere Informationen über MPR (Memory Page Retire) finden Sie unter Prognose-MPR (Memory Page Retire) OMIVV.
3. Gehen Sie wie folgt vor, um Alarme für alle Hosts und ihr Gehäuse zu aktivieren:
   a. Klicken Sie auf **Alarme für alle Hosts und ihr Gehäuse aktivieren**.
   Auf der Seite **Dell EMC Alarmwarnung aktivieren** werden die Cluster und nicht gruppierten Hosts angezeigt, die möglicherweise nach dem Aktivieren der Dell EMC Alarme beeinträchtigt werden.

      ANMERKUNG: Dell EMC Hosts, auf denen Alarme aktiviert sind, die auf einige spezifische kritische Ereignisse reagieren, indem sie in den Wartungsmodus übergehen. Nehmen Sie den Host manuell aus dem Wartungsmodus heraus. Sie können den Alarm bei Bedarf ändern.

      ANMERKUNG: In vCenter 6.7 U1 und 6.7 U2 schlägt die Bearbeitungsoption fehl. Für die Bearbeitung von Alarmdefinitionen wird die Verwendung von Webclient (Flex) empfohlen.

      ANMERKUNG: BMC-Traps verfügen nicht über Meldungs-IDs. Warnungen enthalten also demzufolge diese Details nicht in OMIVV.
   b. Klicken Sie zum Übernehmen der Änderungen auf **WEITER**.
   c. Klicken Sie auf **ANWENDEN**, um die Änderungen zu speichern.
   Die Alarme für alle Hosts und Ihr Gehäuse sind aktiviert.
4. Wählen Sie eine der folgenden Ereignismeldungsebenen aus und klicken Sie dann auf **ANWENDEN**.

- **Keine Ereignisse veröffentlichen**: Es werden keine Ereignisse oder Warnungen an die zugehörigen vCenter weitergeleitet.
- **Alle Ereignisse veröffentlichen**: Alle Ereignisse, einschließlich informativer Ereignisse, sowie von den verwalteten Hosts und Gehäusen empfangene Ereignisse, werden in den zugehörigen vCentern veröffentlicht.
- **Nur kritische Ereignisse und Warnereignisse veröffentlichen**: Nur die kritischen Ereignisse und Ereignisse auf Warnstufe werden in den zugehörigen vCentern angezeigt.
- **Nur Ereignisse im Zusammenhang mit Virtualisierung anzeigen**: Die von den Hosts empfangenen virtualisierungsbezogenen Ereignisse werden in den zugehörigen vCentern veröffentlicht. Virtualisierungsbezogene Ereignisse sind solche, die für Hosts, die VMs ausführen, am wichtigsten sind. Diese Option ist standardmäßig ausgewählt.

5. Klicken Sie auf **ALARME WIEDERHERSTELLEN** und dann auf **ANWENDEN**, um die Standardeinstellungen für vCenter-Alarme für alle Hosts und ihre Gehäuse wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.

   Mit der Option **ALARME WIEDERHERSTELLEN** kann die standardmäßige Alarmkonfiguration wiederhergestellt werden, ohne dass das Produkt de- und neu installiert werden muss. Alle nach der Installation geänderten Dell EMC Alarmkonfigurationen werden durch den Klick auf Option **ALARME WIEDERHERSTELLEN** zurückgesetzt.

   ANMERKUNG: Die Einstellungen für Ereignisse und Alarme werden nach der Wiederherstellung des Geräts nicht aktiviert. Sie können die Einstellungen für Ereignisse und Alarme über die Registerkarte Einstellungen erneut aktivieren.

Prognose-MPR (Memory Page Retire) OMIVV

Memory Page Retire (MPR) ist eine Funktion vor dem Ausfall, die in den unterstützten PowerEdge Hosts verfügbar ist. Diese Funktion ermöglicht es dem Host, das Betriebssystem über die korrigierbaren Speicherfehler zu informieren, die auf einer Speicherseite aufgetreten sind. Derzeit werden MPR-Ereignisse für alle von OMIVV verwalteten Hosts registriert.

Wenn in einem bestimmten Sektor genügend Fehler auftreten, kann dies ein Hinweis auf eine mögliche Schwächung in diesem DIMM sein. Dies kann zu einem nicht korrigierbaren Fehlerereignis und einem potenziellen Systemabsturz führen.

OMIVV sammelt die MEM0002-Warnmeldungen für jedes DIMM, wenn Sie von iDRAC empfangen werden. Sobald die Warnmeldungen einen Schwellenwert (14400) erreicht haben und sich auf alle DIMMs im System angesammelt haben, zeigt OMIVV ein Ereignis auf der vCenter **Ereignissseite** an. Diese Überwachungsfunktion ist eine Art mögliche Prognose von MPR in OMIVV. Weitere Informationen zur Berechnung der Schwellenwerteinstellung finden Sie unter Schwellenwerteinstellung berechnen.

Um die Alarmbenachrichtigung zu senden, aktivieren Sie auf der Seite **Ereignisse und Alarme** von OMIVV die Option **MPR-Alarm für alle Hosts aktivieren**. Weitere Informationen finden Sie unter Konfigurieren von Ereignissen und Alarmen.

Wenn der Schwellenwert für korrigierbare Speicherfehler erreicht ist und der MPR-Prognosealarm aktiviert ist, wird der Host in den Wartungsmodus versetzt.

ANMERKUNG: Die MPR-Funktion wird für PowerEdge MX-Hosts, die mit einem Gehäuse-Zugangsdatenprofil mit Unified IP verwaltet wird, nicht unterstützt.

Schwellenwerteinstellung berechnen

Dieser Schwellenwert (14400) wird basierend auf der Standard-Seitengröße von 1 MB konfiguriert (Standardkonfiguration in ESXi 6.7 und höher). Prognostizierte MPR wird generiert, nachdem 60 % der korrigierbaren Fehleranzahl erreicht wurde. MPR pro 4 KB Seite lautet 96 korrigierbare Fehler und für 1 MB Seitengröße. 60 % der korrigierbaren Fehler sind 14400.

Das Zählen beginnt, wenn der Host zum Host-Anmeldeinformationenprofil hinzugefügt wird. Das Zurücksetzen des Zählers erfolgt, wenn der Schwellenwert erreicht ist oder OMIVV neu gestartet wird.

ANMERKUNG: Wenn OMIVV zurückgesetzt oder neu gestartet wird, wird der Zähler auf Null zurückgesetzt. Dies führt zu einer weniger genauen Prognose des MPR-Ereignisses.

Konfigurationsaufgaben auf der Seite „Einstellungen“

Auf der Seite **Einstellungen** können Sie die folgenden Aufgaben ausführen:

- Garantieablaufbenachrichtigung konfigurieren
- Benachrichtigung über aktuelle Geräteversion konfigurieren
- Konfigurieren von Anmeldeinformationen für die Bereitstellung
- Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben

- Erstkonfiguration

Serviceablaufbenachrichtigung einrichten

Info über diese Aufgabe

Aktivieren Sie die Benachrichtigung zum Ablauf des Service, um benachrichtigt zu werden, wenn die Services für einen der Hosts kurz vor dem Ablauf stehen.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Benachrichtigungen** > **Serviceablaufbenachrichtigung**.
2. Wählen Sie **Gewährleistungsablaufbenachrichtigung für Hosts aktivieren**.
3. Wählen Sie aus, wie viele Tage vor Ablauf des Service Sie benachrichtigt werden möchten.
4. Klicken Sie auf **ANWENDEN**.

Benachrichtigung über aktuelle Geräteversion konfigurieren

Voraussetzungen

Um über die Verfügbarkeit einer neuen OMIVV-Version informiert zu werden, markieren Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren (empfohlen)**. Es empfiehlt sich, dies wöchentlich zu überprüfen. Um die neuesten Funktionen der Geräteversionsbenachrichtigung von OMIVV zu verwenden, müssen Sie über eine Internetverbindung verfügen. Wenn Ihre Umgebung einen Proxy für die Verbindung mit dem Internet benötigt, stellen Sie sicher, dass Sie die Proxy-Einstellungen auf dem Admin-Portal konfigurieren.

Info über diese Aufgabe

Zum Empfangen regelmäßiger Benachrichtigungen zur Verfügbarkeit der aktuellen Version (RPM, OVF, RPM/OVF) von OMIVV führen Sie die folgenden Schritte aus, um die Benachrichtigung zur aktuellen Version zu konfigurieren:

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Anwendungseinstellungen** > **Benachrichtigungen** > **Benachrichtigung zur aktuellen Version**.
2. Aktivieren Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren**.
3. Um Benachrichtigung zur aktuellen Geräteversion zu erhalten, wählen Sie Datum und Uhrzeit aus.
4. Klicken Sie auf **ANWENDEN**.

Konfigurieren von Anmeldeinformationen für die Bereitstellung

Info über diese Aufgabe

OMIVV fungiert als Bereitstellungsserver. Die Anmeldeinformationen für die Bereitstellung ermöglichen Ihnen, mit dem iDRAC zu kommunizieren, der das OMIVV-Plug-in als Bereitstellungsserver im Prozess der automatischen Ermittlung verwendet. Mit den Bereitstellungs-Anmeldeinformationen können Sie iDRAC-Anmeldedaten einrichten, um bis zum Abschluss des Betriebssystem-Bereitstellungsprozesses sicher mit einem Bare-Metal-Server zu kommunizieren, das über die automatische Erkennung erkannt wird.

Nach erfolgreichem Abschluss des Betriebssystem-Bereitstellungsprozesses ändert OMIVV die iDRAC-Anmeldeinformationen wie im Host-Zugangsdatenprofil angegeben. Wenn Sie die Bereitstellungs-Anmeldeinformationen ändern, werden alle neu erkannten Systeme ab diesem Zeitpunkt mit den neuen iDRAC-Anmeldeinformationen bereitgestellt. Die Anmeldeinformationen auf Servern, die vor der Änderung der Bereitstellungs-Anmeldeinformationen erkannt wurden, sind jedoch von dieser Änderung nicht betroffen.

Schritte

1. Klicken Sie auf der OMIVV-Startseite auf **Einstellungen** > **Appliance-Einstellungen** > **Anmeldeinformationen für die Bereitstellung**.
2. Geben Sie den Nutzernamen und das Kennwort ein. Der Standard-Nutzername lautet **root** und das Kennwort **calvin**.

Stellen Sie sicher, dass Sie das Kennwort basierend auf der iDRAC-Nutzerkennwort-Richtlinie eingeben, die in iDRAC festgelegt ist. Stellen Sie außerdem sicher, dass Sie von iDRAC unterstützte Zeichen verwenden.

3. Klicken Sie auf **ANWENDEN**.

Schweregrad der Funktionszustands-Aktualisierungsbenachrichtigung überschreiben

Info über diese Aufgabe

Sie können einstellen, dass der vorhandene Schweregrad der proaktiven Dell HA-Ereignisse für den Dell EMC Host und seine Komponenten mit dem benutzerdefiniertem Schweregrad überschrieben wird, der auf Ihre Umgebung ausgerichtet ist.

Im Folgenden werden die Schweregrade aufgeführt, die für jedes der proaktiven HA-Ereignisse gelten:

- **Info**
- **Mäßig herabgesetzt**
- **Stark herabgesetzt**

ANMERKUNG: Sie können den Schweregrad der proaktiven HA-Komponenten mit dem Schweregrad **Info** anpassen.

Schritte

1. Klicken Sie in OpenManage Integration for VMware vCenter auf **Einstellungen** > **Schweregrad für proaktiven HA überschreiben**. Das Datenraster zeigt alle unterstützten proaktiven Hochverfügbarkeitsereignisse an. Zu den Spalten des Datenrasters gehören Spalten wie Ereignis-IDs, Ereignisbeschreibung, Komponententyp, Standardschweregrad und die Spalte „Schweregrad überschreiben“ für die Anpassung des Schweregrads des Hosts und den dazugehörigen Komponenten.
2. Um den Schweregrad eines Hosts oder seiner Komponente zu ändern, wählen Sie in der Spalte **Schweregrad überschreiben** den erforderlichen Status aus der Dropdownliste aus.
   Diese Richtlinie gilt für alle proaktiven HA-Hosts auf alle vCenter-Servern, die bei OMIVV registriert sind.
3. Wiederholen Sie Schritt 2 für alle Ereignisse, die angepasst werden sollen.
4. Führen Sie eine der folgenden Aktionen aus:
   a. Zum Speichern der Anpassung klicken Sie auf **ANWENDEN**.
   b. Klicken Sie auf **ABBRECHEN**, um die Einstellungen zum Überschreiben des Schweregrads abzubrechen.

   Klicken Sie auf **AUF STANDARDEINSTELLUNG ZURÜCKSETZEN**, um die Einstellungen zum Überschreiben des Schweregrads auf die Standardeinstellungen zurückzusetzen.

A

Zugriff auf Support-Inhalte von der Dell EMC Support-Website

Greifen Sie auf unterstützende Inhalte in Verbindung mit einem Array von Systemverwaltungstools über direkte Links zu, gehen Sie zur Dell EMC Support-Website oder verwenden Sie eine Suchmaschine.

- Direkte Links:
  - Für Dell EMC Enterprise Systems Management und Dell EMC Remote Enterprise Systems Management –https://www.dell.com/esmmanuals
  - Für Dell EMC Virtualisierungslösungen –www.dell.com/virtualizationsolutions
  - Für Dell EMC OpenManage –https://www.dell.com/openmanagemanuals
  - For iDRAC –https://www.dell.com/idracmanuals
  - Für Dell EMC OpenManage Connections Enterprise Systems Management –https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Für Dell EMC Betriebsfähigkeit Tools –https://www.dell.com/serviceabilitytools
- Support-Site von Dell EMC:
  1. Navigieren Sie zu https://www.dell.com/support.
  2. Klicken Sie auf **Alle Produkte durchsuchen**.
  3. Klicken Sie auf der Seite **Alle Produkte** auf **Software** und klicken Sie dann auf den erforderlichen Link:
  4. Klicken Sie auf das gewünschte Produkt und anschließend auf die gewünschte Version.

Für Suchmaschinen: Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.

B

Zugehörige Dokumentation

Zusätzlich zu dieser Anleitung können Sie auf die anderen Anleitungen zugreifen, die unter **https://www.dell.com/support** zur Verfügung stehen. 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 – Sicherheitskonfigurationsleitfaden*
- *OpenManage Integration for VMware vCenter Version 5.4 – API-Handbuch*

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

C

Kontaktaufnahme mit Dell

Voraussetzungen

ANMERKUNG: Wenn Sie über keine aktive Internetverbindung verfügen, so finden Sie Kontaktinformationen auf der Eingangsrechnung, dem Lieferschein, der Rechnung oder im Dell Produktkatalog.

Info über diese Aufgabe

Dell bietet verschiedene Optionen für Online- und Telefonsupport an. Die Verfügbarkeit ist abhängig von Land und Produkt und einige Dienste sind in Ihrem Gebiet möglicherweise nicht verfügbar. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

Schritte

1. Rufen Sie die Website **Dell.com/support** auf.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region in der Drop-Down-Liste **Land oder Region auswählen** am unteren Seitenrand aus.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.