OpenManage Integration for VMware vCenter Version 4.3

Web-Client-Installationsanleitung

DELL EMC

Anmerkungen, Vorsichtshinweise und Warnungen

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

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2018 - 10

Rev. A00

Inhaltsverzeichnis

1

Einführung

Dieses Handbuch enthält eine Schritt-für-Schritt-Anleitungen für die Installation und Konfiguration von OpenManage Integration for VMware vCenter (OMIVV) mit Power Edge-Servern. Lesen Sie nach der OMIVV-Installation die Informationen zu allen Aspekten der Verwaltung – einschließlich Bestandsmanagement, Überwachung und Warnungen, Firmware-Aktualisierungen sowie Garantieverwaltung – im *OpenManage Integration for VMware vCenter-Benutzerhandbuch* unter **Dell.com/support/manuals**.

Themen:

OpenManage Integration for VMware vCenter-Lizenzierung

OpenManage Integration for VMware vCenter 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 OpenManage Integration for VMware vCenter verwaltet werden. Diese 90-Tage-Testversion ist die Standardlizenz, die mitgeliefert wird.
- Standardlizenz – Die Produkt-Vollversion enthält eine Standardlizenz für bis zu zehn vCenter-Server und die erworbene Anzahl an Hostverbindungen, die von OMIVV verwaltet werden.

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.

Die Lizenzierung enthält die folgenden Informationen:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu zehn registrierte und verwendete vCenter-Verbindungen sind aktiviert.
- Höchstzahl der Host-Verbindungslizenzen – entspricht der Anzahl von erworbenen Lizenzen für Hostverbindungen.
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern), die erfasst und in die Bestandsliste aufgenommen wurden.
- Verfügbar – die Anzahl von Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.

ANMERKUNG: Der Standardlizenzzeitraum beträgt nur drei oder fünf Jahre und die zusätzlichen Lizenzen werden zu den existierenden Lizenzen hinzugefügt und nicht überschrieben.

Wenn Sie die Lizenzdatei kaufen, können Sie die XML-Datei (Lizenzschlüssel) über das digitale Schließfach von Dell unter 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 Bestellunterstützung.

Lizenzanforderungen für Hosts und vCenter Server

Im Folgenden werden die Lizenzierungsanforderungen für Hosts und vCenter beschrieben:

- Sie können eine Lizenz zur Unterstützung der Anzahl von Dell EMC Servern erwerben, die durch OMIVV verwaltet werden sollen. Eine Lizenz wird nur verwendet, nachdem ein Host zum Verbindungsprofil hinzugefügt wurde. Die Lizenz ist nicht mit einem bestimmten Server verbunden.
- Eine Instanz von OMIVV unterstützt bis zu 10 Instanzen von vCenter-Servern. Es gibt keine separate Lizenz für die Anzahl der vCenter-Servern.

Software-Lizenz erwerben und hochladen

Bis zum Upgrade auf eine volle Produktversion führen Sie eine Testversion aus. Verwenden Sie den Link **Lizenz kaufen** des Produkts, um zur Dell Website zu navigieren und eine Lizenz zu erwerben. Laden Sie diese nach dem Kauf unter Verwendung der **Verwaltungskonsole** hoch.

Info über diese Aufgabe

ANMERKUNG: Die Option Lizenz kaufen wird nur angezeigt, wenn Sie eine Testlizenz verwenden.

Schritte

1 Führen Sie in OpenManage Integration for VMware vCenter einen der folgenden Tasks aus:
   - Klicken Sie im Register **Lizenzierung** neben **Software Lizenz** auf **Lizenz kaufen**.
   - Klicken Sie im Register **Erste Schritte** unter **Grundlegende Tasks** auf **Lizenz kaufen**.
2 Speichern Sie die Lizenzdatei, die Sie über den Dell Digital Locker heruntergeladen haben, an einem bekannten Speicherplatz.
3 Geben Sie die Verwaltungskonsolen-URL in einen Web-Browser ein.
   Verwenden Sie das Format: `https://<ApplianceIPAddress>`
4 Geben Sie im Anmeldefenster der **Verwaltungskonsole** das Kennwort ein, und klicken Sie auf **Anmelden**.
5 Klicken Sie auf **Lizenz hochladen**.
6 Klicken Sie zum Suchen der Lizenzdatei im Fenster **Lizenz hochladen** auf **Durchsuchen**.
7 Wählen Sie die Lizenzdatei aus, und klicken Sie auf **Hochladen**.

ANMERKUNG: 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).

Optionen nach dem Hochladen von Lizenzen

Lizenzdatei für neue Einkäufe

Bei der Aufgabe einer Bestellung zum Kauf einer neuen Lizenz wird von Dell eine E-Mail mit der Auftragsbestätigung gesendet und Sie können die neue Lizenzdatei über Dell Digital Locker unter http://www.dell.com/support/licensing herunterladen. Sie erhalten die Lizenz im XML-Format. Falls Sie die Lizenz im ZIP-Format erhalten, extrahieren Sie die XML-Lizenzdatei vor dem Hochladen aus der ZIP-Datei.

Stacking-Lizenzen

Ab OMIVV-Version 2.1 hat OMIVV die Möglichkeit, mehrere Standardlizenzen zur Erhöhung der Anzahl unterstützter Hosts auf die Summe der in den hochgeladenen Lizenzen enthaltenen Hosts zu erhöhen. Eine Evaluierungslizenz kann nicht gestapelt werden. Die Anzahl der unterstützten vCenter Server kann nicht durch Stapeln erhöht werden, da hierfür die Verwendung mehrerer Geräte erforderlich ist.

Es gibt einige Beschränkungen im Hinblick auf die Funktionalität von Stapel-Lizenzen. 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 eine Lizenz abgelaufen ist, nachdem sie hochgeladen wurde, besteht die Funktionalität für die vorhandenen Hosts weiterhin. Upgrades auf neue Versionen des OMIVV werden jedoch blockiert.

Ersatz von Lizenzen

Sollte ein Problem mit Ihrer Bestellung vorliegen, erhalten Sie eine Ersatzlizenz von Dell. 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

Appliance-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 Fehlermeldung angezeigt.

Hinzufügen von Hosts zu Verbindungsprofilen

Beim Versuch, einen Host zu einem Verbindungsprofil hinzuzufügen, wird verhindert, dass weitere Hosts hinzugefügt werden, wenn die Anzahl von lizenzierten Servern der 11. Generation oder neuer überschritten wird und über die Lizenzanzahl hinausgeht.

Wichtige Hinweise zu Referenzzwecken

- Ab OMIVV 4.0 wird nur der VMware vSphere Web-Client unterstützt und der vSphere Desktop-Client wird nicht unterstützt.
- Für vCenter 6.5 und höher ist die OMIVV-Appliance nur für die Flash-Version verfügbar. Die OMIVV-Appliance ist nicht verfügbar für die HTML5-Version.
- 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 ein OMIVV-Gerät mit einer gültigen DNS-Registrierung bereitstellen. Bei einer statischen IP-Adresse ist sichergestellt, dass die IP-Adresse des OMIVV-Geräts beim Neustart des Systems gleich bleibt.
- Stellen Sie sicher, dass die OMIVV-Hostnamen-Einträge in der Vorwärts- und Rückwärtssuche Ihres DNS-Servers vorhanden sind.

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

  - DNS-Anforderungen für vSphere 5.5
  - DNS-Anforderungen für vSphere 6.0
  - DNS-Anforderungen für vSphere 6.5 und Platform Services Controller-Gerät

- Für den OMIVV-Gerätemodus stellen Sie sicher, dass Sie OMIVV im entsprechenden Modus basierend auf Ihrer Virtualisierungsumgebung bereitstellen. Weitere Informationen finden Sie unter Konfigurieren des Bereitstellungsmodus.
- Konfigurieren Sie das Netzwerk gemäß den Portanforderungen. Weitere Informationen finden Sie unter Portinformationen.

Hardwareanforderungen

OMIVV bietet vollständige Unterstützung für mehrere Generationen der Dell EMC Server mit Unterstützung des vollen Funktionsumfangs für Server mit iDRAC Express oder Enterprise. Ausführliche Informationen zu den plattformspezifischen Anforderungen finden Sie in den *OpenManage Integration for VMware vCenter Release Notes* (Versionshinweise zu OpenManage Integration for VMware vCenter) unter **Dell.com/support/manuals**. Um zu überprüfen, ob Ihre Host-Server berechtigt sind, prüfen Sie die Informationen zu Folgendem in den nachfolgenden Unterabschnitten:

- Unterstützte Server und die Mindest-BIOS
- Von iDRAC unterstützte Versionen (für Bereitstellung und Verwaltung)
- OMSA-Unterstützung für Server der 11. Generation und ältere Server und die ESXi-Version-Unterstützung (für Bereitstellung und Management)
- Unterstützter Speicher und Speicherplatz für OMIVV

OMIVV erfordert LAN auf der Hauptplatine/Netzwerk-Tochterkarte, das auf das Verwaltungsnetzwerk von iDRAC- und CMC- oder Managementmodul-Systemen und das vCenter-Verwaltungsnetzwerk zugreifen kann.

Konfigurieren des Bereitstellungsmodus

Info über diese Aufgabe

Stellen Sie sicher, dass die folgenden Systemvoraussetzungen für die gewünschten Bereitstellungsmodi erfüllt sind:

Tabelle 1. Systemanforderungen für Bereitstellungsmodi

Bereitstellungsmodi	Anzahl der Hosts	Anzahl der CPUs	Speicher in GB	Mindestspeichergröße
Klein	Bis zu 250	2	8	44 GB
Mittel	Bis 500	4	16	44 GB
Groß	Bis zu 1000	8	32	44 GB

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

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

Schritte

1 Scrollen Sie auf der Seite **GERÄTEMANAGEMENT** runter zu **Bereitstellungsmodus**.

Die Konfigurationswerte des Bereitstellungsmodus wie **Klein**, **Mittel** oder **Groß** werden angezeigt, und der Bereitstellungsmodus ist standardmäßig auf **Klein** gesetzt.

2 Klicken Sie auf **Bearbeiten**, wenn Sie den Bereitstellungsmodus basierend auf die Umgebung aktualisieren möchten.

3 Wählen Sie im Modus **Bearbeiten** den gewünschten Bearbeitungsmodus aus, nachdem sichergestellt wurde, dass die Voraussetzungen erfüllt sind.

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 und überprüft, und eine der folgenden Situationen tritt ein:

- 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 und mit dem Neustart des OMIVV-Geräts fortfahren, um die Aktualisierung des Bereitstellungsmodus zu ermöglichen.

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 des Anmeldebildschirms gestartet. Zum Starten des OMIVV-Geräts muss es heruntergefahren, die Systemressourcen auf die vorhandene Einstellung des Bereitstellungsmodus aktualisiert und die Aufgabe Bereitstellungsmodus zurückstufen ausgeführt werden.

Zurückstufen des Bereitstellungsmodus

1 Melden Sie sich bei der Administratorkonsole an.

2 Ändern Sie den Bereitstellungsmodus im gewünschten Maße.

3 Fahren Sie das OMIVV-Gerät herunter, und ändern Sie die Systemressourcen im gewünschten Maße.

4 Schalten Sie das OMIVV-Gerät ein.

BIOS-, iDRAC-, Lifecycle Controller- Versionen

Die für die Aktivierung von OpenManage Integration for VMware vCenter-Funktionen erforderlichen BIOS-, iDRAC- und Lifecycle Controller-Versionen werden in diesem Abschnitt aufgeführt.

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

ANMERKUNG: Es wird empfohlen, Dell EMC OpenManage Enterprise-Modular Edition Version 1.00.01 mit OMIVV 4.3 zu verwenden.

Tabelle 2. BIOS für Dell PowerEdge-Server der 11. Generation

Server	Mindestversion
PowerEdge R210	1.8.2 oder höher
PowerEdge R210II	1.3.1 oder höher
PowerEdge R310	1.8.2 oder höher
PowerEdge R410	1.9.0 oder höher
PowerEdge R415	1.8.6 oder höher
PowerEdge R510	1.9.0 oder höher

Server	Mindestversion
PowerEdge R515	1.8.6 oder höher
PowerEdge R610	6.1.0 oder höher
PowerEdge R710	6.1.0 oder höher
PowerEdge R710	6.1.0 oder höher
PowerEdge R715	3.0.0 oder höher
PowerEdge R810	2.5.0 oder höher
PowerEdge R815	3.0.0 oder höher
PowerEdge R910	2.5.0 oder höher
PowerEdge M610	6.1.0 oder höher
PowerEdge M610x	6.1.0 oder höher
PowerEdge M710HD	5.0.1 oder höher
PowerEdge M910	2.5.0 oder höher
PowerEdge M915	2.6.0 oder höher
PowerEdge T110 II	1.8.2 oder höher
PowerEdge T310	1.8.2 oder höher
PowerEdge T410	1.9.0 oder höher
PowerEdge T610	6.1.0 oder höher
PowerEdge T710	6.1.0 oder höher

Tabelle 3. BIOS für Dell PowerEdge-Server der 12. Generation

Server	Mindestversion
T320	1.0.1 oder höher
T420	1.0.1 oder höher
T620	1.2.6 oder höher
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
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

Server	Mindestversion
R920	1.1.0 oder höher

Tabelle 4. BIOS für Dell PowerEdge-Server der 13. Generation

Server	Mindestversion
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
M630	1.0.0 oder höher
M830	1.0.0 oder höher
FC430	1.0.0 oder höher
FC630	1.0.0 oder höher
FC830	1.0.0 oder höher

Tabelle 5. BIOS für Dell PowerEdge-Server der 14. Generation

Server	Mindestversion
R940	1.0.0 oder höher
R740	1.0.0 oder höher
R740xd	1.0.0 oder höher
R640	1.0.0 oder höher
M640	1.0.0 oder höher
T640	1.0.0 oder höher
T440	1.0.0 oder höher
R540	1.0.0 oder höher
FC640	1.0.0 oder höher
R6415	1.0.0 oder höher
R7425	1.0.0 oder höher

Server	Mindestversion
R7415	1.0.0 oder höher
MX740C	1.0.0 oder höher
MX840C	1.0.0 oder höher

Tabelle 6. iDRAC und Lifecycle Controller für die Bereitstellung

Generation	Version	
	iDRAC	Lifecycle-Controller
PowerEdge Server der 11. Generation	3.35 Für modulare 1.85 für Rack- oder Tower-Systeme	1.5.2 oder höher
PowerEdge Server der 12. Generation	2.30.30.30 oder höher	2.30.30.30 oder höher
PowerEdge-Server der 13. Generation	2.30.30.30 oder höher	2.30.30.30 oder höher
PowerEdge-Server der 14. Generation	3.00.00.00 und höher	3.00.00.00 und höher

Tabelle 7. BIOS- und iDRAC-Anforderungen für den Cloud-Server

Modell	BIOS	iDRAC mit Lifecycle Controller
C6320	1.0.2	2.30.30.30 oder höher
C4130	1.0.2	2.30.30.30 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

Unterstützte Funktionen auf Power Edge-Servern

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

Tabelle 8. Unterstützte Funktionen auf Power Edge-Servern

Funktionen	Plattform		
	11.	12. und 13.	14.
Hardware-Bestandsaufnahme	J	J	J
Ereignisse und Alarme	J (nur SNMP v1)	J (SNMP v1 und v2)	J (SNMP v1 und v2)
Komponentenbezogene Funktionszustandsüberwachung*	J	J	J
BIOS/ Firmwareaktualisierungen #	J	J	J
Proaktive Hochverfügbarkeit$	N	J	J

Funktionen	Plattform		
	11.	12. und 13.	14.
Garantie-Informationen	J	J	J
Host-Übereinstimmung	J	J	J
Automatische/Manuelle Ermittlung von Bare-Metal-Server	J	J	J
Bare-Metal-Compliance	J	J	J
Hardwarekonfiguration	J	J	J
Bare-Metal-Hypervisorbereitstellung	J	J	J
Blinkende Server-LED	J	J	J
SEL-Protokolle anzeigen/löschen	J	J	J
iDRAC verknüpfen und starten	J	J	J
iDRAC-Reset	J	J	J
Systemsperrmodus	N	N	J
Systemprofil	N	N	J
Clusterprofil	N	Y ^	J
Hostverwaltung mit einheitlicher Gehäuse-IP	N	N	J@
Support für OEM-Server	N	J~	J

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

In der Cloud mit Modellnummer C6320 werden Firmware-Aktualisierungen für die Zusatzkarten nicht unterstützt.

$ Funktion für proaktive Hochverfügbarkeit ist nur auf vCenter 6.5 oder höher mit ESXi 6.0 oder höher anwendbar. Desweiteren wird die Funktion für proaktive Hochverfügbarkeit auf Servern mit Embedded PSU sowie Cloud-Server-Modelle nicht unterstützt.

^ Im Clusterprofil werden Konfigurationsabweichungen nicht unterstützt.

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

~ Nur für Server der 13. Generation unterstützt.

Unterstützte Funktionen für PowerEdge-Gehäuse

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

Tabelle 9. 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
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

Erforderlicher Speicherplatz für bereitgestellten Speicher

Das virtuelle OMIVV-Gerät erfordert mindestens 44 GB Festplattenspeicher für bereitgestellten Speicher.

Standardmäßige Virtual Appliance-Konfiguration

Das virtuelle OMIVV-Gerät wird mit 8 GB RAM und 2 virtuellen CPUs bereitgestellt (Bereitstellungsmodus „Klein“).

Softwareanforderungen

Stellen Sie sicher, dass die vSphere-Umgebung die Anforderungen bezüglich des virtuellen Geräts, des Schnittstellenzugriffs und der Überwachungsschnittstelle erfüllt.

Voraussetzungen für den VMware vSphere Web-Client

- Unterstützt vCenter 6.0 und höher
- Erfordert Web Client Services von vCenter (vSphere Desktop-Client wird nicht unterstützt)

Spezifische Software-Anforderungen finden Sie ebenfalls in der *OpenManage Integration for VMware vCenter Compatibility Matrix* (OpenManage Integration for VMware vCenter-Kompatibilitäts-Matrix) unter Dell.com/support/manuals.

Anforderungen für OpenManage Integration for VMware vCenter

Unterstützte ESXi-Versionen auf verwalteten Hosts

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

Tabelle 10. Unterstützte ESXi-Versionen

ESXi-Versionsunterstützung	Server-Generation			
	11G	12G	13G	14G
v5.1	J	J	N	N
v5.1 U1	J	J	N	N
v5.1 U2	J	J	J	N
v5.1 U3	J	J	J (außer M830, FC830 und FC430)	N
v5.5	J	J	N	N
v5.5 U1	J	J	N	N
v5.5 U2	J	J	J	N
v5.5 U3	J	J	J	N
v6.0	J	J	J	N
v6.0 U1	J	J	J	N
v6.0 U2	J	J	J	N
v6.0 U3	J	J	J	J
v6.5	N	J	J	N
v6.5 U1	N	J	J	J
v6.5 U2	N	J	J	J
v6.7	N	J	J	J
v6.7 U1	N	J	J	J

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

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

Tabelle 11. Unterstützte vCenter-Serverversionen

vCenter-Version	Web-Client-Support
v6.0 U2	J
v6.0 U3	J
v6.5	J
v6.5 U1	J

vCenter-Version	Web-Client-Support
v6.5 U2	J
v6.7	J
v6.7 U1	J

ANMERKUNG: Weitere Informationen zum Registrieren eines vCenter-Servers finden Sie im *OpenManage Integration for VMware vCenter Version 4.3 Web Client Install Guide* (Installationshandbuch zu OpenManage Integration for VMware vCenter Version 4.3 Web-Client) unter Dell.com/support/manuals.

OpenManage Integration for VMware vCenter Version 4.3 unterstützt VMware vRealize Operations Manager (vROPS) Version 1.1 und 1.2.

Portinformationen

Virtuelles Gerät und verwaltete Knoten

In OMIVV führt OMIVV bei der Bereitstellung des OMSA-Agenten unter Verwendung des Links *Nicht-konforme Hosts reparieren* im Assistenten **Nicht-konforme vSphere-Hosts korrigieren** die folgende Aktion aus:

- Startet den HTTP Client-Service
- Aktiviert Port 8080
- Stellt den Port für ESXi 5.0 oder höher zum Herunterladen und Installieren von OMSA VIB zur Verfügung

Nach Abschluss der OMSA VIB-Installation wird der Dienst automatisch angehalten und die Schnittstelle geschlossen.

Tabelle 12. Virtual Appliance

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
53	DNS	TCP	Keine	Ausgang	OMIVV-Gerät zu DNS-Server	DNS-Client	Konnektivität zum DNS-Server oder Auflösen der Hostnamen.
69	TFTP	UDP	Keine	Ausgang	OMIVV-Gerät zu TFTP-Server	TFTP-Client	Wird für die Firmware-Aktualisierung auf 11G-Servern mit alter Firmware verwendet.
443	HTTP oder HTTPS	TCP	Keine	Ausgang	OMIVV-Gerät zu Internet	Dell Online-Datenzugriff	Konnektivität zu Online-Garantie (Internet), Firmware und aktuellen RPM-Informationen.
80	HTTP	TCP	Keine	Eingang	ESXi-Server zu OMIVV-Gerät	HTTP-Server	Wird im Betriebssystem-Bereitstellungsprozess für Skripts nach der Installation zur Kommunikation mit dem OMIVV-Gerät verwendet.
162	SNMP-Agent	UDP	Keine	Eingang	iDRAC/ESXi zu OMIVV-Gerät	SNMP-Agent (Server)	Für den Empfang von SNMP-Traps von verwalteten Knoten.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV UI zu OMIVV-Gerät	HTTPS-Server	Von OMIVV angebotene Webdienste. Diese Webdienste werden vom vCenter Web-Client und Dell Admin-Portal genutzt.

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
443	WSMAN	TCP	128 Bit	Ein/Aus	OMIVV-Gerät zu/von iDRAC/OMSA	iDRAC/OMSA-Kommunikation	iDRAC-, OMSA- und CMC-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
445	SMB	TCP	128 Bit	Ausgang	OMIVV-Gerät zu CIFS	CIFS-Kommunikation	Für die Kommunikation mit Windows-Freigaben.
4433	HTTPS	TCP	128 Bit	Eingang	iDRAC zu OMIVV-Gerät	Automatische Ermittlung	Bereitstellungsserver, der für die automatische Ermittlung von verwalteten Knoten verwendet wird.
2049	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Gerät zu NFS	Öffentliche Freigabe	Öffentliche NFS-Freigabe, die vom OMIVV-Gerät für die verwalteten Knoten verfügbar gemacht und für Firmwareaktualisierungs- und Betriebssystem-Bereitstellungsprozesse verwendet wird.
4001 zu 4004	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Gerät 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.
11620	SNMP-Agent	UDP	Keine	Eingang	iDRAC zu OMIVV-Gerät	SNMP-Agent (Server)	Port, der für den Empfang von Standard-SNMP-Warnungen über UDP:162 verwendet wird. Daten von iDRAC, OMSA und CMC werden zur Verwaltung und Überwachung der verwalteten Knoten empfangen.
Benutzer definierte	beliebig	UDP/TCP	Keine	Ausgang	OMIVV-Gerät zu Proxy-Server	Proxy	Für die Kommunikation mit dem Proxy-Server

Tabelle 13. Verwaltete Knoten (ESXi)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
162, 11620	SNMP	UDP	Keine	Ausgang	ESXi zu OMIVV-Gerät	Hardware-Ereignisse	Asynchrone SNMP-Traps, die von ESXi gesendet werden. Dieser Port muss über ESXi geöffnet werden.
443	WSMAN	TCP	128 Bit	Eingang	OMIVV-Gerät zu ESXi (OMSA)	iDRAC/OMSA-Kommunikation	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV-Gerät zu ESXi	HTTPS-Server	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
8080	HTTP	TCP	128 Bit	Ausgang	ESXi zu OMIVV-Gerät	HTTP-Server; lädt den OMSA VIB herunter und behebt nicht konforme vSphere-Hosts	Hilft ESXi beim Herunterladen des OMSA-/Treiber-VIB.

Tabelle 14. Verwaltungsknoten (iDRAC oder CMC oder Management Modul)

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
443	WSMAN/ HTTPS-, REST/ HTTPS	TCP	128 Bit	Eingang	OMIVV-Gerät zum iDRAC oder CMC oder jedes einzelne Verwaltungsmodul	iDRAC-Kommunikation	Bietet Informationen an die Management Station und nehmen Sie die Kommunikation bis MX Gehäuse durch Verwendung von REST oder HTTPS-Protokolle. Dieser Port muss über iDRAC und CMC geöffnet werden.
4433	HTTPS	TCP	128 Bit	Ausgang	iDRAC zu OMIVV-Gerät	Automatische Ermittlung	Für die automatische Ermittlung von iDRAC (verwalteten Knoten) in der Management Station.
2049	NFS	UDP	Keine	Ein/Aus	iDRAC zu/von OMIVV	Öffentliche Freigabe	Für iDRAC zum Zugriff auf die öffentliche NFS-Freigabe, die vom OMIVV-Gerät verfügbar gemacht wird. Wird für die Betriebssystembereitstellung und Firmwareaktualisierung verwendet. Zum Zugriff auf die DRAC-Konfigurationen über OMIVV. Wird im Bereitstellungsprozess verwendet.
4001 zu 4004	NFS	UDP	Keine	Ein/Aus	iDRAC zu/von OMIVV	Öffentliche Freigabe	Für iDRAC zum Zugriff auf die öffentliche NFS-Freigabe, die vom OMIVV-Gerät verfügbar gemacht wird. Wird für die Betriebssystembereitstellung und Firmwareaktualisierung verwendet. Zum Zugriff auf die DRAC-Konfigurationen über OMIVV. Wird im Bereitstellungsprozess verwendet.
69	TFTP	UDP	128 Bit	Ein/Aus	iDRAC zu/von OMIVV	Trivial File Transfer (Einfache Dateiübertragung)	Wird für die erfolgreiche Verwaltung des iDRAC über die Management Station verwendet.

Voraussetzungs-Checkliste

Checkliste, bevor Sie mit der Produktinstallation beginnen:

- Überprüfen Sie, ob Sie über Benutzername und Kennwort für OMIVV verfügen, um auf den vCenter Server zuzugreifen. Der Benutzer hat möglicherweise eine Administratorrolle mit allen erforderlichen Berechtigungen oder einen Nicht-Administratorbenutzer 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-Benutzer.
- Stellen Sie sicher, dass Sie über das Root-Kennwort für ESXi-Hostsysteme oder die Active Directory-Anmeldeinformationen, die Administratorrechte auf dem Host haben, verfügen.
- Überprüfen Sie, ob Sie über den Benutzernamen und das Kennwort verfügen, der bzw. das mit iDRAC Express oder Enterprise assoziiert ist und über Administratorrechte auf dem iDRAC verfügt.
- Überprüfen Sie, ob der vCenter-Server ausgeführt wird.
- Bestimmen Sie den Speicherort des OMIVV-Installationsverzeichnisses.
- Stellen Sie sicher, dass die VMware vSphere-Umgebung die Anforderungen bezüglich des virtuellen Geräts, des Schnittstellenzugriffs und der Überwachungsschnittstelle erfüllt. Installieren Sie außerdem Adobe Flash Player auf einem Client-Systems, falls erforderlich. Weitere Informationen zu der unterstützten Flash Player Version finden Sie in der *OpenManage Integration for VMware vCenter Compatibility Matrix* (OpenManage Integration for VMware vCenter-Kompatibilitäts-Matrix).

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

ANMERKUNG: OMIVV zeigt die VMware Tools als „Wird ausgeführt (Veraltet)“ bei einer Bereitstellung auf ESXi 5.5 und höher an. Sie können eine Aktualisierung der VMware Tools nach einer erfolgreichen Bereitstellung des OMIVV-Geräts oder zu einem beliebigen späteren Zeitpunkt durchführen, falls erforderlich.

ANMERKUNG: Es wird empfohlen, dass sich OMIVV und vCenter-Server im gleichen Netzwerk befinden.

ANMERKUNG: Das OMIVV-Gerätenetzwerk sollte Zugriff auf iDRAC, Host und vCenter haben.

Installieren, Konfigurieren und Aktualisieren von OMIVV

Voraussetzung

Stellen Sie sicher, dass die Hardwareanforderungen erfüllt sind und Sie die benötigte VMware v Center-Software ausführen.

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_<Versionsnummer>.<Buildnummer>.zip* von der Dell Support-Website unter **Dell.com/support** herunter. Weitere Informationen zum Herunterladen von OMIVV finden Sie unter Herunterladen von Dell OpenManage Integration for VMware vCenter.
2. Navigieren Sie zu dem Speicherort, an dem Sie die Datei heruntergeladen haben, und extrahieren Sie den Inhalt.
3. Stellen Sie mithilfe des vSphere-Webclient eine Open Virtualization Format-Datei (OVF), die das OMIVV-Gerät enthält, bereit. Siehe Bereitstellen der OMIVV-OVF.
4. Laden Sie die Lizenzdatei hoch. Weitere Informationen zur Lizenzierung finden Sie unter Hochladen einer Lizenz.
5. Registrieren Sie das OMIVV-Gerät über die Verwaltungskonsole beim vCenter-Server. Siehe Registrieren von OMIVV und Importieren der Lizenzdatei.
6. Verwenden Sie zum Konfigurieren des Geräts den **Erstkonfigurationsassistenten**. Siehe Konfigurationstasks im Konfigurationsassistenten.

Herunterladen von Dell OpenManage Integration for VMware vCenter

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** > **Server** > **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 **Kategorie Systemverwaltung** 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 der OMIVV OVF unter Verwendung des vSphere-Web-Clients

Voraussetzung

Stellen Sie sicher, dass Sie die Produkt-Zip-Datei (*Dell_OpenManage_Integration_<Versionsnummer>.<Build-Nummer>.zip*) bereits von der Dell Website heruntergeladen und extrahiert haben.

Schritte

1 Machen Sie die virtuelle Festplatte für OMIVV Integration for OpenManage vCenter ausfindig, die Sie heruntergeladen und extrahiert haben, und führen Sie **Dell_OpenManage_Integration.exe** aus.

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

Die unterstützte Server-BS-Version 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 das Gerät laden, zugreifen kann.

4 Starten Sie den **VMware vSphere Web Client**.

5 Wählen Sie im **VMware vSphere-Web-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 Führen Sie im Fenster **Quelle auswählen** die folgenden Unteraufgaben aus:

a Wählen Sie **URL** aus, wenn Sie das OVF-Paket aus dem Internet herunterladen möchten.

b Wählen Sie die **Lokale Datei** aus und klicken Sie auf **Durchsuchen**, wenn Sie das OVF-Paket auf Ihrem lokalen System auswählen möchten.

ANMERKUNG: Der Installationsvorgang kann 10 bis 30 Minuten dauern, wenn sich das OVF-Paket auf einer Netzwerkfreigabe befindet. Für eine schnellstmögliche Installation wird empfohlen, die OVF-Datei auf einem lokalen Laufwerk zu hosten.

7 Klicken Sie auf **Weiter**.

Das Fenster **Details überprüfen** wird mit den folgenden Informationen angezeigt:

- **Produkt**: Der Name der OVF-Vorlage wird angezeigt.
- **Version**: Die Version der OVF-Vorlage wird angezeigt.
- **Hersteller**: Der Name des Anbieters wird angezeigt.
- **Publisher**: Der Name des Herausgebers wird angezeigt.
- **Download-Größe**: Die tatsächliche Größe der OVF-Vorlage in Gigabyte wird angezeigt.
- **Größe auf Festplatte**: Details über breite und schlanke Bereitstellung werden angezeigt.
- **Beschreibung**: Die Kommentare werden hier angezeigt.

8 Klicken Sie auf **Weiter**.

Das Fenster **Name und Verzeichnis anzeigen** wird angezeigt.

9 Führen Sie im Fenster **Name und Verzeichnis** folgende Unterschritte aus:

a Geben Sie im Textfeld **Name** den Namen der Vorlage ein. Der Benutzername kann aus bis zu 80 Zeichen bestehen.

b Wählen Sie aus der Liste **Verzeichnis oder Datenzentrum auswählen** einen Speicherort aus, um die Vorlage bereitzustellen.

10 Klicken Sie auf **Weiter**.

Das Fenster **Speicher auswählen** wird angezeigt.

11 Führen Sie im Fenster **Speicher auswählen** die folgenden Unterschritte aus:

a In der Dropdown-Liste **Formatieren der virtuellen Festplatte** wählen Sie 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.

12 Klicken Sie auf **Weiter**.

Das Fenster **Netzwerke einrichten**, das Einzelheiten über die Quelle und Zielnetzwerke enthält, wird angezeigt.

13 Klicken Sie im Fenster **Setup-Netzwerke** auf **Weiter**.

ANMERKUNG: Es wird empfohlen, dass sich OMIVV und der vCenter-Server im selben Netzwerk befinden.

14 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 ein Fenster mit dem Status der Fertigstellung an, in dem Sie den Fortschritt der Aufgabe verfolgen können.

Erstellen einer Zertifikatsignierungsanforderung

Voraussetzung

Stellen Sie sicher, dass Sie das Zertifikat vor der Registrierung von OMIVV mit dem vCenter hochladen.

Info über diese Aufgabe

Das Erzeugen einer Zertifikatsignierungsanforderung (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. Klicken Sie zum Fortsetzen der Anforderung auf **Weiter** oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

2 Wenn Sie mit der Anforderung fortfahren, geben Sie im Dialogfeld **ZERTIFIKATSIGNIERUNGSANFORDERUNG ERSTELLEN** den **allgemeinen Namen**, den **Organisationsnamen**, die **Organisationseinheit**, den **Standort**, den **Staatsnamen**, das **Land** und die **E-Mail** für die Anforderung ein. Klicken Sie auf **Continue** (Weiter).

3 Klicken Sie auf **Herunterladen**, dann speichern Sie die resultierende Zertifikatsanforderung an einem zugänglichen Speicherort.

HTTPS-Zertifikat hochladen

Voraussetzung

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

Info über diese Aufgabe

Die HTTPS-Zertifikate werden für die sichere Kommunikation zwischen dem virtuellen Gerät und Hostsystemen verwendet. Um diese sichere Kommunikation einzurichten, muss eine CSR an eine Zertifizierungsstelle gesendet werden, dann wird das resultierende Zertifikat mithilfe der Administration Console hochgeladen. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

ANMERKUNG: Sie können entweder den Microsoft Internet Explorer, Firefox oder Chrome verwenden, um Zertifikate hochzuladen.

Schritte

1 Klicken Sie auf der Seite **GERÄTE-MANAGEMENT** auf **Zertifikat hochladen** im Bereich **HTTPS-ZERTIFIKATE**.

2 Klicken Sie auf **OK** im Dialogfeld **ZERTIFIKAT HOCHLADEN**.

3 Klicken Sie zum Auswählen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.

4 Klicken Sie auf **Abbrechen**, wenn Sie das Hochladen abbrechen möchten.

ANMERKUNG: Wenn Sie für das Gerät ein benutzerdefiniertes Zertifikat hochgeladen haben, laden Sie vor der vCenter-Registrierung das neue Zertifikat hoch. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden im Web-Client Kommunikationsfehler angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung von vCenter rückgängig machen und sich erneut registrieren.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats

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**.

Registrieren eines vCenter Servers durch einen Nicht-Administratorbenutzer

Sie können vCenter Server für das OMIVV Gerät mit vCenter Administrator-Anmeldeinformationen oder mit einem Nicht-Administrator-Benutzer mit den Dell Berechtigungen registrieren.

Info über diese Aufgabe

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

Schritte

1 Zum Ändern der für eine Rolle ausgewählten Berechtigungen fügen Sie die Rolle hinzu und wählen Sie die erforderlichen Berechtigungen für die Rolle aus oder ändern Sie eine vorhandene Rolle.

In der VMware vSphere-Dokumentation finden Sie die erforderlichen Schritte zum Erstellen/Ändern einer Rolle und zur Auswahl von Berechtigungen im vSphere Webclient. Details zur Auswahl aller erforderlichen Berechtigungen für die Rolle finden Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Benutzer.

ANMERKUNG: Der vCenter Administrator muss eine Rolle hinzufügen oder ändern.

2 Weisen Sie einen Benutzer zu der neu erstellten Rolle zu, nachdem Sie eine Rolle definiert und Berechtigungen für die Rolle ausgewählt haben.

In der VMware vSphere Dokumentation finden Sie weitere Informationen über das Zuweisen von Berechtigungen im vSphere Webclient.

ANMERKUNG: Der vCenter Administrator muss im vSphere Client Berechtigungen zuweisen.

Ein Nicht-Administrator-Benutzer von vCenter Server mit den erforderlichen Berechtigungen kann jetzt vCenter registrieren und/oder die Registrierung aufheben, Anmeldeinformationen ändern oder das Zertifikat aktualisieren.

3 Registrieren Sie einen vCenter Server mit einem Nicht-Administrator-Benutzer mit den erforderlichen Berechtigungen.

4 Weisen Sie der in Schritt 1 erstellten oder bearbeiteten Rolle Dell-Berechtigungen zu. Siehe Zuweisen von Dell Berechtigungen zur Rolle im vSphere Webclient.

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

Erforderliche Berechtigungen für Nicht-Administrator-Benutzer

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

ANMERKUNG: Beim Registrieren eines vCenter Servers mit OMIVV durch einen Nicht-Administrator-Benutzer wird eine Fehlermeldung 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

ANMERKUNG: Weisen Sie die folgenden Berechtigungen für die Funktionszustandsaktualisierung zu, wenn Sie VMware vCenter 6.5 verwenden oder auf vCenter 6.5 oder höher aktualisieren:

- Funktionszustand-Update-Anbieter
  - Registrieren
  - Registrierung aufheben
  - Aktualisierung
- Host
  - CIM
    - CIM-Interaktion
  - Konfiguration
    - Erweiterte Einstellungen
    - Verbindung
    - Wartung
    - Netzwerkkonfiguration
    - Abfragen von Patches

- Sicherheitsprofil und Firewall

ANMERKUNG: Weisen Sie die folgenden Berechtigungen zu, wenn Sie VMware vCenter 6.5 verwenden oder auf vCenter 6.5 oder höher aktualisieren:

- Host-Konfig.
  - Erweiterte Einstellungen
  - Verbindung
  - Wartung
  - Netzwerkkonfiguration
  - Abfragen von Patches
  - Sicherheitsprofil und Firewall

– Bestandsaufnahme
  - Hinzufügen von Hosts zu einem Cluster
  - Hinzufügen von eigenständigen Hosts
  - Cluster ändern

ANMERKUNG: Stellen Sie sicher, dass Sie die Berechtigung zum Ändern des Clusters zuweisen, wenn Sie vCenter 6.5 verwenden oder eine Aktualisierung auf vCenter 6.5 oder höher durchführen.

- Hostprofil
  – Bearbeiten
  – Ansicht
- Berechtigungen
  – Ändern von Berechtigungen
  – Ändern einer Rolle
- Sitzungen
  – Validieren einer Sitzung
- Task
  – Erstellen von Tasks
  – Aktualisieren von Tasks

ANMERKUNG: Wenn ein Nicht-Administratorbenutzer versucht, einen vCenter Server zu registrieren, ist es zwingend erforderlich, Dell Berechtigungen zu der vorhandenen Rolle hinzuzufügen. Weitere Informationen über das Zuweisen von Dell Berechtigungen finden Sie unter Dell Berechtigungen vorhandener Rolle zuweisen.

Registrieren von vCenter Server durch Nicht-Administrator - Benutzer mit den erforderlichen Berechtigungen

Sie können vCenter-Server für das OMIVV-Gerät mit einem Nicht-Administrator-Benutzer mit den erforderlichen Berechtigungen registrieren. Siehe Schritt 5 bis Schritt 9 in **Registrieren von OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei**. für Informationen zum Registrieren eines vCenter-Servers über einen Benutzer, der kein Administrator ist, oder als Administrator.

Dell Berechtigungen vorhandener Rolle zuweisen

Info über diese Aufgabe

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

ANMERKUNG: Stellen Sie sicher, dass Sie als Benutzer mit Administratorrechten angemeldet sind.

Schritte

1 Melden Sie sich mit Administratorrechten beim vSphere Web Client an.

2 Klicken Sie im vSphere Web-Client im linken Fensterbereich auf **Verwaltung → Rollen**.

3 Wählen Sie ein vCenter Serversystem aus der Dropdownliste **Rollenanbieter** aus.

4 Wählen Sie die Rolle aus der Liste **Rollen** aus und klicken sie auf .

5 Klicken Sie auf **Berechtigungen**, erweitern Sie **Dell** und wählen Sie die folgenden Dell Berechtigungen für die ausgewählte Rolle aus. Klicken Sie anschließend auf **OK**:

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

Siehe Sicherheitsrollen und Berechtigungen im *OpenManage Integration for VMware vCenter User's Guide* (OpenManage Integration for VMware vCenter-Benutzerhandbuch), das unter **Dell.com/support/manuals** verfügbar ist, um weitere Informationen über die verfügbaren OMIVV-Rollen innerhalb von vCenter zu erhalten.

Die Änderungen an Berechtigungen und Rollen werden sofort wirksam. Der Benutzer mit erforderlichen Berechtigungen kann nun die OpenManage Integration für VMware vCenter Vorgänge durchführen.

ANMERKUNG: Für alle vCenter Operations verwendet OMIVV die Berechtigungen des registrieren Benutzers und nicht die Berechtigungen des angemeldeten Benutzers.

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

Registrieren der OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei

Voraussetzung

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

ANMERKUNG: Wenn Sie für Ihr Gerät ein benutzerdefiniertes Zertifikat hochgeladen haben, laden Sie vor der vCenter-Registrierung das neue Zertifikat hoch. Wenn Sie das neue benutzerdefinierte Zertifikat nach der vCenter-Registrierung hochladen, werden im Web-Client Kommunikationsfehler angezeigt. Um dieses Problem zu beheben, müssen Sie die Registrierung von vCenter rückgängig machen und sich erneut registrieren.

Schritte

1 Klicken Sie im vSphere-Web-Client auf **Startseite** > **Hosts und Cluster**, suchen Sie dann im linken Fenster das gerade bereitgestellte OMIVV und klicken Sie auf **Virtuelle Maschine einschalten**.

Während der Bereitstellung wird die VM automatisch nach Abschluss der Bereitstellung eingeschaltet, wenn Sie **Nach Bereitstellung einschalten** auswählen.

2 Zum Ausführen der **Verwaltungskonsole** klicken Sie auf die Registerkarte **Konsole** im Hauptfenster **VMware vCenter**.

3 Warten Sie, bis OMIVV vollständig gestartet wurde, und geben Sie dann den Benutzernamen **Admin** ein (die Standardeinstellung lautet „Admin“) und drücken Sie die **Eingabetaste**.

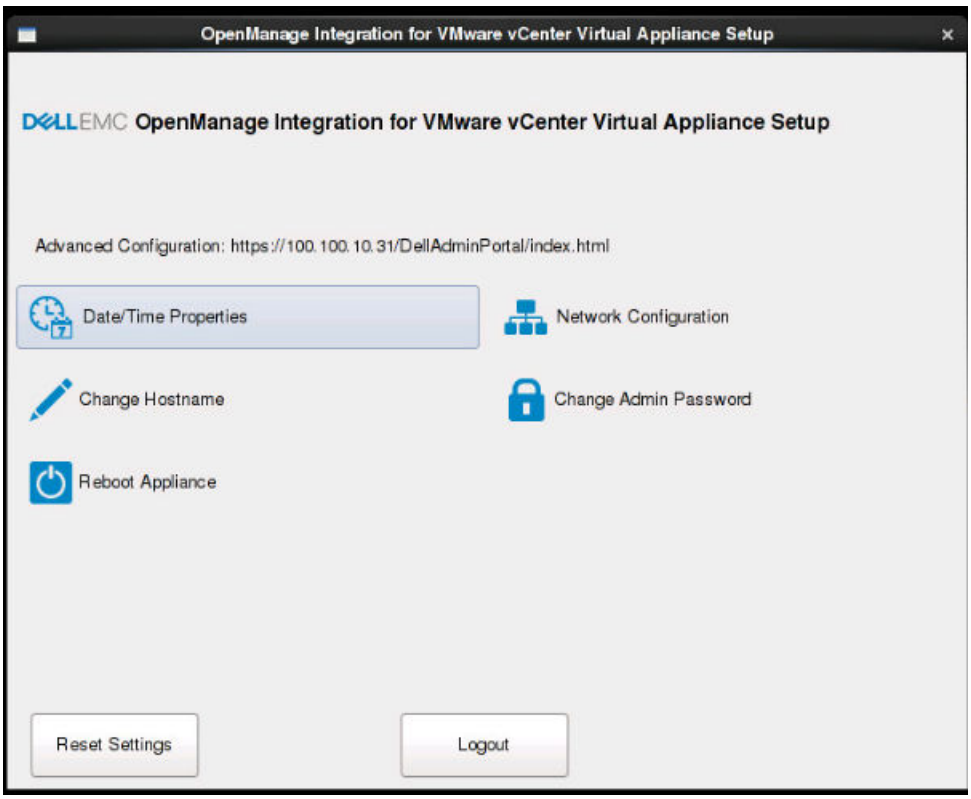
4 Geben Sie ein neues Administratorkennwort ein. Stellen Sie sicher, dass das Administratorkennwort den Kennwörter-Komplexitätsanforderungen entspricht, die in der Befehlszeilenschnittstelle angezeigt werden. Drücken Sie die **Eingabetaste.**

5 Geben Sie das Kennwort, das Sie zuvor eingegeben haben, erneut ein und drücken Sie die **Eingabetaste**.

Drücken Sie die **Eingabetaste** , um die Konfiguration der Netzwerk- und Zeitzoneninformationen im OMIVV-Gerät vorzunehmen.

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

Abbildung 1. Registerkarte „Konsole“



7 Wählen Sie auf der Registerkarte **Datum und Uhrzeit Datum und Uhrzeit über das Netzwerk synchronisieren**.
Das Feld **NTP-Server** wird angezeigt.

8 Fügen Sie die gültigen NTP-Server-Informationen hinzu, mit denen Ihr vCenter synchronisiert ist.

9 Klicken Sie auf **Zeitzone** und wählen Sie die entsprechende Zeitzone aus und klicken Sie auf **OK**.

10 Klicken Sie zum Konfigurieren der statischen IP zum OMIVV-Gerät auf **Netzwerkkonfiguration** oder fahren Sie mit Schritt 17 fort.

11 Wählen Sie **Auto eth0** aus, und klicken Sie dann auf **Bearbeiten**.

12 Wählen Sie die Registerkarte **IPv4-Einstellungen** und dann **Manuell** in der Dropdown-Liste **Methode** aus.

13 Klicken Sie auf **Hinzufügen** und fügen Sie eine gültige IP-Adresse, Netzmaske und Gateway-Informationen hinzu.

14 Im Feld **DNS-Server** stellen Sie die Details zum DNS-Server bereit.

15 Klicken Sie auf **Anwenden**.

16 Klicken Sie zum Ändern des Hostnamens des OMIVV-Geräts auf **Hostnamen ändern**.

17 Geben Sie einen gültigen Hostnamen ein und klicken Sie auf **Hostnamen aktualisieren**.

ANMERKUNG: Nachdem Hostnamen und NTP geändert wurden, muss das System neu gestartet werden.

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

Vor dem Öffnen der Verwaltungskonsole stellen Sie sicher, dass Sie manuell alle Bezüge auf das Gerät wie z. B. Bereitstellungsserver in iDRAC, DRM aktualisieren.

18 Öffnen Sie die **Verwaltungskonsole** von einem unterstützten Browser aus.
Um die **Verwaltungskonsole** in der Registerkarte **Hilfe und Support** von OpenManage Integration for VMware vCenter zu öffnen, klicken Sie auf den Link unter **Verwaltungskonsole** oder starten Sie einen Web-Browser und geben Sie die URL **https://<ApplianceIP or Appliance hostname>** ein.

Die IP-Adresse ist die IP-Adresse der Geräte-VM und nicht die IP-Adresse des ESXi-Hosts. Sie können über die oben in der Konsole angezeigte URL auf die Verwaltungskonsole zugreifen.

Zum Beispiel: **https://10.210.126.120** oder **https://myesxihost**

Die URL unterscheidet nicht zwischen Groß- und Kleinschreibung.

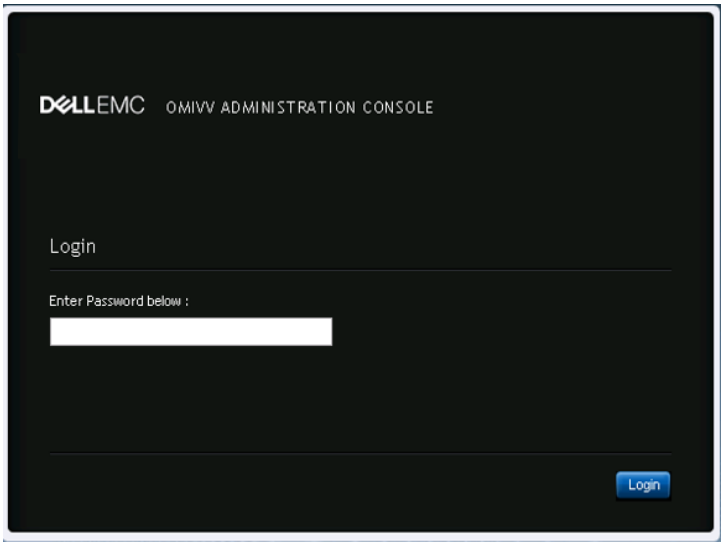


Abbildung 2. Verwaltungskonsole

19 Geben Sie im Anmeldefenster der **Verwaltungskonsole** das Kennwort ein und klicken Sie dann auf **Anmelden**.

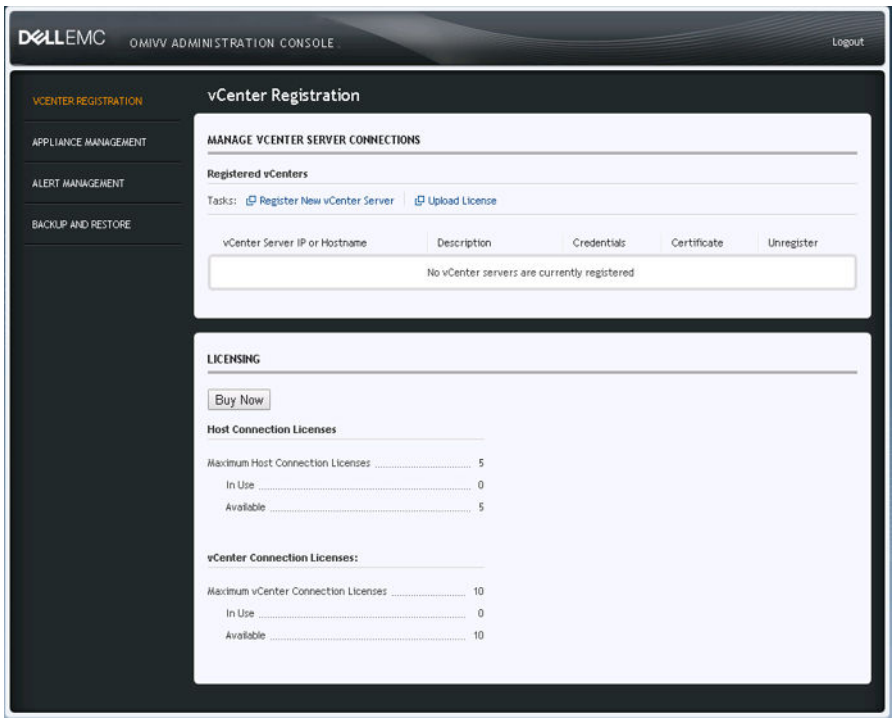


Abbildung 3. vCenter-Registrierungsfenster innerhalb der Verwaltungskonsole

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

21 Führen Sie im Fenster **Neuen vCenter-Server registrieren** die folgenden Unterschritte aus:

a Geben Sie unter **vCenter-Name** im Textfeld **IP oder Hostname des vCenter-Servers** die IP oder den Hostnamen des Servers und anschließend in das Textfeld **Beschreibung** eine Beschreibung ein.

Die Beschreibung ist optional.

ANMERKUNG: Es wird empfohlen, die OpenManage Integration für VMware vCenter mit einem vollständig qualifizierten Domänennamen (FQDN) im VMware vCenter zu registrieren. Achten Sie darauf, dass der Hostname des vCenter vom DNS-Server für FQDN-basierte Registrierungen korrekt aufgelöst werden kann.

b Unter **vCenter Benutzerkonto** in **vCenter Benutzername** geben Sie den Admin-Benutzernamen ein oder den Benutzernamen, der über die erforderlichen Berechtigungen verfügt.

Geben Sie den **Benutzernamen** als Domäne\Benutzer oder Domäne/Benutzer oder Benutzer@Domäne ein. OMIVV verwendet für die Verwaltung von vCenter das Administratorkonto oder ein Benutzerkonto mit den erforderlichen Berechtigungen.

c Geben Sie in **Kennwort** das Kennwort ein.

d Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.

22 Klicken Sie auf **Registrieren**.

ANMERKUNG: OpenManage Integration for VMware vCenter unterstützt derzeit bis zu 1000 Hosts für große Einsatzmodus mit einer einzigen vCenter-Instanz oder mehrere vCenter-Server mithilfe des verknüpften Modus.

23 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 von Dell Digital Locker unter http://www.dell.com/support/licensing heruntergeladen werden und Sie können diese Lizenz in Ihr virtuelles Gerät importieren. Klicken Sie zum Importieren der Lizenzdatei auf **Lizenz hochladen**.

24 Klicken Sie im Fenster **Lizenz hochladen** auf **Durchsuchen**, um zur Lizenzdatei zu wechseln und klicken Sie anschließend auf **Hochladen**, um die Lizenzdatei zu importieren.

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 auf www.dell.com/support/softwarecontacts.

Sobald OMIVV registriert ist, wird das OMIVV-Symbol unter der Kategorie **Verwaltung** auf der Web Client-Startseite angezeigt.

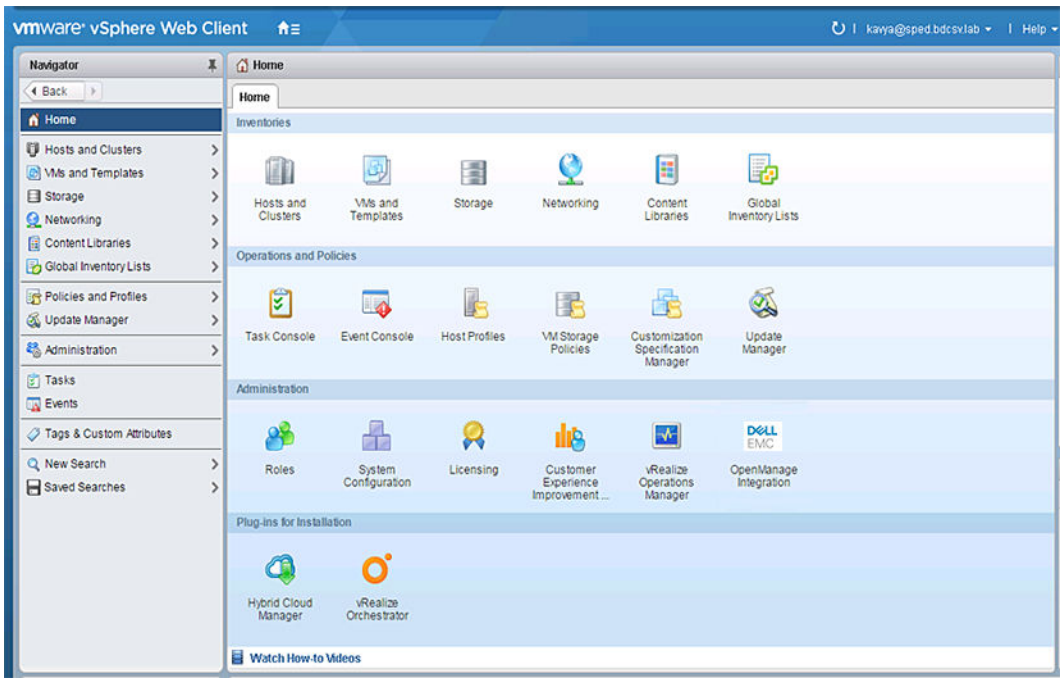


Abbildung 4. OpenManage Integration for VMware vCenter wurde erfolgreich zum vCenter hinzugefügt

Beispiel

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

Beispiel: Benutzer X mit ausreichender Berechtigung registriert OMIVV mit vCenter und Benutzer Y verfügt nur über Dell Berechtigungen. Benutzer Y kann sich nun bei VCenter anmelden und ein Firmware-Update von OMIVV auslösen. Während das Update durchgeführt wird, nutzt OMIVV die Berechtigungen von Benutzer X, damit das Gerät in den Wartungsmodus versetzt werden kann oder der Host erneut gestartet werden kann.

Aktualisieren eines registrierten vCenters

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

- Für Nicht-Administratorbenutzer:
  a. Weisen Sie Nicht-Administratorbenutzern bei Bedarf zusätzliche Berechtigungen zu. Informationen dazu finden Sie unter Erforderliche Berechtigungen für Nicht-Administrator-Benutzer.

     Weisen Sie die zusätzlichen Berechtigungen zum Beispiel zu, wenn Sie eine Aktualisierung von vCenter 6.0 auf vCenter 6.5 durchführen.
  b. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.
- Für Administratorbenutzer:
  a. Führen Sie einen Neustart des registrierten OMIVV-Geräts durch.

Überprüfen der Installation

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 Web-Client.
2. Bestätigen Sie, dass das OMIVV-Symbol im vSphere Web-Client angezeigt wird.
3. Stellen Sie sicher, dass vCenter mit OMIVV kommunizieren kann, indem Sie einen Ping-Befehl vom vCenter-Server zur IP-Adresse oder dem Hostnamen des virtuellen Geräts senden.
4. Klicken Sie in vSphere Web Client auf **Start** > **Administration** > **Lösungen** und dann auf **Plug-in-Verwaltung** (in älteren vCenter-Versionen) oder **Client-Plug-ins** (in neueren Versionen).

   Weitere Informationen über die Zugriffsbeschränkungen für die Seite **Plug-in-Verwaltung** oder **Client-Plug-ins** finden Sie in der VMware Dokumentation.
5. Überprüfen Sie im Fenster **Plug-in-Verwaltung** oder **Client-Plug-ins**, ob OMIVV installiert und aktiviert ist.

Aktualisieren des Repository-Speicherorts des virtuellen Geräts und des virtuellen Geräts

Voraussetzung

Um sicherzustellen, dass alle Daten geschützt sind, führen Sie eine Sicherung der OMIVV-Datenbank vor dem Aktualisieren des virtuellen Geräts aus. Siehe das Thema **Verwalten von Backups und Wiederherstellungen** im Benutzerhandbuch.

Schritte

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

ANMERKUNG: Das OMIVV-Gerät benötigt eine Internetverbindung, um verfügbare Aktualisierungsmechanismen anzuzeigen und die RPM-Aktualisierung durchzuführen. Stellen Sie sicher, dass das OMIVV-Gerät über eine Internetverbindung verfügt. Abhängig von Ihren Netzwerkeinstellungen müssen Sie Proxy aktivieren und Proxy-Einstellungen bereitstellen, wenn Ihr Netzwerk Proxy benötigt. Siehe das Thema Einrichten des HTTP-Proxy im *Benutzerhandbuch* – .

ANMERKUNG: Stellen Sie sicher, dass Repository-Pfad aktualisieren gültig ist.

Für die verfügbare Version des virtuellen Geräts werden entsprechenden RPM- und OVF-Aktualisierungsmechanismen mit einem Häkchen angezeigt. Im folgenden werden die möglichen Optionen des Aktualisierungsmechanismus dargestellt und Sie können eine dieser Optionen für den Aktualisierungsmechanismus durchführen:

- Wenn ein Häkchen neben RPM angezeigt wird, können Sie eine RPM-Aktualisierung von der vorhandenen Version auf die neueste verfügbare Version durchführen. Siehe Durchführen einer Aktualisierung von einer vorhandenen Version auf die neueste Version.
- 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 Geräteversion ausführen. Siehe Aktualisieren des Geräts durch Sichern und Wiederherstellen.
- Wenn ein Häkchen neben RPM und OVF angezeigt wird, können Sie eine der genannten Optionen zur Aktualisierung Ihres Geräts ausführen. In diesem Szenario ist die empfohlene Option die RPM-Aktualisierung.

2 Zur Aktualisierung des virtuellen Geräts führen Sie die genannten Aufgaben den Upgrade-Mechanismen durch, je nach Version von OMIVV.

ANMERKUNG: Stellen Sie sicher, dass Sie sich von allen Webclient-Sitzungen an den registrierten vCenter-Servern abmelden.

ANMERKUNG: Stellen Sie vor der Anmeldung an einem registrierten vCenter-Server sicher, dass Sie alle Geräte gleichzeitig unter dem gleichen Plattform Service Controller (PSC) aktualisieren. Andernfalls werden möglicherweise inkonsistente Informationen in den OMIVV-Instanzen angezeigt.

3 Klicken Sie auf **GERÄTEMANAGEMENT** und überprüfen Sie die Aktualisierungsmechanismen.

OMIVV aus vorhandener Version auf aktuelle Version aktualisieren

1 Aktivieren Sie auf der Seite **GERÄTEMANAGEMENT** die Option „Proxy“ entsprechend Ihren Netzwerkeinstellungen und richten Sie die „Proxy-Einstellungen“ ein, wenn Ihr Netzwerk Proxy benötigt. Siehe **Einrichten des HTTP-Proxy** im *Benutzerhandbuch*.

2 Zur Aktualisierung des OpenManage Integration Plug-ins von einer vorhandenen Version auf die aktuelle 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 den 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**.
- Zur Aktualisierung der neuesten heruntergeladenen RPM-Ordner oder -Dateien, wenn keine Internetverbindung vorhanden ist, laden Sie alle Dateien und Ordner über den Pfad https://linux.dell.com/repo/hardware/vcenter-plugin-x64/latest/ herunter und kopieren Sie sie auf eine HTTP-Freigabe.

  Klicken Sie im Fenster **Geräteverwaltung** im Bereich **Geräteaktualisierung** auf **Bearbeiten** und fügen Sie dann im Textfeld **Repository-Pfad aktualisieren** den Pfad für die Offline-HTTP-Freigabe ein und klicken Sie auf **Anwenden**.

3 Vergleichen Sie die verfügbare virtuelle Geräteversion und die aktuelle virtuelle Geräteversion und stellen Sie sicher, dass die verfügbare virtuelle Geräteversion größer ist als die aktuelle virtuelle Geräteversion.

4 Klicken Sie unter **Geräteeinstellungen** auf **Virtuelles Gerät aktualisieren**, um die Aktualisierung des virtuellen 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.

ANMERKUNG: Während des Upgrade-Vorgangs wird das Gerät ein- oder zweimal neu gestartet.

ANMERKUNG: Sobald das Gerät RPM-aktualisiert ist, führen Sie Folgendes aus:

- Leeren Sie den Browser-Cache bevor Sie sich beim Dell Administratorportal anmelden.
- Installieren Sie die VMware-Tools neu.
  Für die Neuinstallation der VMware-Tools:
  a Klicken Sie mit der rechten Maustaste auf das OMIVV-Gerät.
  b Bewegen Sie den Mauszeiger über **Gast** und klicken Sie dann auf **VMware-Tools installieren/aktualisieren**.
  c Klicken Sie im Dialogfeld **VMware-Tools installieren/aktualisieren** auf **Automatische Tool-Aktualisierung** und klicken Sie dann auf **OK**.
  Sie können den Installationsstatus in **Letzte Aufgaben** sehen.

ANMERKUNG: 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 virtuellen Geräte gleich sind. Wenn Sie die proaktive HA auf Clustern aktiviert haben, hebt OMIVV die Registrierung des Dell Inc. Providers für diese Cluster auf und registriert den Dell Inc. Provider nach dem Aktualisieren erneut. Das heißt, Funktionszustandaktualisierungen für Dell EMC Hosts stehen erst dann zur Verfügung, wenn die Aktualisierung abgeschlossen ist.

Aktualisieren des Geräts durch Sichern und Wiederherstellen

Info über diese Aufgabe

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

Schritte

1 Sichern Sie die Datenbank für die ältere Version.
2 Deaktivieren Sie das ältere OMIVV-Gerät im vCenter.

ANMERKUNG: Heben Sie die Registrierung des OMIVV-Plug-ins von vCenter nicht auf. Das Aufheben der Registrierung des Plug-ins in vCenter entfernt alle durch das OMIVV-Plug-in auf vCenter registrierten Alarme und alle Anpassungen an den Alarmen, wie Maßnahmen usw.

3 Stellen Sie das neue OpenManage Integration-Gerät OVF bereit.
4 Starten Sie das neue OpenManage Integration-Gerät.
5 Richten Sie für das neue Gerät das Netzwerk, die Zeitzone usw. ein.

ANMERKUNG: Stellen Sie sicher, dass die neue OpenManage Integration Version dieselbe IP-Adresse, wie das alte Gerät hat.

ANMERKUNG: Das OMIVV-Plug-in kann möglicherweise nicht richtig ausgeführt werden, wenn die IP-Adresse für das neue Gerät sich von der IP-Adresse des älteren Geräts unterscheidet. In einem solchen Fall müssen Sie die Registrierung aller vCenter-Instanzen rückgängig machen und sie dann neu registrieren.

6 Im Lieferumfang des OMIVV-Geräts ist ein Standardzertifikat enthalten. Wenn Sie ein benutzerdefiniertes Zertifikat für Ihr Gerät möchten, aktualisieren Sie dasselbe. Siehe Erstellen einer Zertifikatsignierungsanforderung und HTTPS-Zertifikat hochladen. Andernfalls überspringen Sie diesen Schritt.
7 Stellen Sie die Datenbank auf dem neuen OMIVV-Gerät wieder her. Siehe **Wiederherstellen der OMIVV-Datenbank aus einem Backup** im *Benutzerhandbuch*.
8 Überprüfen des Geräts. Siehe Installationsprüfung im *Installationshandbuch zu OpenManage Integration for VMware vCenter*, das unter Dell.com/support/manuals bereitgestellt wird.
9 Führen Sie die **Bestandsaufnahme** auf allen registrierten vCenter-Servern aus.

ANMERKUNG: Dell EMC empfiehlt, dass Sie nach der Aktualisierung die Bestandsaufnahme erneut auf allen Hosts durchführen, die vom Plug-in verwaltet werden. Informationen zum Ausführen der Bestandsaufnahme nach Bedarf finden Sie im Planen von Bestandsaufnahme-Jobs.

ANMERKUNG: Wenn die IP-Adresse der neuen OMIVV-Version y von der OMIVV-Version x geändert wird, konfigurieren Sie das Trap-Ziel für die SNMP-Traps so, dass es sich über dem neuen Gerät befindet. Für Server der 12. Generation und höher wird die IP-Änderung durch Ausführung der Bestandsaufname auf diesen Hosts korrigiert. Während der Ausführung der Bestandsaufnahme auf Hosts der 12. Generation werden diese Hosts, falls sich die SNMP-Traps nicht über der neuen IP befinden, als nicht konform aufgelistet. Bei Hosts vor der 12. Generation, die mit früheren Versionen kompatibel waren, wird die IP-Änderung als nicht konform angezeigt und Sie müssen Dell EMC OpenManage Server Administrator (OMSA) konfigurieren. Zum Beheben von Konformitätsproblemen bei vSphere-Hosts lesen Sie Ausführen des Assistenten zum Beheben von nicht konformen vSphere-Hosts im *Benutzerhandbuch* .

ANMERKUNG: Nach der Sicherung und Wiederherstellung von einer früheren OMIVV-Version auf eine neuere OMIVV-Version gehen Sie wie folgt vor, wenn Sie zwei Millionen Fehler sehen oder das Dell EMC Logo nicht in vCenter angezeigt wird:

- Starten Sie den vSphere Web-Client-Service auf dem vCenter Server neu.
- Wenn das Problem weiterhin besteht:
  - Um zu VMware vCenter Server Appliance zu gelangen, gehen Sie zu **/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity** und um zu Windows vCenter zu gelangen, gehen Sie in den Ordner **C:\ProgramData\VMware \vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity** im vCenter Gerät und prüfen Sie, ob alte Daten vorhanden sind, wie beispielsweise: com.dell.plugin.OpenManage_Integration_for_VMware_vCenter_WebClient-X. 0.0.XXX.
  - Löschen Sie den Ordner für die frühere OMIVV-Version manuell.

Wiederherstellen von OMIVV, 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: Das Aufheben der Plug-in-Registrierung entfernt alle benutzerdefinierten Einstellungen der registrierten Alarme des Plug-ins. Die folgenden Schritte stellen die benutzerdefinierten Einstellungen nicht wieder her. Sie registrieren aber erneut die Alarme mit ihren Standardeinstellungen.

Schritte

1. Führen Sie Schritt 3 bis Schritt 5 unter Aktualisieren des Geräts durch Sichern und Wiederherstellen aus.
2. Registrieren Sie das Plugin auf demselben vCenter, auf dem Sie zuvor das frühere Plugin registriert hatten.
3. Um die Migration abzuschließen, führen Sie Schritt 6 bis Schritt 9 unter Aktualisieren des Geräts durch Sichern und Wiederherstellen aus.

2

Gerätekonfiguration für VMware vCenter

Nachdem Sie die grundlegende Installation von OMIVV und die Registrierung der vCenter abgeschlossen haben, wird der **Erstkonfigurationsassistent** angezeigt, wenn Sie auf das OMIVV-Symbol klicken. Sie können damit fortfahren, Geräte unter Verwendung eines der folgenden Verfahren zu konfigurieren:

- Konfigurieren des Geräts mit dem **Erstkonfigurationsassistenten**
- Konfigurieren des Geräts über die Registerkarte **Einstellungen** in OMIVV.

Sie können den **Erstkonfigurationsassistenten** zum Konfigurieren der OMIVV-Geräteeinstellungen beim ersten Start verwenden. Für nachfolgende Instanzen verwenden Sie die Registerkarte **Einstellungen**.

ANMERKUNG: Die Benutzeroberfläche ist bei beiden Methoden ähnlich.

Themen:

Konfigurationstasks im Konfigurationsassistenten

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

Unter Verwendung des Konfigurations-Assistenten können Sie die folgenden Aufgaben anzeigen und ausführen:

- Willkommens-Seite im Konfigurationsassistenten anzeigen.
- Wählen Sie vCenter aus. Siehe Auswählen von vCenters.
- Erstellen Sie ein neues Verbindungsprofil. Siehe Erstellen eines neuen Verbindungsprofils.
- Erstellen Sie ein Gehäuseprofil. Die in einem MX-Gehäuse mit einem deaktivierten iDRAC IPv4 vorhandenen Hosts müssen über ein Gehäuseprofil verwaltet werden. Informationen dazu finden Sie unter Erstellen eines Gehäuse-Profils.
- Konfigurieren von Ereignissen und Alarmen. Siehe Konfigurieren von Ereignissen und Alarmen.
- Planen Sie Bestandsaufnahme-Jobs. Siehe Planen von Bestandsaufnahme-Jobs.
- Führen Sie einen Serviceabfrage-Job aus. Siehe Ausführen eines Serviceabfrage-Jobs.

Anzeigen des Begrüßungsdialogs des Konfigurationsassistenten

Um OMIVV nach dem Installieren und Registrieren im vCenter zu konfigurieren, führen Sie folgende Schritte durch, um den **Erstkonfigurationsassistenten** anzuzeigen:

1 Klicken Sie im vSphere Web-Client auf die **Startseite** und dann auf das Symbol **OpenManage Integration.**

Sie können eine der folgenden Optionen für den Zugriff auf den Erstkonfigurationsassistenten verwenden:

- Wenn Sie das erste Mal auf das Symbol für **OpenManage Integration** klicken, wird der **Erstkonfigurationsassistent** automatisch angezeigt.

- Klicken Sie unter **OpenManage Integration** > **Erste Schritte** auf **Erstkonfigurationsassistenten starten**.

2 Überprüfen Sie im Dialogfeld **Willkommen** die Schritte, und klicken Sie dann auf **Weiter**.

Auswählen der vCenter

Info über diese Aufgabe

Im Dialogfeld **vCenter-Auswahl** können Sie die folgenden vCenter konfigurieren:

- Ein spezifisches vCenter
- Alle registrierten vCenter

So zeigen Sie das Dialogfeld **vCenter-Auswahl** an:

Schritte

1 Klicken Sie im **Erstkonfigurationsassistent** im Dialogfeld **Willkommen** auf **Weiter**.

2 Wählen Sie ein oder alle registrierten vCenter aus der **vCenter**-Dropdown-Liste aus.

Wählen Sie ein vCenter, das noch nicht konfiguriert wurde bzw. wenn Sie der Umgebung ein vCenter hinzugefügt haben. Die vCenter-Auswahlseite ermöglicht Ihnen die Auswahl eines oder mehrerer vCenter zur Konfiguration Ihrer Einstellungen.

3 Klicken Sie im Dialogfeld **Verbindungsprofilbeschreibung** auf **Weiter**.

ANMERKUNG: Wenn mehrere vCenter-Server als Bestandteil des gleichen SSO vorhanden sind und mit derselben OMIVV-Anwendung registriert sind und Sie die Konfiguration eines einzelnen vCenters ausgewählt haben, müssen Sie die Schritte 1 bis 3 wiederholen, bis Sie jedes vCenter konfiguriert haben.

Verbindungsprofil erstellen

Voraussetzungen

Bevor Sie die Active Directory-Anmeldeinformationen mit einem Verbindungsprofil verwenden, muss Folgendes sichergestellt werden:

- Das Active Directory-Benutzerkonto muss in Active Directory vorhanden sein.
- iDRAC und der Host müssen für die Active Directory-basierte Authentifizierung konfiguriert sein.

Info über diese Aufgabe

Ein Verbindungsprofil speichert die iDRAC- und Host-Anmeldeinformationen, die OMIVV für die Kommunikation mit Dell EMC Servern verwendet. Jeder Dell EMC Server muss einem Verbindungsprofil zugeordnet sein, damit er von OMIVV verwaltet werden kann. Sie können einem einzelnen Verbindungsprofil mehrere Server zuweisen. Sie können ein Verbindungsprofil mithilfe des Konfigurationsassistenten oder über die Registerkarte **OpenManage Integration for VMware vCenter** > **Einstellungen** erstellen. Sie können sich am iDRAC und dem Host mithilfe von Active Directory-Anmeldeinformationen anmelden.

ANMERKUNG: Die Active Directory-Anmeldeinformationen können werden entweder dieselben oder unterschiedlich für den iDRAC und den Host sein.

ANMERKUNG: Sie können ein Verbindungsprofil nicht erstellen, falls die Anzahl an hinzugefügten Hosts das Lizenzlimit zur Erstellung eines Verbindungsprofils überschreitet.

ANMERKUNG: Ein MX-Gehäuse-Host kann mit einer einzigen einheitlichen Chassis-Management-IP verwaltet werden. Informationen zur Verwaltung eines MX-Gehäuses unter Verwendung eines Gehäuse-Profils finden Sie unter Erstellen eines Gehäuse-Profils. Dell EMC empfiehlt das Verwalten eines MX-Gehäuse-Hosts mit einer iDRAC-IP, um die vollständigen OMIVV-Funktionen zu erhalten.

Schritte

1 Klicken Sie auf das Dialogfeld **Verbindungsprofilbeschreibung** auf **Weiter**.

2 Geben Sie im Dialogfeld **Name und Anmeldeinformationen des Verbindungsprofils** den **Profilnamen** der Verbindung und eine optionale **Beschreibung** des Verbindungsprofils ein.

3 Führen Sie im Dialogfeld **Name und Anmeldeinformationen des Verbindungsprofils** unter **iDRAC-Anmeldeinformationen**, abhängig davon, ob iDRAC mit oder ohne Active Directory konfiguriert werden soll, folgende Schritte aus:

ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, die Anwendung von Hardwareprofilen sowie von Systemprofilen bei Servern der 14. Generation und die Bereitstellung des Hypervisors.

- Für iDRAC-IPs, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, wählen Sie **Active Directory verwenden** aus. Anderenfalls scrollen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.
  1. Geben Sie unter Active Directory-**Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: **Domäne\Benutzername** oder benutzername@domäne. Der Benutzername darf maximal 256 Zeichen haben.
  2. Geben Sie unter Active Directory-**Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
  3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
  4. Führen Sie je nach Bedarf einen der folgenden Schritte aus:
     - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
     - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
- Zum Konfigurieren der iDRAC-Anmeldeinformationen ohne Active Directory führen Sie die folgenden Tasks aus:
  1. Geben Sie unter **Benutzername** den Benutzernamen ein. Der Benutzername ist auf 16 Zeichen beschränkt. Informationen zu Benutzernamen-Einschränkungen für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.
  2. Geben Sie im Feld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
  3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
  4. Führen Sie eine der folgenden Aktionen aus:
     - Um das iDRAC-Zertifikat herunterzuladen und zu speichern und es während aller zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
     - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

4. Führen Sie unter **Host-Root** einen der folgenden Schritte aus:
   - Für Hosts, auf denen Sie Active Directory benutzen möchten, und die für Active Directory bereits konfiguriert und aktiviert wurden, wählen Sie **Active Directory verwenden** aus. Anderenfalls führen Sie folgende Schritte zum Konfigurieren Ihrer Host-Anmeldeinformationen durch:
     1. Geben Sie unter Active Directory-**Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: **Domäne\Benutzername** oder benutzername@domäne. Der Benutzername ist auf 256 Zeichen beschränkt.

        ANMERKUNG: Siehe die folgenden Informationen zu Host-Benutzernamen und Domänen-Einschränkungen:

        Anforderungen für Host-Benutzernamen:

        - Zwischen 1 und 64 Zeichen lang
        - Keine nicht druckbaren Zeichen

        Host-Domänen-Anforderungen:

        - Zwischen 1 und 64 Zeichen lang
        - Das erste Zeichen muss ein alphabetisches Zeichen sein.
        - Leerzeichen sind nicht zulässig.
     2. Geben Sie unter Active Directory-**Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     3. Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.
     4. Führen Sie eine der folgenden Aktionen aus:
        - Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
        - Um das iDRAC-Zertifikat nicht zu speichern und dessen Prüfung während allen zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.
   - Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie die folgenden Tasks aus:
     1. Im Textfeld **Benutzername** lautet der Benutzername `root`. Dies ist der Standardbenutzername und Sie können ihn nicht ändern. Falls Active Directory eingestellt ist, können Sie einen beliebigen Active Directory-Benutzer auswählen, nicht nur root.

2 Geben Sie im Feld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für die ESXi-Hosts verwendet werden.

3 Geben Sie unter **Kennwort bestätigen** das Kennwort erneut ein.

4 Führen Sie eine der folgenden Aktionen aus:

- Um das Host-Zertifikat herunterzuladen und zu speichern und es während allen zukünftigen Verbindungen zu validieren, aktivieren Sie das Kontrollkästchen **Zertifikatprüfung aktivieren**.
- Um das Host-Zertifikat nicht zu speichern und dessen Prüfung während aller zukünftigen Verbindungen nicht auszuführen, heben Sie die Markierung des Kontrollkästchens **Zertifikatprüfung aktivieren** auf.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite **Dem Verbindungsprofil zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken auf **OK**.

ANMERKUNG: Wenn die OEM-Hosts nicht im Fenster „Hosts auswählen“ angezeigt werden, fügen Sie die Hosts mit dem Assistenten zum Hinzufügen von OEM-Hosts hinzu, siehe Hinzufügen von OEM-Hosts im *Benutzerhandbuch*.

7 Um das Verbindungsprofil zu prüfen, wählen Sie einen oder mehrere Hosts aus und klicken Sie auf **Verbindung testen**.

ANMERKUNG: Dieser Schritt ist optional und überprüft, ob die Host- und iDRAC-Anmeldeinformationen korrekt sind. Dieser Schritt ist zwar optional, Dell EMC empfiehlt jedoch den Test des Verbindungsprofils.

ANMERKUNG: Wenn der WBEM-Dienst für alle Hosts, auf denen ESXi 6.5 oder höher ausgeführt wird, deaktiviert ist, wird WBEM automatisch aktiviert, wenn Sie die Verbindung testen und die Bestandsaufnahme auf diesen Hosts durchführen.

ANMERKUNG: Wenn Sie Alle registrierten vCenter beim Erstellen des Verbindungsprofils auswählen, schlägt das Testen der Verbindung für alle Hosts fehl, auf denen ESXi 6.5 oder höher ausgeführt wird und auf denen der WBEM-Dienst deaktiviert ist. In einem solchen Fall wird empfohlen, die Aktionen des Verbindungsprofilassistenten abzuschließen, die Bestandsaufnahme auf den Hosts durchzuführen und dann das Verbindungsprofil erneut zu prüfen.

ANMERKUNG: Möglicherweise sehen Sie, dass der Verbindungstest für den Host fehlschlägt und darauf hingewiesen wird, dass ungültige Anmeldeinformationen eingegeben wurden, obwohl gültige Anmeldeinformationen eingegeben wurden. Es kann vorkommen, dass die ESXi den Zugriff blockiert. Warten Sie 15 Minuten und versuchen Sie dann erneut, die Verbindung zu testen.

8 Zur Erstellung des Profils klicken Sie auf **Weiter**.

Nachdem Sie auf „Weiter“ klicken, werden alle Details, die Sie in diesem Assistenten eingeben, gespeichert, und Sie können die Details über den Assistenten nicht mehr ändern. Sie können weitere Verbindungsprofile für dieses vCenter-Detail über die Seite **Profile** > **verwalten Verbindungsprofile** ändern oder erstellen, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Siehe **Ändern von Verbindungsprofilen** im *OpenManage Integration for VMware vCenter-Benutzerhandbuch* unter Dell.com/support/manuals. .

ANMERKUNG: Bei Servern, die nicht über eine iDRAC Express- oder Enterprise-Karte verfügen, ist das Ergebnis für den iDRAC-Verbindungstest Für dieses System nicht anwendbar.

Wenn Hosts einem Verbindungsprofil hinzugefügt werden, wird die IP-Adresse von OMIVV automatisch auf das SNMP Trap-Ziel des iDRAC des Hosts gesetzt, und OMIVV aktiviert automatisch den WBEM (Web-Based Enterprise Management)-Service für Hosts mit ESXi 6.5 und höher. 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 nicht konformer Hosts, bei denen das SNMP Trap-Ziel neu konfiguriert werden muss und/oder die WBEM Services aktiviert werden müssen, finden Sie unter **Berichterstattung und Festsetzen der Kompatibilität für vSphere Hosts** im *OpenManage Integration for VMware vCenter-Benutzerhandbuch* unter Dell.com/support/manuals. .

Planen von Bestandsaufnahme-Jobs

Info über diese Aufgabe

Sie können den Bestandsaufnahmen-Zeitplan unter Verwendung des Konfigurationsassistenten oder OpenManage Integration unter der Registerkarte **OpenManage Integration** > **Verwalten** > **Einstellungen** konfigurieren.

ANMERKUNG: Um sicherzustellen, dass OMIVV weiterhin aktualisierte Informationen anzeigt, wird empfohlen, dass Sie einen regelmäßigen Bestandsaufnahme-Job planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

ANMERKUNG: Ein Gehäuse wird automatisch erkannt, sobald die Bestandsaufnahme für alle Hosts ausgeführt wurde. Wenn das Gehäuse zu einem Gehäuse-Profil hinzugefügt wird, wird die Bestandsaufnahme automatisch ausgeführt. In einer SSO-Umgebung mit mehreren vCenter-Severn wird die Gehäusebestandsaufnahme automatisch bei jedem vCenter ausgeführt, wenn die Bestandsaufnahme für ein beliebiges vCenter planmäßig ausgeführt wird.

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 Wählen Sie im **Erstkonfigurationsassistenten** im Fenster **Bestandsaufnahme-Zeitplan Bestandsaufnahme-Datenabruf aktivieren** aus, falls dies nicht aktiviert ist. **Abrufen von Bestandsaufnahmedaten** ist standardmäßig aktiviert.

2 Führen Sie unter **Zeitplan für den Abruf von Bestandsaufnahmedaten** folgende Schritte durch:

   a Aktivieren Sie die Kontrollkästchen neben den Wochentagen, an denen eine Bestandsaufnahme erstellt werden soll.

   Standardmäßig ist die Option **Auf alle Tage** ausgewählt.

   b Geben Sie in **Uhrzeit für Bestandsaufnahme-Datenabruf** die Zeit im Format SS:MM ein.

   Bei der von Ihnen eingegebenen Zeit muss es sich um die bei Ihnen geltende Ortszeit handeln. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.

   c Klicken Sie auf **Weiter**, um die Änderungen zu übernehmen und fortzufahren.

Sobald Sie auf "Weiter" klicken, werden alle Details, die Sie in diesem Assistenten angeben, gespeichert. Sie können die Details nicht mithilfe dieses Assistenten ändern. Sie können die Details zum Bestandsaufnahme-Zeitplan der Hosts über die Registerkarte **Verwalten** > **Einstellungen** ändern, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Weitere Informationen finden Sie unter **Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme** im *OpenManage Integration for VMware vCenter User's Guide (Benutzerhandbuch)* unter Dell.com/support/manuals.

Ausführen von Serviceabfrage-Jobs

Info über diese Aufgabe

Die Konfiguration für Serviceabfrage-Jobs ist in OMIVV unter "Einstellungen" verfügbar. Darüber hinaus können Serviceabfrage-Jobs auch unter **Job-Warteschlange** > **Service** ausgeführt bzw. geplant werden. Die geplanten Jobs werden in der Job-Warteschlange aufgelistet. In einer SSO-Umgebung mit mehreren vCenter-Servern wird die Gehäusegarantie automatisch bei jedem vCenter ausgeführt, wenn die Garantie für ein beliebiges vCenter ausgeführt wird. Jedoch wird der Service nicht automatisch hinzugefügt, wenn er nicht zum Gehäuseprofil 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 Im Dialogfeld **Servicezeitplan** wählen Sie **Serviceabruf aktivieren**.

2 Führen Sie unter **Serviceabrufzeitplan** eine der folgenden Aktionen aus:

   a Aktivieren Sie das Kontrollkästchen neben den Wochentagen, an denen die Garantie ausgeführt werden soll.

   b Geben Sie die Uhrzeit in dem Format SS:MM ein.

   Bei der von Ihnen eingegebenen Zeit muss es sich um die bei Ihnen geltende Ortszeit handeln. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.

3 Um die Änderungen anzuwenden und fortzufahren, klicken Sie auf **Weiter** und fahren Sie mit den Einstellungen unter **Alarm und Ereignis** fort.

Nachdem Sie auf „Weiter“ klicken, werden alle Details, die Sie in diesem Assistenten eingeben, gespeichert, und Sie können die Details über den Assistenten nicht mehr ändern. Sie können die Details zum Serviceabfrage-Zeitplan über die Registerkarte **Einstellungen** ändern, nachdem Sie die Konfiguration über den Konfigurationsassistenten abgeschlossen haben. Weitere Informationen finden Sie unter **Modifizieren eines Zeitplans zum Erstellen eines Service-Jobs** im *OpenManage Integration for VMware vCenter User's Guide (Benutzerhandbuch)* unter **Dell.com/support/manuals**.

Konfigurieren von Ereignissen und Alarmen

Sie können Ereignisse und Alarme unter Verwendung des **Konfigurationsassistenten** oder über die Registerkarte **Einstellungen** für Ereignisse und Alarme einrichten. Zum Empfangen von Ereignissen von Servern wird OMIVV als Trap-Ziel konfiguriert. Bei Hosts der 12. Generation und höher müssen die SNMP-Trap-Ziele in iDRAC festgelegt sein. Bei Hosts vor der 12. Generation müssen die Trap-Ziele in OMSA eingestellt sein.

Info über diese Aufgabe

ANMERKUNG: OMIVV unterstützt SNMP-v1 und v2-Alarme für Hosts der 12. Generation und höher. Bei Hosts vor der 12. Generation unterstützt OMIVV nur SNMP v1-Warnungen.

Schritte

1 Wählen Sie im **Erstkonfigurationsassistenten** unter **Anzeigeebenen für das Ereignis** eine der folgenden Optionen:

- Keine Ereignisse übermitteln – Hardware-Ereignisse blockieren
- Alle Ereignisse übermitteln – Alle Hardware-Ereignisse übermitteln
- Nur kritische Ereignisse und Warnungsereignisse übermitteln – Nur kritische und Warnungsereignisse der Hardware übermitteln
- Nur kritische Ereignisse und Warnungsereignisse in Bezug auf Virtualisierung übermitteln – Nur kritische und Warnungsereignisse in Bezug auf Virtualisierung übermitteln ist die Standardeinstellung für die Ereignis-Übermittlung

2 Wählen Sie **Alarme für alle Dell EMC Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

ANMERKUNG: Dell EMC Hosts mit aktivierten Alarmen reagieren auf bestimmte kritische Ereignisse, indem sie in den Wartungsmodus übergehen; Sie können den Alarm nach Bedarf ändern.

Das Dialogfeld **Aktivieren der Dell EMC Alarmwarnung** wird angezeigt.

3 Um die Änderung zu akzeptieren, klicken Sie auf **Fortsetzen** oder, um den Vorgang abzubrechen, klicken Sie auf **Abbrechen**.

ANMERKUNG: Sie müssen diesen Schritt nur dann abschließen, wenn Alarme für Dell EMC Hosts aktivieren ausgewählt wurde.

4 Klicken Sie auf **Standard-Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell EMC Server im vCenter wiederherzustellen.

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

ANMERKUNG: Nach dem Wiederherstellen des Geräts sind die Einstellungen für Ereignisse und Alarme nicht aktiviert, selbst wenn die GUI „Aktiviert“ anzeigt. Sie können die Einstellungen Ereignisse und Alarme über die Registerkarte Einstellungen erneut aktivieren.

ANMERKUNG: BMC-Traps verfügen nicht über Meldungs-IDs. Warnungen enthalten also demzufolge diese Details nicht in OMIVV.

5 Klicken Sie auf **Anwenden**.

Konfigurieren einer SNMP-Trap-Communityzeichenfolge

1 Klicken Sie auf der Seite **OpenManage Integration for VMware vCenter** auf der Registerkarte **Verwalten** > **Einstellungen** unter **Geräteeinstellungen** auf das ✎ an der **OMSA-SNMP-Trap-Communityzeichenfolge**.

Das Dialogfeld **Einstellungen zur OMSA-SNMP-Trap-Communityzeichenfolge** wird angezeigt. Standardmäßig wird in der SNMP-Trap-Communityzeichenfolge **public** angezeigt.

2 Passen Sie den **public**-Text an eine beliebige Zeichenfolge an und klicken Sie auf **Anwenden**.

ANMERKUNG: Die Konfiguration der SNMP-Trap-Communityzeichenfolge für PowerEdge-Server der 11. Generation wird während der Installation oder Aktualisierung von OMSA über OMIVV festgelegt.

Konfigurationsaufgaben über die Registerkarte Einstellungen

Unter Verwendung der Registerkarte Einstellungen können Sie die folgenden Konfigurationsaufgaben anzeigen und ausführen:

- Aktivieren Sie den OMSA-Link. Lesen Sie dazu Aktivieren des OMSA-Links.
- Konfigurieren Sie die Serviceablaufbenachrichtigungseinstellungen. Lesen Sie dazu Konfigurieren der Serviceablaufbenachrichtigungseinstellungen.
- Richten Sie das Firmware-Aktualisierungs-Repository ein. Lesen Sie dazu Einrichten des Firmware-Aktualisierungs-Repositorys.
- Konfigurieren Sie die Benachrichtigung zur aktuellen Geräteversion. Lesen Sie dazu Konfigurieren der Benachrichtigung zur aktuellen Geräteversion.
- Konfigurieren Sie Ereignisse und Alarme und zeigen Sie sie an. Siehe Konfigurieren von Ereignissen und Alarmen.
- Zeigen Sie die Datenabrufzeitpläne für Bestandsaufnahme und Service an. Lesen Sie dazu Anzeigen der Datenabrufzeitpläne für Bestandsaufnahme und Service.

Geräteeinstellungen

In diesem Abschnitt konfigurieren Sie das folgende OMIVV-Gerät:

- Garantieablaufbenachrichtigung
- Repository für die Firmware-Aktualisierung
- Benachrichtigung über aktuelle Geräteversion
- Anmeldeinformationen für die Bereitstellung

Konfigurieren von Serviceablaufbenachrichtigungseinstellungen

1. Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **unter Geräteeinstellungen** auf **Serviceablaufbenachrichtigung**.
2. Erweitern Sie **Serviceablaufbenachrichtigung** zur Anzeige folgender Optionen:
   - **Serviceablaufbenachrichtigung** – Zeigt an, ob die Einstellung aktiviert oder deaktiviert ist
   - **Warnung** – Einstellung der Anzahl der Tage bis zur ersten Warnung
   - **Kritisch** – Einstellung der Anzahl der Tage bis zur kritischen Warnung
3. Zur Konfiguration der Serviceablaufschwellenwerte für eine Warnung zum Serviceablauf klicken Sie auf das Symbol auf der rechten Seite der **Serviceablaufbenachrichtigung**.
4. Verfahren Sie im Dialogfeld **Serviceablaufbenachrichtigung** wie folgt:
   a. Falls Sie diese Einstellung aktivieren möchten, wählen Sie **Serviceablaufbenachrichtigung für Hosts aktivieren** aus.
   Durch die Auswahl des Kontrollkästchens wird die Serviceablaufbenachrichtigung aktiviert.
   b. Verfahren Sie unter **Mindesttageschwellenwertalarm** wie folgt:
      1. Wählen Sie in der Drop-Down-Liste **Warnung** den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf des Service gewarnt werden wollen.
      2. Wählen Sie in der Drop-Down-Liste **Kritisch** den zeitlichen Abstand in Tagen aus, mit dem Sie vor Ablauf des Service gewarnt werden wollen.
5. Klicken Sie auf **Anwenden**.

Repository für die Firmwareaktualisierung einrichten

Info über diese Aufgabe

Sie können das Firmware-Aktualisierungs-Repository der Registerkarte **Einstellungen** von OMIVV erstellen.

ANMERKUNG: Sie können die Firmware über dieses Repository nur für Nicht-VSAN-Hosts und Cluster aktualisieren.

Schritte

1 Klicken Sie in OpenManage Integration für VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **Geräteeinstellungen** auf der rechten Seite des Repository für die **Firmwareaktualisierung** auf das Symbol .

2 Wählen Sie im Dialogfeld **Repository für die Firmware-Aktualisierung** eine der folgenden Optionen aus:

- **Dell Online**: Das Standard-Repository für Firmwareaktualisierungen ist auf Dell Online (**https://downloads.dell.com**) eingestellt. OMIVV lädt die ausgewählte Firmware-Aktualisierung vom Dell Repository herunter und aktualisiert die verwalteten Hosts.
- **Dell Custom Online**: OMIVV lädt die ausgewählten Firmware-Updates von Dell Custom Online herunter und wendet sie bei Bedarf auf die verwalteten Hosts an.

  ANMERKUNG: Basierend auf den Netzwerkeinstellungen müssen Proxy-Einstellungen aktiviert werden, wenn das Netzwerk einen Proxy benötigt.

- **Freigegebener Netzwerkordner**: Sie können über ein lokales Repository der Firmware in einer CIFS-basierten oder NFS-basierten Netzwerkfreigabe verfügen. Dieses Repository kann ein Abbild der Server Update Utility (SUU), das Dell regelmäßig veröffentlicht, oder ein benutzerdefiniertes Repository sein, das unter Verwendung von DRM erstellt wurde. OMIVV muss auf diese Netzwerkfreigabe zugreifen können.

  ANMERKUNG: Wenn Sie CIFS-Freigabe verwenden, dürfen die Kennwörter für Repositorien nicht mehr als 31 Zeichen umfassen.

  ANMERKUNG: Stellen Sie sicher, dass Sie die neueste DRM-Version (Dell EMC Repository Manager) (3.0) verwenden.

  a Wenn Sie **Dell Custom Online** auswählen, geben Sie den **Katalog-Onlinepfad** im folgenden Format ein:
  - http://Freigabe/Dateiname.xml.gz
  - http://Freigabe/Dateiname.gz
  - https://Freigabe/Dateiname.xml.gz
  - https://Freigabe/Dateiname.gz

  b Wenn Sie **Freigegebenen Netzwerkordner** ausgewählt haben, dann geben Sie den **Speicherort der Katalogdatei** im folgenden Format ein:
  - NFS-Freigabe für xml-Datei – Host:/Freigabe/Dateiname.xml
  - NFS-Freigabe für gz-Datei – Host:/Freigabe/Dateiname.gz
  - CIFS-Freigabe für xml-Datei – \\host\Freigabe\Dateiname.xml
  - CIFS-Freigabe für gz-Datei – \\host\Freigabe\Dateiname.gz

  ANMERKUNG: OMIVV unterstützt nur Server Message Block(SMB)-Version 1.0- und SMB-Version 2.0-basierte CIFS-Freigaben. Dell EMC empfiehlt die Verwendung von Freigaben auf Basis von SMB-Version 2.0.

  ANMERKUNG: Wenn Sie CIFS-Freigabe verwenden, fordert OMIVV Sie dazu auf, den Benutzernamen und das Kennwort einzugeben.

  c Um den Speicherort der angegebenen Katalogdatei zu überprüfen, klicken Sie auf **Test starten**. Diese Validierung ist zwingend erforderlich, um fortzufahren.

  : Zeigt an, dass die Testverbindung erfolgreich ist.

  : Zeigt an, dass die Testverbindung fehlgeschlagen ist.

3 Klicken Sie auf **Anwenden**.

ANMERKUNG: Es kann bis zu 10 Minuten ab Lesen des Katalog von der Quelle und aktualisieren der OMIVV-Datenbank dauern.

Erstellen von Katalogen in DRM mithilfe von OMIVV

Info über diese Aufgabe

Dieser Abschnitt beschreibt das Verfahren zum Erstellen eines Katalogs in DRM Version 3.0 und höher.

Schritte

1 Klicken Sie auf der Startseite auf **Neues Repository hinzufügen**.

Das Fenster **Repository hinzufügen** wird aufgerufen.

2 Führen Sie im Fenster **Repository hinzufügen** die folgenden Schritte aus:

a Geben Sie den **Repository-Namen** und eine **Beschreibung** an.

b Wählen Sie im Drop-Down-Menü **Basiskatalog** einen Katalog aus.

c Wählen Sie im Drop-Down-Menü **Integration-Typ OpenManage Integration for VMware vCenter** aus.

3 Geben Sie im Fenster **OpenManage Integration for VMware vCenter** die **Virtuelle Appliance-IP**, die **vCenter Server-IP**, den **Benutzernamen** und das **Passwort** ein und klicken Sie auf **Verbinden**.

Der erstellte Katalog wird auf der Startseite angezeigt.

4 Um den Katalog zu exportieren, wählen Sie einen Katalog aus und klicken Sie auf **Exportieren**.

Konfigurieren der Benachrichtigung über aktuelle Geräteversion

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 in OpenManage Integration for VMware vCenter auf die Registerkarte **Verwalten → Einstellungen** unter **Geräteeinstellungen**, rechts neben **Benachrichtigung über aktuelle Geräteversion** auf das Symbol für klicken.

Standardmäßig ist die Benachrichtigung zur aktuellen Version deaktiviert.

2 Führen Sie im Dialogfeld **Benachrichtigung zur aktuellen Version und Abrufplan** folgende Schritte aus:

a Wenn Sie die Benachrichtigung zur aktuellen Version aktivieren möchten, wählen Sie das Kontrollkästchen **Benachrichtigung zur aktuellen Version aktivieren** aus.

b Wählen Sie unter **Letzter Serviceabrufzeitplan** die Wochentage für den Job aus.

c Geben Sie bei **Abrufzeit der aktuellen Version** die erforderliche Ortszeit an.

Die von Ihnen angegebene Zeit entspricht Ihrer Ortszeit. Stellen Sie sicher, dass Sie jeglichen Zeitunterschied zur Ausführung dieser Aufgabe für die Zeit auf dem OMIVV-Gerät einkalkulieren.

3 Klicken Sie zum Speichern der Einstellungen auf **Anwenden**, klicken Sie zum Zurücksetzen der Einstellungen auf **Löschen**, und klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.

Konfigurieren von Anmeldeinformationen für die Bereitstellung

Die Anmeldeinformationen für die Bereitstellung ermöglichen Ihnen die Einrichtung der Anmeldeinformationen zur sicheren Kommunikation mit einem Bare-Metal-System, das mithilfe der Auto-Ermittlung erkannt wird, bis die Bereitstellung des Betriebssystems vollständig ist. Zur sicheren Kommunikation mit iDRAC verwendet OMIVV Anmeldeinformationen für die Bereitstellung von der ersten Erfassung bis zum Ende des Bereitstellungsprozesses. Nachdem der BS-Bereitstellungsvorgang erfolgreich abgeschlossen wurde, ändert OMIVV die Anmeldeinformationen von iDRAC wie im Verbindungsprofil angegeben. Wenn Sie die Anmeldeinformationen der Bereitstellung ändern, werden alle neu erkannten Systeme ab diesem Punkt mit den neuen Anmeldeinformationen bereitgestellt. Die Anmeldeinformationen auf Servern, die vor der Änderung der Anmeldeinformationen der Bereitstellung erfasst wurden, sind von dieser Änderung nicht betroffen.

Info über diese Aufgabe

ANMERKUNG: OMIVV fungiert als Bereitstellungsserver. Die Anmeldeinformationen für die Bereitstellung werden benutzt, um mit dem iDRAC zu kommunizieren, der das OMIVV-Plug-in als Provisionierungsserver im Prozess der automatischen Ermittlung verwendet.

Schritte

1 Klicken Sie in OpenManage Integration for VMware vCenter auf die Registerkarte **Einstellungen** > **Verwalten** unter **Geräteeinstellungen** auf der rechten Seite der **Anmeldeinformationen der Bereitstellung** auf das Symbol für .

2 Geben Sie in **Anmeldeinformationen für die Bereitstellung eines Bare-Metal-Servers** unter **Anmeldeinformationen** die folgenden Werte ein:

- Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
  Der Benutzername darf nicht mehr als 16 (ASCII-druckbare Zeichen) umfassen.
- Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
  Das Kennwort darf nicht mehr als 20 (ASCII-druckbare Zeichen) umfassen.
- Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
  Stellen Sie sicher, dass die Kennwörter übereinstimmen.

3 Zum Speichern der angegebenen Anmeldeinformationen klicken Sie auf **Anwenden**.

vCenter-Einstellungen

In diesem Abschnitt konfigurieren Sie die folgenden vCenter-Einstellungen:

- Aktivieren von OMSA-Links. Siehe Aktivieren des OMSA-Links.
- Ereignisse und Alarme konfigurieren. Siehe Konfigurieren von Ereignissen und Alarmen.
- Konfigurieren von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service. Siehe Konfigurieren von Zeitplänen für den Abruf von Daten für Bestandsaufnahmen und Service.

Aktivieren von OMSA-Link

Voraussetzung

Installieren und konfigurieren Sie den OMSA Web Server vor dem Aktivieren des OMSA-Links. Anweisungen, wie Sie den Webserver für die verwendete OMSA-Version installieren und konfigurieren finden Sie im Installationshandbuch *Dell OpenManage Server Administrator Installation Guide*.

Info über diese Aufgabe

ANMERKUNG: OMSA wird nur auf PowerEdge-Servern der 11. Generation benötigt.

Schritte

1 Klicken Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Einstellungen** > **Verwalten** unter **vCenter-Einstellungen** rechts neben der URL des OMSA Webservers auf das Symbol für .

2 Geben Sie im Dialogfeld **OMSA-Web-Server-URL** die URL ein.
Stellen Sie sicher, dass Sie die vollständige URL zusammen mit HTTPS und der Portnummer 1311 angeben.

https://<OMSA Server-IP oder FQDN>:1311

3 Zur Anwendung der OMSA-URL auf alle vCenter wählen Sie **Diese Einstellungen auf alle vCenter anwenden** aus.

ANMERKUNG: Wenn Sie das Kontrollkästchen nicht aktivieren, wird die OMSA-URL nur auf ein vCenter angewandt.

4 Um zu überprüfen, ob der OMSA-URL-Link, den Sie bereitgestellt haben, funktioniert, navigieren Sie zur Registerkarte **Zusammenfassung** des Hosts und überprüfen Sie, ob der OMSA-Konsolenlink im Abschnitt **OMIVV Host-Information** aktiv ist.

Konfigurieren von Ereignissen und Alarmen

Info über diese Aufgabe

Das Dialogfeld **Ereignisse und Alarme** aktiviert oder deaktiviert alle Hardware-Alarme. Der aktuelle Alarm-Status wird auf der Registerkarte „Alarme“ im vCenter angezeigt. Ein kritisches Ereignis deutet auf einen tatsächlichen oder bevorstehenden Datenverlust oder auf einen Systemausfall hin. Ein Warnereignis bedarf nicht unbedingt sofortiger Aufmerksamkeit, kann aber auf ein mögliches zukünftiges Problem hindeuten.

Die Ereignisse und Alarme können auch mit dem VMware Alarm Manager aktiviert werden. Die Ereignisse werden auf der Registerkarte „Tasks und Ereignisse“ im vCenter in der Ansicht „Hosts und Cluster“ angezeigt. Um die Ereignisse von den Servern zu empfangen, ist OMIVV als SNMP-Trap-Ziel konfiguriert. Für Hosts der 12. Generation und höher wird das SNMP-Trap-Ziel in iDRAC festgelegt. Bei Hosts vor der 12. Generation wird das Trap-Ziel in OMSA eingestellt. Sie können die Ereignisse und Alarme in Dell OpenManage Integration for VMware vCenter auf der Registerkarte **Verwaltung** > **Einstellungen** konfigurieren. Erweitern Sie unter den vCenter-**Einstellungen** die Überschrift **Ereignisse und Alarme** zur Anzeige der vCenter-Alarme für Dell EMC Hosts (Aktiviert oder Deaktiviert) und der Ereignisanzeigeebene.

ANMERKUNG: OMIVV unterstützt SNMP v1-Alarme und -v2-Alarme für Hosts der 12. Generation und höher. Bei Hosts vor der 12. Generation unterstützt OMIVV SNMP v1-Alarme.

ANMERKUNG: Um die Dell Ereignisse zu erhalten, müssen Sie Alarme sowie Ereignisse aktivieren.

Schritte

1. Erweitern Sie in OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** > **Einstellungen** unter **vCenter Einstellungen Ereignisse und Alarme**.

   Es werden die aktuellen **vCenter-Alarme für Dell EMC Hosts** (Aktiviert/Deaktiviert) oder alle vCenter-Alarme und die **Ereignisanzeigeebene** angezeigt.

2. Klicken Sie auf das Symbol rechts neben **Ereignisse und Alarme**.
3. Wählen Sie **Alarme für alle Dell EMC Hosts aktivieren**, um alle Hardware-Alarme und -Ereignisse zu aktivieren.

   ANMERKUNG: Die Dell EMC Hosts mit aktivierten Alarmen reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus wechseln; Sie können den Alarm nach Bedarf ändern.
4. Klicken Sie auf **Standard-Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die durch diesen Schritt bewirkten Änderung in Kraft treten; er ist nur verfügbar, wenn **Alarme für Dell EMC Hosts aktivieren** ausgewählt ist.
5. Wählen Sie unter **Ereignisanzeigeebene** entweder „Keine Ereignisse veröffentlichen“, „Alle Ereignisse veröffentlichen“, „nur kritische Ereignisse und Warnungsereignisse veröffentlichen“ oder „nur virtualisierungsbezogene kritische Ereignisse und Warnungsereignisse veröffentlichen“ aus. Weitere Informationen finden Sie im Abschnitt **Ereignisse, Alarme und Systemüberwachung** im *OpenManage Integration for VMware vCenter User's Guide (Benutzerhandbuch)*.
6. Falls Sie diese Einstellungen auf alle vCenters anwenden möchten, wählen Sie **Diese Einstellungen auf alle vCenters anwenden** aus.

   ANMERKUNG: Die Auswahl der Option überschreibt die vorhandenen Einstellungen für alle vCenters.

   ANMERKUNG: Die Option ist nicht verfügbar, wenn Sie bereits Alle registrierten vCenter aus der Dropdown-Liste auf der Registerkarte Einstellungen ausgewählt haben.
7. Klicken Sie zum Speichern auf **Anwenden**.

Anzeigen der Datenabrufzeitpläne für Bestandsaufnahme und Service

1. Klicken Sie in OpenManage Integration with VMware vCenter auf die Registerkarte **Verwalten** > **Einstellungen** unter **vCenter-Einstellungen** auf **Zeitplan für den Abruf von Daten**.

Der „Zeitplan für den Abruf von Daten“ wird bei Anklicken erweitert, um die Zeitpläne für Bestandsaufnahme und Service aufzudecken.

2 Klicken Sie auf das Symbol neben **Bestandslistenabfrage** oder **Serviceabfrage**.

Im Dialogfeld **Bestandslisten-/Serviceabfrage** können Sie die folgenden Informationen zur Bestandslisten- oder Serviceabfrage anzeigen:

- Sie sehen, ob die Bestandsaufnahme- und/oder Serviceabfrage aktiviert oder deaktiviert ist.
- Sie sehen die Wochentage, für die diese Option aktiviert ist.
- Sie sehen die Tageszeit, zu der sie aktiviert ist.

3 Wenn Sie den Zeitplan für den Abruf von Daten ändern wollen, Führen Sie die folgenden Schritte durch:

a Aktivieren Sie unter **Bestandsaufnahme-/Servicedaten** das Kontrollkästchen **Bestandsaufnahme-/Servicedatenabruf aktivieren**.

b Wählen Sie unter **Datenabrufzeitpläne für Bestandsaufnahme/Service** die Wochentage für den Job aus.

c Geben Sie im Textfeld **Uhrzeit des Datenabrufs zu Bestandsaufnahme/Service** die Ortszeit für diesen Job ein.

Möglicherweise müssen Sie den Zeitunterschied zwischen Job-Konfiguration und Job-Umsetzung berücksichtigen.

d Klicken Sie zum Speichern der Einstellungen auf **Anwenden**, klicken Sie zum Zurücksetzen der Einstellungen auf **Löschen**, und klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.

4 Klicken Sie erneut auf **Zeitplan für den Abruf von Daten**, um die Pläne der Bestandsaufnahme und den Service zusammenzuführen und in einer einzigen Zeile anzuzeigen.

Erstellen eines Gehäuse-Profils

Für die Überwachung des Gehäuses wird ein Gehäuse-Profil benötigt. Gehäuse-Anmeldeinformationenprofile können einem oder mehreren Gehäusen zugewiesen werden.

Info über diese Aufgabe

Sie können sich am iDRAC und dem Host mithilfe von Active Directory-Anmeldeinformationen anmelden.

Schritte

1 Klicken Sie in OpenManage Integration for VMware vCenter auf **Verwalten**.

2 Klicken Sie auf **Profile**, und klicken Sie dann auf **Anmeldeprofile**.

3 Erweitern Sie **Anmeldedaten-Profile**, und klicken Sie auf die Registerkarte **Gehäuseprofile**.

4 Klicken Sie auf der Seite **Gehäuse-Profile** auf das Symbol , um ein **Neues Gehäuse-Profil** zu erstellen.

5 Führen Sie auf der Seite des **Gehäuse-Profil-Assistenten** die folgenden Schritte aus:

Führen Sie Folgendes im Abschnitt **Name und Anmeldeinformationen** unter **Gehäuseprofil** aus:

a Geben Sie den Profilnamen in das Textfeld **Profilname** ein.

b Geben Sie im Textfeld **Beschreibung** eine Beschreibung ein, dies ist optional.

Führen Sie Folgendes im Abschnitt **Anmeldeinformationen** aus:

a Geben Sie im Textfeld **Benutzername** den Benutzernamen mit Administratorrechten ein, der in der Regel für die Anmeldung am Chassis Management Controller verwendet wird.

b Geben Sie im Textfeld **Kennwort** das Kennwort für den entsprechenden Benutzernamen ein.

c Geben Sie im Textfeld **Kennwort überprüfen** dasselbe Kennwort ein, das Sie im Textfeld **Kennwort** eingegeben haben. Die Kennwörter müssen übereinstimmen.

ANMERKUNG: Bei den Anmeldeinformationen kann es sich um lokale oder Active-Directory-Anmeldeinformationen handeln. Bevor Sie die Active Directory-Anmeldeinformationen mit einem Verbindungsprofil verwenden, müssen das Active Directory-Benutzerkonto in Active Directory vorhanden, und der Chassis Management Controller für die Active Directory-basierte Authentifizierung konfiguriert sein.

6 Klicken Sie auf , um das Gehäuse dem Gehäuse-Profil zuzuordnen.

ANMERKUNG: Das Gehäuse, das erkannt wird, verfügbar ist und manuell mit MX-Gehäuse hinzufügen hinzugefügt wird, steht erst nach erfolgreicher Durchführung der Bestandsaufnahme aller unter jenem Gehäuse vorhandenen modularen Hosts für die Zuordnung zu diesem Gehäuseprofil zur Verfügung.

7 Um entweder ein einzelnes Gehäuse oder mehrere Gehäuse auszuwählen, wählen Sie die entsprechenden Kontrollkästchen neben der Spalte **IP/Host-Name** aus.

Wenn das ausgewählte Gehäuse bereits Teil eines anderen Profils ist, wird eine Warnungsmeldung angezeigt, die darauf hinweist, dass das ausgewählte Gehäuse einem Profil zugeordnet ist.

Sie haben z. B. ein Profil **Test,** das Chassis A zugordnet ist. Wenn Sie ein anderes Profil, **Test 1,** erstellen und versuchen, Gehäuse A **Test 1** zuzuordnen, wird eine Warnmeldung angezeigt.

8 Auf **OK**.klicken.

Die Seite **Zugewiesene Gehäuse** wird angezeigt.

9 Das Testen der Verbindung ist obligatorisch und wird für das ausgewählte Gehäuse automatisch ausgeführt.

Der Verbindungstest wird automatisch ausgeführt:

- Zum ersten Mal nach Auswahl des Gehäuses
- Wenn die Anmeldeinformationen geändert werden
- Wenn das Gehäuse neu ausgewählt wurde

ANMERKUNG: Für ein mit einer MCM-Gruppe konfiguriertes MX-Gehäuse empfiehlt Dell EMC die Verwaltung aller Führungs- und Mitgliedsgehäuse unter Verwendung des Hauptgehäuses. Der Vorgang des Verbindungstests für Mitgliedsgehäuse schlägt fehl und der Testergebnisstatus wird als Fehler angezeigt. Klicken Sie auf den IP-Link des Hauptgehäuses, um die gesamte MCM-Gruppe zu ermitteln.

Das Testergebnis wird in der Spalte **Testergebnis** als **Erfolgreich** oder **Fehlgeschlagen** angezeigt. Um die Konnektivität des Gehäuses manuell zu testen, wählen Sie das Gehäuse aus und klicken Sie auf  .

ANMERKUNG: Wenn in den registrierten vCenters keine mit dem hinzugefügten MX-Gehäuse verknüpften Hosts vorhanden sind, schlägt der Test der jeweiligen Gehäuseverbindung fehl.

ANMERKUNG: Nur erfolgreich geprüfte Gehäuse werden dem Gehäuseprofil zugeordnet.

10 Um das Profil abzuschließen, klicken Sie auf **Fertig stellen**.

ANMERKUNG: Stellen Sie sicher, dass Sie über mindestens ein erfolgreich überprüftes Gehäuse verfügen, um den Assistenten abzuschließen.

Informationen zum Hinzufügen einer MX-Gehäuse-Managementmodul-IP finden Sie unter **Hinzufügen der MX-Gehäuse-IP oder des FQDN** im *Benutzerhandbuch*.

3

Zugriff auf Dokumente von der Dell EMC Support-Website

Sie können auf die Dokumente zugreifen, indem Sie die folgenden Links verwenden:

- Für Dokumente zu Dell EMC Enterprise Systems Management – www.dell.com/SoftwareSecurityManuals
- Für Dokumente zu Dell EMC OpenManage – www.dell.com/OpenManageManuals
- Für Dokumente zu Dell EMC Remote Enterprise Systems Management – www.dell.com/esmmanuals
- Für Dokumente zu iDRAC und Dell EMC Lifecycle Controller – www.dell.com/idracmanuals
- Für Dokumente zu Dell EMC OpenManage Connections Enterprise Systems Management – www.dell.com/OMConnectionsEnterpriseSystemsManagement
- Für Dokumente zu Dell EMC Serviceability Tools – www.dell.com/ServiceabilityTools
- a Rufen Sie die Website www.dell.com/Support/Home auf.

  b Klicken Sie auf **Wählen Sie aus allen Produkten**.

  c Klicken Sie im Abschnitt **Alle Produkte** auf **Software und Sicherheit**, und klicken Sie dann auf einen der folgenden Links:
  - **Verwaltung von Systemen der Enterprise-Klasse**
  - **Remote-Verwaltung von Systemen der Enterprise-Klasse**
  - **Wartungstools**
  - **Dell Client Command Suite**
  - **Connections Client-Systemverwaltung**

  d Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.
- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.

4

Zugehörige Dokumentation

Zusätzlich zu dieser Anleitung können Sie auf die anderen Anleitungen zugreifen, die unter **Dell.com/support** zur Verfügung stehen. Klicken Sie auf **Aus allen Produkten auswählen** und anschließend auf **Software und Sicherheit** > **Virtualisierungslösungen**. Klicken Sie auf **OpenManage Integration for VMware vCenter 4.3**, um auf die folgenden Dokumente zuzugreifen:

- *OpenManage Integration for VMware vCenter Version 4.3 Web Client User's Guide (OpenManage Integration for VMware vCenter Version 4.3 – Web-Client-Benutzerhandbuch)*
- *OpenManage Integration for VMware vCenter Version 4.3 Release Notes (OpenManage Integration for VMware vCenter Version 4.3 – Versionshinweise)*
- *OpenManage Integration for VMware vCenter Version 4.3 Compatibility Matrix (OpenManage Integration for VMware vCenter Version 4.3 – Kompatibilitäts-Matrix)*

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